SCMDM 2008. Часть V. ЧаВО.

Вот и добрался до последней из запланированных статей про SCMDM 2008. Чтобы никого не вводить в заблуждение сразу хочу пояснить – ЧаВО, обозначенное в заголовке, это Часто Возникающие Ошибки, а не Частые Вопросы. Другими словами, в этой части я расскажу об основных проблемах, с которыми столкнулся сам, с которыми сталкивались другие, и о возможном разрешении этих проблем.

Как и с любым другим продуктом при работе с SCMDM наступает момент, когда что-то работает не так, как это предполагалось, либо не работает совсем. Именно с этого момента начинается самое интересное – траблушинг, т.е. поиск причин некорректной работы ПО и их исправление.

Для удобства рассмотрения возможных проблем предлагаю выделить три основных стадии работы с SCMDM, в которые включены действия, достаточно похожие между собой:

1. Установка серверных ролей
2. Подключение клиентских устройств
3. Применение политик и распространение ПО

Для каждой стадии будет правильным использовать свои методы выявления корня проблемы, поэтому каждый вариант будет рассматриваться отдельно.

Проблемы при установке серверных ролей.

Установка серверов SCMDM не является сложной и, если следовать инструкциям, проходит в основном успешно. Однако учитывая достаточно большое количество нюансов, относящихся к предварительной подготовке (т.н. prerequisites), на этом этапе могут возникать проблемы, связанные со следующими моментами:

1. Ошибки при подготовке Active Directory. Как правило, появляются в двух случаях – не до конца удалены следы предыдущих неудачных установок либо нехватка прав у пользователя, выполняющего подготовку. Во втором случае следует удостовериться, что учетная запись входит в группы Enterprise Admins, Schema Admins и Domain Admins.
2. Несоблюдение обязательных требований к предустановленному ПО. Например, учитывая требование к наличию PowerShell, Вы можете задействовать службу WSUS для того, чтобы доставить данный пакет в виде обновления на Windows Server 2003. Однако при установке SCMDM будет получено сообщение о том, что PowerShell не найден и установка будет прекращена. Самое неприятное в данной ситуации, что удалить уже накаченный PowerShell через «Установку и удаление программ» в панели управления не получится – делать это нужно руками, найдя каталог обновления в домашней папке Windows.
3. Несоблюдение требований к доступности сетевых портов на сетевом оборудовании и серверах. Перед началом установки лучше всего удостовериться еще раз, что все нужные SCMDM порты открыты и серверы в состоянии общаться между собой, а также с контроллерами домена, сервером SQL и т.д.

4. Проблемы с выпущенными сертификатами. Данная проблема может привести к тому, что связь между ролями установлена не будет и, например, DM-сервер просто не сможет общаться с Gateway'ем.

Если во время установки Вы столкнулись с проблемами, самым правильным решением будет использование *Best Practice Analyzer*, входящего в состав Resource Kit. Данное приложение позволит Вам провести проверку серверов, на которые вы предполагаете устанавливать SCMDM на соблюдение требований как к аппаратной, так и программной составляющих. Также, используя BPA, можно проверить доступность необходимых портов.

