



Перед вами вторая статья из цикла, посвященного System Center Mobile Device Manager 2008. В ней я расскажу о подготовке предприятия к внедрению SCMDM. Для того, чтобы материал был более понятным и жизненным, все описываемое в этой и следующей статьях, будет рассматриваться с позиции некоей абстрактной организации «Компания», которая развивается, несмотря на всякие мировые потрясения, и руководство которой достигло понимания того, что парк мобильных устройств должен управляться системными администраторами также, как и обычные настольные ПК.

На момент начала работ «Компания» владеет зарегистрированным доменным именем **company.ru**, обладает уже сформированной сетевой инфраструктурой на базе Active Directory и использует домен **company.local** в качестве внутреннего. Дополнительно оговорюсь, что при развертывании будет создан один экземпляр службы MDM с именем **scmdmins**. Также будут задействованы два public IP из имеющегося в распоряжении «Компании» пула общедоступных IP-адресов.

Если попробовать схематично представить структуру, которая будет получена в процессе внедрения, то выйдет примерно следующее:

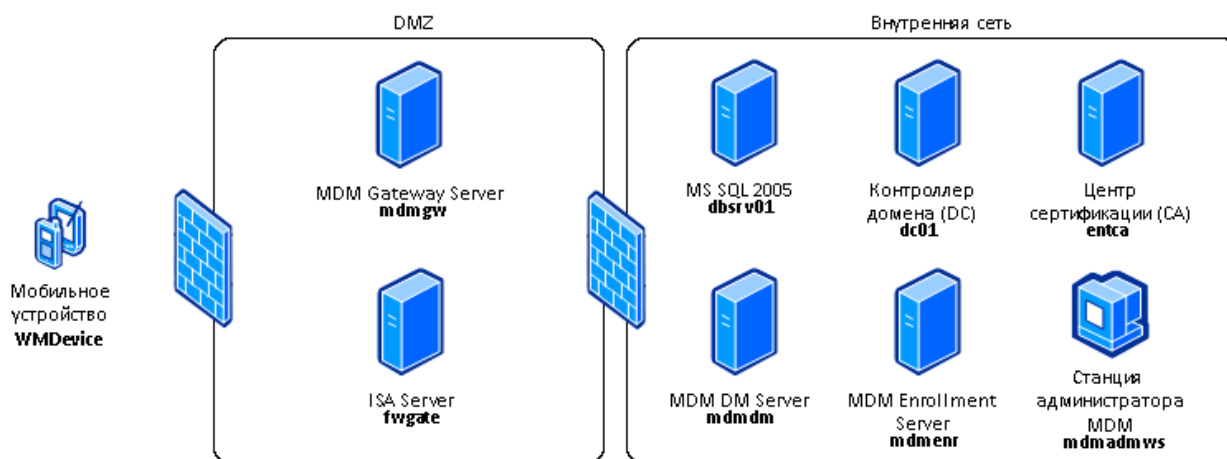


Рис. 1 Планируемая архитектура MDM после внедрения

Для того, чтобы работы прошли максимально эффективно и безболезненно, системные администраторы «Компании» решили разбить их на несколько этапов – обследование и планирование, подготовка, внедрение:

1. На этапе обследования и планирования выясняется, что есть в наличии и что необходимо добавить в существующую инфраструктуру для проведения успешного внедрения. Рассчитать нагрузку на систему и определить аппаратные требования к серверам<sup>1</sup>.

<sup>1</sup> Я не ставлю своей задачей показать весь процесс внедрения со стороны взаимоотношений заказчика и исполнителя (в данном случае руководства и ИТ-подразделения компании). Также, приведенные этапы могут быть дополнены при необходимости в зависимости от сложности инфраструктуры, масштаба внедрения и появления дополнительных требований от заказчика.

2. На этапе подготовки проводятся работы по добавлению недостающих служб в инфраструктуру предприятия, подготовке сетевого оборудования и подготовке службы каталогов Active Directory.
3. На этапе внедрения производится установка ролей MDM DM Server, MDM Enrollment Server, MDM Gateway Server и их первичная настройка, выполняется установка инструментов администратора MDM на его рабочую станцию.
4. Этап опытной эксплуатации.

Хочу еще раз предупредить, что в этой статье я пройду этапы 1 и 2, а 3-й этап будет в следующей... Итак, давайте рассмотрим подробнее **этап 1 – обследование и планирование**.

Те, кто прочитали [первую статью](#) о MDM, уже знают, что для внедрения MDM необходимо:

1. Уровень леса и домена не ниже Windows Server 2003 Native.
2. Дополнительные службы в сети предприятия, без которых внедрение MDM невозможно.

