Административные шаблоны групповой политики

http://gpo-planet.com/?p=1821

Contents

Введение

Большинство доступных в операционных системах Windows параметров групповой политики, которые зависят от системного реестра, также называемых реестро-зависящими политиками можно найти в расширении административных шаблонов. **Административными шаблонами** называются параметры групповой политики, основанные на данных системного реестра, которые отображаются в узлах **«Административные шаблоны»** узлов конфигурации компьютера и конфигурации пользователя. К таким параметрам относятся настройки панели управления, панели задач, сетевых параметров, параметров рабочего стола и многое другое. Сами по себе административные шаблоны представляют собой текстовые файлы, указывающие на изменение определенных параметров реестра и генерирующие пользовательский интерфейс для настройки политики административного шаблона в оснастке **«Редактор управления групповыми политиками»**, которая и позволяет изменять значение параметров реестра на целевых компьютерах.

В большинстве случаев, административные шаблоны предназначены для простого способа настройки параметров пользователей и компьютеров и применения таких политик для изменения соответствующих настроек пользователей и компьютеров организации. Административные шаблоны предоставляют возможности динамического управления администраторам и разработчиками всевозможными настройками своих приложений. Политики административных шаблонов в узле конфигурации компьютера, модифицируют значения параметров в разделах HKLMSoftwarePolicies и HKLMSoftwareMicrosoftWindowsCurrentVersionPolicies, а административные шаблоны конфигурации пользователя — HKCUSoftwarePolicies и HKCUSoftwareMicrosoftWindowsCurrentVersionPolicies.

Распространяются административные шаблоны групповых политик на клиентские компьютеры таким образом. Сразу после загрузки операционной системы и выполнения пользователем входа в свою учетную запись, загружаются все параметры системного реестра, установленные по умолчанию, а после этого в разделах реестра выполняется анализ некоторых дополнительных параметров и, в том случае, если разделы содержат дополнительные параметры, указаные в политиках административных шаблонов, то существующие записи в реестре будут перезаписываться. Если политики административных шаблонов изменяли параметры реестра в разделах Policies, то в случае удаления административного шаблона или перемещения пользователя в другое подразделение организации, где данный шаблон на него не будет распространяться, информация о существующих параметрах политики будет удалена и после следующей загрузки или выполнения входа, будут использоваться параметры, указанные операционной системой по умолчанию.

В операционных системах Windows, разработанных до Windows Vista и Windows Server 2008, для административных шаблонов использовались файлы, с расширением .adm. У таких административных шаблонов был ряд недостатков. Для создания ADM-файла, который будет использоваться при развертывании конфигурации в многоязыковой организации, вам придется создавать отдельные ADM-файлы для каждого языка. А чтобы отредактировать параметры реестра в таком шаблоне, вам нужно будет вносить изменения в каждый ADM-файл, что крайне неудобно. Ко второму недостатку можно отнести то, что файлы административных шаблонов .adm расположены как компонент объекта **«Шаблон групповой политики»** (Group Policy Template — GPT), которые представляют собой коллекцию файлов в каталоге SYSVOL каждого контроллера домена. И если такой шаблон используется сразу в нескольких объектах GPO, то в папке SYSVOL он будет сохранен несколько раз. Также, при редактировании объекта групповой политики, который содержит ADM-файл, редактор объектов групповой политики загружает этот шаблон из контейнера групповой политики (Group Policy Container — GPC), чтобы создать пользовательский интерфейс. Административные шаблоны ADM не поддерживали такие типы данных реестра, как мультистроковые значения и параметры QWORD.

С выходом операционных систем Windows Vista и Windows Server 2008, административные шаблоны существенно изменились. Теперь административные шаблоны представляют собой пару XML-файлов. А именно: не связанный с языком файл (**ADMX**), описывающий структуру категорий и параметров политики административных шаблонов, отображаемых в оснастке редактора управления групповыми политиками, а также набор зависящих от языка файлов (**ADML**), которые предоставляют локализованные фрагменты, отображаемые в оснастке редактора управления групповыми политиками. Каждый ADML-файл представляет один язык, для которого требуется поддержка. Изменения параметров реестра административных шаблонов вносятся в один ADMX-файл.