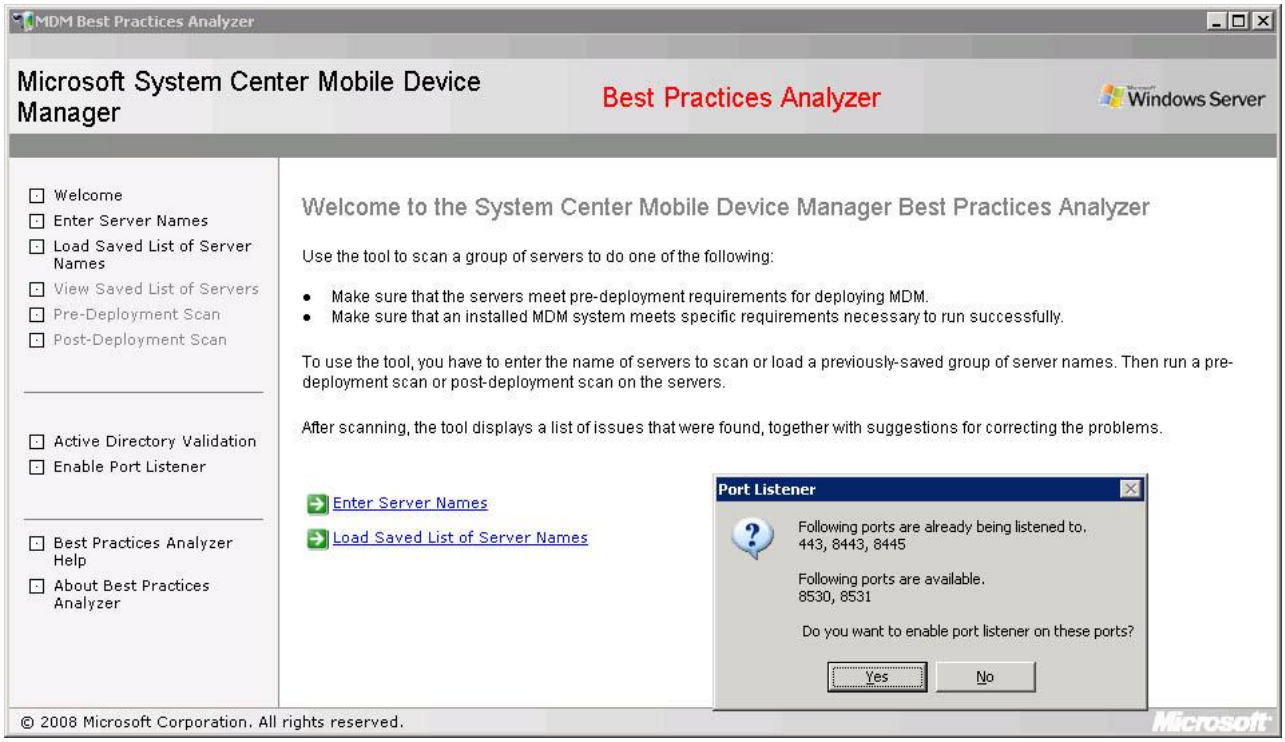

Рис 1. SCMDM Best Practice Analyzer

Для выявления проблем с сертификатами серверов самым правильным будет чтение журналов на всех участвующих серверах.

Проблемы с подключением клиентских устройств.

На этом этапе происходит подключение устройств либо для первичной инициализации, либо для установки рабочего подключения. В случае инициализации устройство подключается к Enrollment-серверу, получает от него первоначальные настройки (напр. информацию о Gateway-сервере), машинный сертификат, а также устанавливается расписание для последующих обновлений политик и установки ПО. К наиболее частым проблемам, возникающим на этапе инициализации устройства, и причинам, их вызывающим (вместе с возможными решениями), можно отнести следующие:

1. Не синхронизировано время на устройстве и Enrollment-сервере – приводит к ошибке во время присоединения устройства к домену. Т.к. служба времени в домене играет очень важную роль, то люфт времени на устройстве может быть не более ±5 минут. Самое логичное решение этой задачи – привести настройки времени и даты в соответствие с доменными.

2. Проблема с разрешением FQDN-имени Enrollment-сервера – это означает, что Вы забыли либо неправильно прописали имя во внешней зоне DNS. Самый простой способ диагностики – *ping* по FQDN. Сами пинги может и не пойдут (в зависимости от настроек), но имя разрешиться должно. Если нет – проверяйте записи во внешней зоне. Так же можно воспользоваться помощью *nslookup*.

3. Проблемы с публикацией порта Enrollment-сервера во внешнюю сеть. В качестве диагностики могу предложить *telnet*, если он не запрещен. Но скорее всего трафик телнета фильтруется, поэтому можно в строке браузера набрать полный адрес с портом, по которым опубликован Enrollment-сервер, и посмотреть на результат. Сообщение о невозможности отобразить страницу будет говорить о проблемах с публикацией, а предупреждение о невозможности проверить сертификат говорит о том, что публикация выполнена успешна и проблема в чем-то еще.

4. Истечение срока действия Pre-enrollment'а. В SCMDM операция по инициализации устройства должна быть проведена за определенный промежуток времени (по умолчанию в течении 24 часов, но интервал может быть изменен). В случае, если устройство не было присоединено к домену за отведенный интервал, то pre-enrollment аннулируется. Проверить, ожидается ли инициализация устройства, можно в консоли управления SCMDM.