Именно эти требования становятся первыми, которые подвергаются проверке. В ходе обследования выясняется, что уровень леса и домена «Компании» соответствует требуемому, т.к. миграция с Windows Server 2000 успешно завершилась еще несколько лет назад и администраторы полностью используют возможности WS 2003.

Из дополнительных сервисов MDM требует:

- MS SQL Server 2005 в редакции не ниже Standard – используется для хранения базы данных о мобильных устройствах;
- Центр сертификации (CA) на базе Windows Server 2003 – используется для выпуска сертификатов для серверов MDM и управляемых устройств;
- Служба фильтрации сетевого трафика на базе ISA Server – не является обязательной, но Microsoft настоятельно рекомендует использовать ISA для безопасной публикации некоторых служб MDM, например MDM Enrollment Server.

Все из перечисленных служб присутствуют в сети<sup>2</sup>. Также в сети присутствует служба WSUS, но MDM требует, чтобы WSUS и MDM DM Server находились на одном сервере, поэтому необходимо развернуть еще один экземпляр. После того, как исследование инфраструктуры завершено, начинается этап изучения аппаратных требований. MDM использует систему различных ролей – MDM DM Server, MDM Enrollment Server, MDM Gateway Server – и для них есть рекомендованная аппаратная конфигурация, причем она является одинаковой для всех ролей:

---

<sup>2</sup> Описывать процесс установки и настройки этих сервисов я не буду, поэтому если будет нужна дополнительная информация, то наилучшим решением будет обратиться к документации по соответствующим продуктам и [библиотеке TechNet](#).

Таб. 1 Рекомендованная аппаратная конфигурация для компонентов MDM

Компонент	Требование
Центральный процессор	<ul style="list-style-type: none"> <li>Обязательно наличие 64-разрядного процессора на базе EM64T от Intel либо AMD64 от AMD</li> <li>Рекомендованная конфигурация должна иметь не менее 2-х процессоров, обладающих тактовой частотой не менее 2700 МГц</li> </ul>
Оперативная память	<ul style="list-style-type: none"> <li>4 Гб оперативной памяти</li> </ul>
Дисковое пространство	<ul style="list-style-type: none"> <li>100 Гб свободного пространства</li> </ul>
Сетевое оборудование	<ul style="list-style-type: none"> <li>Один сетевой адаптер с пропускной способностью 100 Мбит и выше на серверах, где размещены роли MDM DM Server и MDM Enrollment Server</li> <li>Два сетевых адаптера с пропускной способностью 100 Мбит и выше на серверах с ролью MDM Gateway Server</li> </ul>

Администраторы, оценив приведенные требования и изучив данные о допустимом количестве пользователей для каждой из ролей (до 15 000 пользователей MDM DM и Gateway, до 25 конкурирующих подключений на Enrollment Server), пришли к выводу, что 500 пользователей, устройствами которых требуется управлять, потребует от них выделения 3-х физических серверов<sup>3</sup>, которые они и заказывают.

На этом этап обследования и планирования заканчивается и начинается **2-й этап – подготовка к внедрению MDM.**

При внедрении MDM этап подготовки можно условно разбить на три подэтапа:

1. Подготовка серверов, на которые будет устанавливаться Система
2. Подготовка сетевого оборудования
3. Подготовка Active Directory к внедрению MDM

Вот об этом я и расскажу подробно.

После того, как сервера были доставлены, на них устанавливаются ОС и дополнительные компоненты, необходимые для установки MDM. Требования к операционной системе и дополнительным компонентам приведены в Таблице 2.

<sup>3</sup> В этой и следующей статье я не буду рассматривать вопросы практической организации отказоустойчивого решения, т.к. это однотипно по сравнению с имеющейся задачей и решается увеличением количества серверов и использованием балансировщиков нагрузки.

Таб. 2 Требования к операционной системе и дополнительным компонентам

Роль MDM	Операционная система	Дополнительные компоненты
MDM Device Management Server	Windows Server 2003 Standard x64 Edition with SP2	<ul style="list-style-type: none"> <li>Сервер должен являться членом домена AD</li> <li>.NET Framework 2.0 SP1 или выше</li> <li>IIS 6.0 с установленной службой World Wide Web Publishing</li> <li>Windows Server Update Services (WSUS) 3.0 SP1</li> <li>Опционально может быть установлена служба Microsoft Report Viewer для работы с отчетами</li> </ul>
MDM Enrollment Server		<ul style="list-style-type: none"> <li>Сервер должен являться членом домена AD</li> <li>.NET Framework 2.0 SP1 или выше</li> <li>IIS 6.0 с установленной службой World Wide Web Publishing</li> </ul>
MDM Gateway Server		<ul style="list-style-type: none"> <li>.NET Framework 2.0 SP1 или выше</li> <li>IIS 6.0 с установленной службой World Wide Web Publishing</li> </ul>

При установке WSUS на сервер, предназначенный для MDM DM Server, этот экземпляр настраивается как выделенный, потому что его конфигурация как downstream при наличии других WSUS в сети не рекомендована Microsoft.