5. Невозможность присоединения устройства из-за имени устройства. Если в домен ранее вводилось устройство с таким же именем, а потом была выполнена удаленная очистка устройства, то оно попадает в список заблокированных устройств и ввести аппарат с таким же именем не получиться, пока не будет удалена запись о блокировке. Для этого можно воспользоваться скриптами входящим в состав *MDM Server Tools* из Resource Kit'а (*MDM Blocked Device Cleanup Tool*).

6. Использование «тюнингованных» прошивок на устройствах – зачастую те, кто делают собственные сборки, выбрасывают из них массу того, что считают не очень нужным. Здесь только один совет – используйте оригинальные прошивки, все остальное может оказаться бомбой с часовым механизмом.

Собственно этот список покрывает примерно 70-75% часто возникающих проблем на этапе инициализации. Главной трудностью при проведении диагностики на этом этапе является невозможность использования какого-то унифицированного инструмента. Но для решения некоторых задач, могу порекомендовать утилиту *Windows Mobile IP Utility* от *Enterprise Mobile*, которая позволяет просмотреть настройки для различных сетевых подключений устройства, а также выполнить такие задачи как ping, trace route, измерить скорость подключения с мобильного устройства. Для всего остального рекомендую чтение журналов, документации TechNet и включение логики.

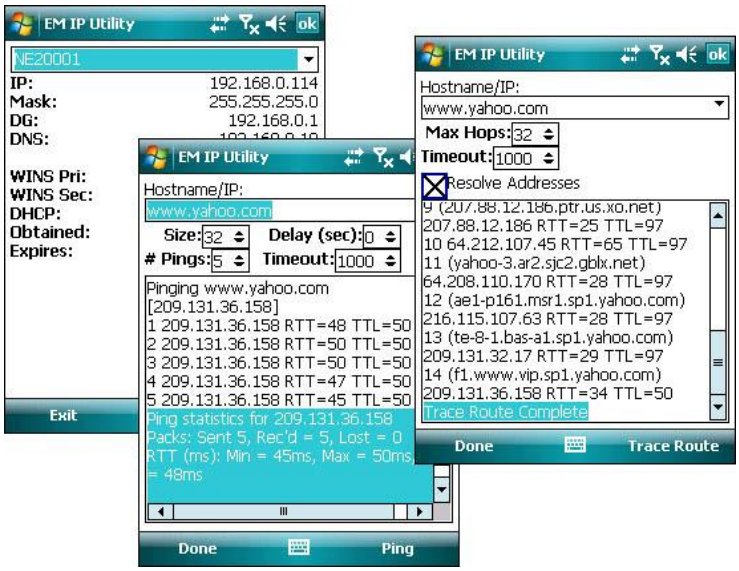

Рис 2. Windows Mobile IP Utility

Следующий этап, на котором могут возникнуть затруднения – это установка рабочего подключения устройства к Gateway-серверу и внутренним службам. При подключении к шлюзу устройство получает IP-адрес из пула, выделенного администратором и настроенного на Gateway'е, после чего может обращаться со службами внутри сети.

Наиболее распространенными ошибками являются:

1. Ошибки при разрешении FQDN Gateway-сервера. Как и в предыдущем пункте возможны варианты, что запись либо не создана, либо создана с ошибкой, поэтому необходимо проверить содержимое соответствующей зоны. Можно, конечно, отдавать устройству не FQDN, а IP-адрес Gateway'я, но лучше этого делать, т.к. адрес может измениться, а запись в DNS поменять гораздо проще, чем изменить настройки на всех аппаратах. Используя инструмент *MDM VPN Diagnostics Tool* можно просмотреть настройки VPN, включая имя Gateway'я, к которому происходит подключение, а также вручную изменить.

2. Закрыты нужные для подключения порты. Выражается это следующим образом – процесс подключения становиться вечным. Для диагностики можно использовать *MDM VPN Diagnostics Tool* из Resource Kit'а. Данный инструмент позволяет провести диагностику по портам (*Port Filtration Tests*).

3. Сотовый оператор не поддерживает трансляцию IPSec. Сам столкнулся с такой проблемой, когда первый раз экспериментировал с «живой» системой. Одна из сложностей была в том, что MDM VPN Diagnostics Tool при запуске Port Filtration Tests показывает, что все порты доступны. Потратил много времени на диагностику, в итоге просто вставил сим-карту другого оператора и все сразу заработало. Оказалось, что не поддерживается трансляция протокола IP 50. Самое неприятное, что пользователь может оказаться в зоне роуминга, где трансляция IPSec не поддерживается, и до тех пор, пока он не подключится к «родной» сети, либо к сети с поддержкой трансляции, устройство не сможет установить связь с Gateway'ем.