После того, как сервера подготовлены, они разносятся в соответствующие сегменты сети и начинается настройка сетевого оборудования. Основная задача этого подэтапа – настроить фильтрацию трафика как между серверами MDM, так и между серверами и мобильными устройствами, обеспечив «хождение» необходимых данных.

Так, внешний межсетевой экран должен быть настроен на работу по следующим портам:

Таб. 3 Список портов, настраиваемый на внешнем брандмауэре

Назначение	Источник трафика	Точка назначения	Порт
Инициализация мобильных устройств	Неуправляемое мобильное устройство	Прокси-сервер с публикацией MDM Enrollment Server	TCP 443
Подключение устройства по Mobile VPN	Мобильное устройство, включенное в домен	MDM Gateway Server	UDP 500
			UDP 4500
			UDP 8901
			Protocol 50 IPsec

Помимо внешнего брандмауэра, необходимо настроить и внутренний межсетевой экран:

Таб. 4 Список портов, настраиваемый на внутреннем брандмауэре

Назначение	Источник трафика	Точка назначения	Порт
Служебный трафик	MDM DM Server	MDM Gateway Server	TCP 443
DNS	Мобильное устройство, включенное в домен	Внутренний сервер DNS	UDP 53
WINS		Внутренний сервер WINS	UDP 137
WSUS (нешифрованный)	MDM DM Server	Мобильное устройство, включенное в домен	TCP 8530
WSUS (с SSL)			TCP 8531

И есть еще одно действие, выполняемое на сетевом оборудовании на этом этапе. Более подробно оно будет описано в следующей статье, т.к. относится к настройке Gateway Server, но суть его сводится к добавлению постоянного маршрута в дополнительную подсеть на маршрутизаторах тех сетевых сегментов, с которыми будут работать мобильные устройства. Именно поэтому в таблицах портов присутствует два вида мобильных устройств – включенных в домен и не включенных.

После того, как все сетевое оборудование настроено, можно переходить к следующему шагу – подготовке Active Directory к внедрению MDM.

На этом этапе есть несколько нюансов, о которых я хотел бы заранее предупредить:

- При внедрении MDM **изменений в схему не вносится**, поэтому неудачная установка может быть безболезненно откатена назад.
- **Все создаваемые на этом этапе объекты (группы, подразделения, шаблоны) не могут быть переименованы.** Если вы попытаетесь проделать это, то получите неработоспособную Систему.
- При написании имен экземпляров MDM можно использовать только символы латинского алфавита A-Z, a-z, арабские цифры 0-9, черту (-), и подчеркивание(\_). Длина имени не должна превышать 30 символов.
- При указании имен экземпляров центра сертификации, содержащих пробелы в имени, необходимо имя сервера CA и имя экземпляра указывать в кавычках, например **/ca:"entca.company.local\enterprise ca"**.
- При указании имен серверов необходимо использовать их полное доменное имя (FQDN).

Подготовка AD выполняется при помощи утилиты Active Directory Configuration Tool (ADConfig), поставляемой вместе с инсталляционным пакетом MDM и заключается в следующем:

1. В командной строке выполняется команда на создание нового экземпляра MDM **ADConfig.exe /createInstance:<имя экземпляра MDM> /domain:<имя домена AD>**, в случае «Компании» это будет **ADConfig.exe /createInstance:scmdmins /domain:company.local**.

При выполнении команды будет выдано два сообщения:

*«This will create Active Directory containers, service connection points (SCPs), and universal groups for the System Center Mobile Device Manager instance: scmdmins in domain company.local. Do you want to proceed ([y|n])?»*

*«Checking the forest for MDM instance: scmdmins. The MDM instance scmdmins is not enabled for domain company.local. Do you want to enable the System Center Mobile Device Manager instance scmdmins for the domain company.local? This will enable devices in this domain to be managed by the System Center Mobile Device Manager scmdmins instance. Do you want to proceed ([y|n])?»*

В первом вам сообщают, что в процессе работы в AD будут созданы новые объекты и предлагают подтвердить ваше согласие на это, а во втором говорится, что созданный экземпляр MDM не связан с указанным доменом и предлагается подтвердить эту привязку.