4. Не указаны маршруты к сегменту с мобильными устройствами и, как следствие, невозможно получить доступ к ресурсам внутренней сети. Выражается это следующим образом –

устройство в состоянии подключиться к Gateway'ю, но не происходит накатывания политик, невозможно пропинговать внутренние адреса и т.д. Единственно верное решение – прописать маршруты. При диагностике это можно сделать на самом сервере при помощи команды *route add*, а потом централизованно на сетевом оборудовании.

5. Устройство находится в списке заблокированных устройств. Иногда бывает, что администратор при просмотре сведений об устройстве случайно переводит его в состояние заблокированных. При этом оно остается в списке подключенных и узнать о его статусе можно только специально озадачившись его состоянием. Поэтому призываю просматривать и этот список в случае возникновения проблем.

Для диагностики проблем, возникающих при подключении к шлюзу, рекомендую использовать инструменты, входящие в состав Resource Kit. Особенно полезны две клиентских утилиты – MDM VPN Diagnostics Tool, про которую я уже писал, и MDM Connect Now Tool, позволяющую инициировать подключение устройства вне расписания и позволяющую включить журналирование на устройстве.

Проблемы с применение политик и распространением ПО.

При распространении ПО все действия сводятся к правильному выпуску сертификата, которым пакеты будут подписаны, доставке сертификатов на устройства и назначении пакетов на группы. Проблемы с подписывающим сертификатом проявляются сразу при подписывании ПО и для их устранения рекомендую пройти процедуру выпуска без каких-либо отклонений.

При проблемах с доставкой пакетов первое, что необходимо сделать, это проверить, что пакет назначен группе в консоли распространения ПО (MDM software distribution). Если устройство по каким-то причинам оказалось не в той группе, в которой ожидалось, то необходимо проверить групповую политику, отвечающую за целевую группу (Enable client-side targeting). Если все настроено верно, но ПО не доставляется, то необходимо проверить, что устройству назначены все необходимые сертификаты в групповых политиках (Windows Mobile Settings -> Certificates).

При выявлении проблем с установкой ПО можно воспользоваться утилитой MDM Managed Device Status Viewer из Resource Kit, которая позволяет, в том числе, отслеживать проблемы с установкой пакетов.

И последняя категория рассматриваемых проблем – применение политик. Вообще тут все проще всего – если политики не накатываются, то необходимо проверить прописаны ли маршруты, есть ли связь между DM и Gateway серверами, не вносились ли изменения в списки безопасности политики. Единственное, что может поначалу ввести в ступор, это принцип обновления политик. Т.е. представим такую ситуацию – вы создали новую политику, накатили ее на устройства, вам что-то не понравилось, вы внесли изменения и при помощи MDM Connect Now Tool синхронизировали политики на устройстве. А в итоге ничего не изменилось… Суть в том, что для каждого устройства на DM сервере производится калькуляция итоговой политики и она-то и пересылается на устройство. А калькуляция эта происходит с некоторым временным интервалом (по умолчанию 8 часов), и обновление политик произойдет не раньше истечения этого интервала. Поэтому для отладки можно и нужно использовать командлет Update-MobilePolicyCalculation, который позволяет пересчитать итоговую политику раньше.

Заключение

В заключение могу дать несколько советов для упрощения диагностики проблем:

1. Используйте стандартную тактику при создании системы с нуля – сначала все отрабатываете на одном тестовом устройстве, добиваетесь того, что все работает как надо, а потом начинаете ввод устройств пользователей.
2. Активно используйте тот инструментарий, который предлагает Microsoft – BPA, утилиты из Resource Kit.
3. Используйте логический подход при разрешении проблем – что сейчас должно происходить, кто чем должен заниматься и т.д. Понимание процесса очень упрощает диагностику.
4. Читайте официальный раздел Troubleshooting for Mobile Device Manager в библиотеке TechNet.
5. Там же есть очень полезная страница MDM Error and Event Messages.

Надеюсь, что вся серия статей оказалась как минимум познавательной, а может кому-то и помогла либо поможет в будущем. Если у вас есть вопросы по SCMDM – их можно задать мне либо по почте, либо в комментариях. Пишите, а я постараюсь помочь.