В процессе выполнения этой команды вы увидите, что в каталоге AD создаются новые объекты:

**Таб. 5** Список создаваемых объектов AD

Объект	Тип	Расположение
SCMDM	container	CN=SCMDM,CN=System,DC=company,DC=local
SCMDM Infrastructure Groups	container	OU=SCMDM Infrastructure Groups,CN=System,DC=company,DC=local
SCMDM Managed Devices	container	OU=SCMDM Managed Devices (scmdmins),DC=company,DC=local
ServerAdmins	group	CN=SCMDMServerAdmins (scmdmins),CN=Users,DC=company,DC=local
DeviceAdmins	group	CN=SCMDMDeviceAdmins (scmdmins),CN=Users,DC=company,DC=local
DeviceSupport	group	CN=SCMDMDeviceSupport (scmdmins),CN=Users,DC=company,DC=local
HelpdeskOperator	group	CN=SCMDMHelpdeskOperator (scmdmins),CN=Users,DC=company,DC=local
DeviceManagementServers	group	CN=SCMDMDeviceManagementServers (scmdmins),OU=SCMDM Infrastructure Groups (scmdmins),DC=company,DC=local
EnrollmentServers	group	CN=SCMDMEnrollmentServers (scmdmins),OU=SCMDM Infrastructure Groups (scmdmins),DC=company,DC=local
EnrolledDevices	group	CN=SCMDMEnrolledDevices (scmdmins),OU=SCMDM Infrastructure Groups (scmdmins),DC=company,DC=local
SelfServiceServers	group	CN=SCMDMSelfServiceServers (scmdmins),OU=SCMDM Infrastructure Groups (scmdmins),DC=company,DC=local
AuthorizedUsers	group	CN=SCMDMAuthorizedUsers (scmdmins),CN=Users,DC=company,DC=local
ReadOnlyUsers	group	CN=SCMDMReadOnlyUsers (scmdmins),CN=Users,DC=company,DC=local
SecurityAdmins	group	CN=SCMDMSecurityAdmins (scmdmins),CN=Users,DC=company,DC=local
scmdmins	service connection point	CN=scmdmins,CN=SCMDM,CN=System,DC=company,DC=local

2. Далее последовательно выполняются команды **ADConfig.exe /createTemplates:<имя экземпляра MDM>** и **ADConfig.exe /enableTemplates:<имя экземпляра MDM> /ca:<FQDN-имя центра сертификации>\<имя экземпляра CA>**. Т.е. для «Компании» выполняются **ADConfig.exe /createTemplates:scmdmins** и **ADConfig.exe /enableTemplates:scmdmins /ca:entca.company.local\entca**, где entca.company.local – имя сервера центра сертификации «Компании», entca – имя используемого экземпляра.

В процессе выполнения этих команд создаются и разрешаются к использованию шаблоны сертификатов с именами SCMDMWebServer, SCMDMMobileDevice, SCMDMGCМ. В будущем именно эти шаблоны будут использоваться для выпуска сертификатов для серверов MDM и

устройств, подключаемых к нему. Как и при выполнении предыдущей команды, исполнение этих нужно будет подтвердить вручную.

3. Следующий шаг является опциональным, т.к. при выполнении команды **ADConfig.exe /enableGPSecurity: <имя экземпляра MDM>** вносятся изменения в списки безопасности существующих объектов групповых политик, чтобы MDM мог позволить применять их на мобильные устройства. Если для управления устройствами планируется создавать новые политики, то этот шаг можно пропустить.
4. Последний шаг подготовительного процесса не является обязательным, но очень рекомендуется к выполнению – исполнение команды **ADConfig.exe /ValidateInstance :<имя экземпляра MDM>**. Тут хочу обратить внимание, что:

Выполнение этой команды с неустановленным MDM приводит к предупреждениям о том, что SCMDM не установлен и не найдены некоторые из ключевых параметров;

- В случае, если при выполнении предыдущих шагов были допущены ошибки – администратор тут же должен был получить сообщение о них.
- В общем проводить проверку или нет – это личное дело каждого, но я бы рекомендовал это сделать как минимум для успокоения – все предупреждения прогнозируемы, ничего вне плана не происходит...

На этом этап по подготовке к установке MDM завершается и можно приступать непосредственно к установке MDM. О том, как это происходит, я расскажу в следующей статье.

*Алексей Ватулин*