К дополнительным преимуществам ADMX/ADML файлов административных шаблонов можно отнести то, что если используются именно эти административные шаблоны, то объект групповой политики содержит только данные, необходимые клиентам обработки групповой политики, а при редактировании объектов GPO редактор управления групповой политикой извлекает файлы ADMX и ADML на локальной машине. В том случае, если компьютеры организации входят в состав домена Active Directory, административные шаблоны располагаются в таком центральном хранилище, как папка SYSVOL, откуда они и загружаются. На компьютерах, которые входят в состав рабочей группы, ADMX файлы располагаются в папке %SystemRoot%PolicyDefinitions, а языковые файлы ADML хранятся в папке %SystemRoot%PolicyDefinitions[MUIculture], где последняя папка должна соответствовать краткой форме языка определенной страны, указанной в ISO-формате. Например, файлы для русского языка локализованы в папке RU-RU. Список сокращений языков вы можете найти в следующей таблице:

Язык	Код в формате ISO-639-1
Африкаанс	AF
Арабский	AR
Баскский	EU
Белорусский	BE
Болгарский	BG
Каталанский	CA
Китайский (Китай)	ZH, ZH-CN
Китайский (Тайвань)	ZH-TW
Хорватский	HR
Чешский	CS

Датский	DA
Нидерландский	NL
Английский (Великобритания)	EN-GB
Английский (США)	EN-US
Эстонский	ET
Фарерский	FO
Финский	FI
Французский	FR, FR-FR
Французский (Канада)	FR-CA
Немецкий	DE
Греческий	EL
Иврит	HE, IW
Венгерский	HU
Исландский	IS
Индонезийский	ID, IN
Итальянский	IT
Японский	JA
Корейский	KO
Латышский	LV
Литовский	LT
Норвежский	NO
Польский	PL
Португальский	PT
Португальский (Бразилия)	PT-BR
Румынский	RO
Русский	RU
Сербский	SP
Словацкий	SK
Словенский	SL
Испанский	ES, ES-ES
Шведский	SV
Тайский	TH
Турецкий	TR
Украинский	UK
Вьетнамский	VI

На контроллерах домена, административные шаблоны располагаются в центральном хранилище, которое также называется контейнером групповых политик и содержит атрибуты, используемые для распространения GPO в домене, подразделениях и сайтах, а именно в папке %SystemRoot%sysvol%domainname%policiesPolicyDefinitions. В свою очередь, языковые файлы ADML хранятся в папке %SystemRoot%sysvol%domainname%policiesPolicyDefinitions[MUIculture], соответственно. Для того чтобы создать центральное хранилище, вам нужно на контроллере домена создать корневую папку внутри %SystemRoot%sysvol%domainname%policiesPolicyDefinitions, после этого создать папки для

каждого языка, который необходим для распространения групповых политик. На следующем шаге следует скопировать все ADMX и ADML файлы с административной рабочей машины в папку PolicyDefinitions. Это можно сделать или вручную, или используя следующую команду:

```
Copy %systemroot%PolicyDefinitions*
%logonserver%sysvol%userdomain%policiesPolicyDefinitions
```

После настройки центрального хранилища, редактор управления групповой политикой распознает его и загружает все административные шаблоны не из локального хранилища, а именно из указанного вами центрального хранилища.

На следующей иллюстрации вы можете увидеть папку PolicyDefinitions клиентского компьютера с операционной системой Windows 7:

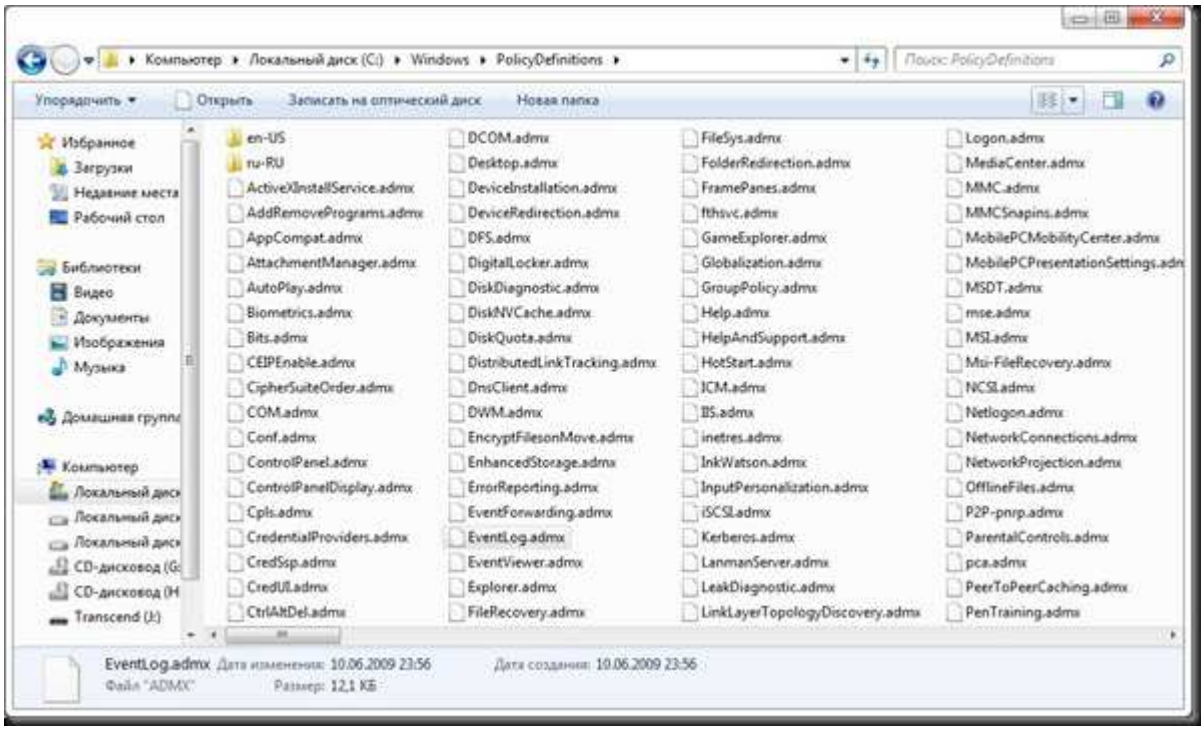

Рис. 1. Папка PolicyDefinitions на клиентском компьютере

Также, в связи с тем, что теперь административные шаблоны поддерживают мультистроковые типы данных реестра, администраторы могут выполнять такие задачи, как:

- вывод нескольких строк текста и сортировки записей параметров политики;
- редактирование настроенных параметров и добавление новых позиций в строки;
- редактирование существующего параметра;
- выполнение выборки одной или нескольких записей;
- удаление выбранных записей.

Поддержка типа значений реестра QWORD позволяет использовать параметры политики административных шаблонов для 64-разрядных приложений. Помимо этого, стоит обратить ваше внимание и на тот факт, что в операционных системах Windows Server 2008 R2 и Windows 7 насчитывается около 3200 административных шаблонов, что почти в два раза больше, чем было в операционной системе Windows XP с административными шаблонами ADM (их тогда было около 1400).

Как я уже упомянул в начале этой статьи, управлять административными шаблонами вы можете при помощи оснастки **«Редактор управления групповой политикой»**. Во время редактирования объекта групповой политики, оснастка операционной системы Windows Server 2008/2008 R2

считывает все ADMX файлы, о расположении которых я говорил немного ранее, а затем отображает, согласно ADMX-файлам категории и параметры в узле **ПолитикиАдминистративные шаблоны** в разделах **«Конфигурация компьютера»** и **«Конфигурация пользователя»**. В параметрах политик административных шаблонов всегда можно найти три следующие опции: **«Включить»**, **«Отключить»** и **«Не задано»**, которые изменяют параметр реестра для внесения изменений, отвечающих контексту параметра политики, изменение, выполняющее обратное действие, а также опция, позволяющая оставить параметры реестра без изменений. Значение по умолчанию для каждого параметра политики «Не задано». Опять же, я уже упоминал, что начиная с операционных систем Windows Vista и Windows Server 2008, для редактора объектов групповой политики больше не используются ADM-файлы. Но, несмотря на это, если вам необходимо управлять настройками предыдущих операционных систем, вы можете добавить ADM-файлы.

Далее в этой статье вы узнаете об архитектуре и синтаксисе административных шаблонов.

Архитектура административных шаблонов

Если разобраться, то архитектура административных шаблонов групповых политик не такая уж и сложная. Основными компонентами в распространении административных шаблонов являются системный администратор, контроллер домена и целевой клиентский компьютер. Небольшая схема, которая позволит вам иметь четкое представление архитектуры расширения административных шаблонов, отображена ниже:

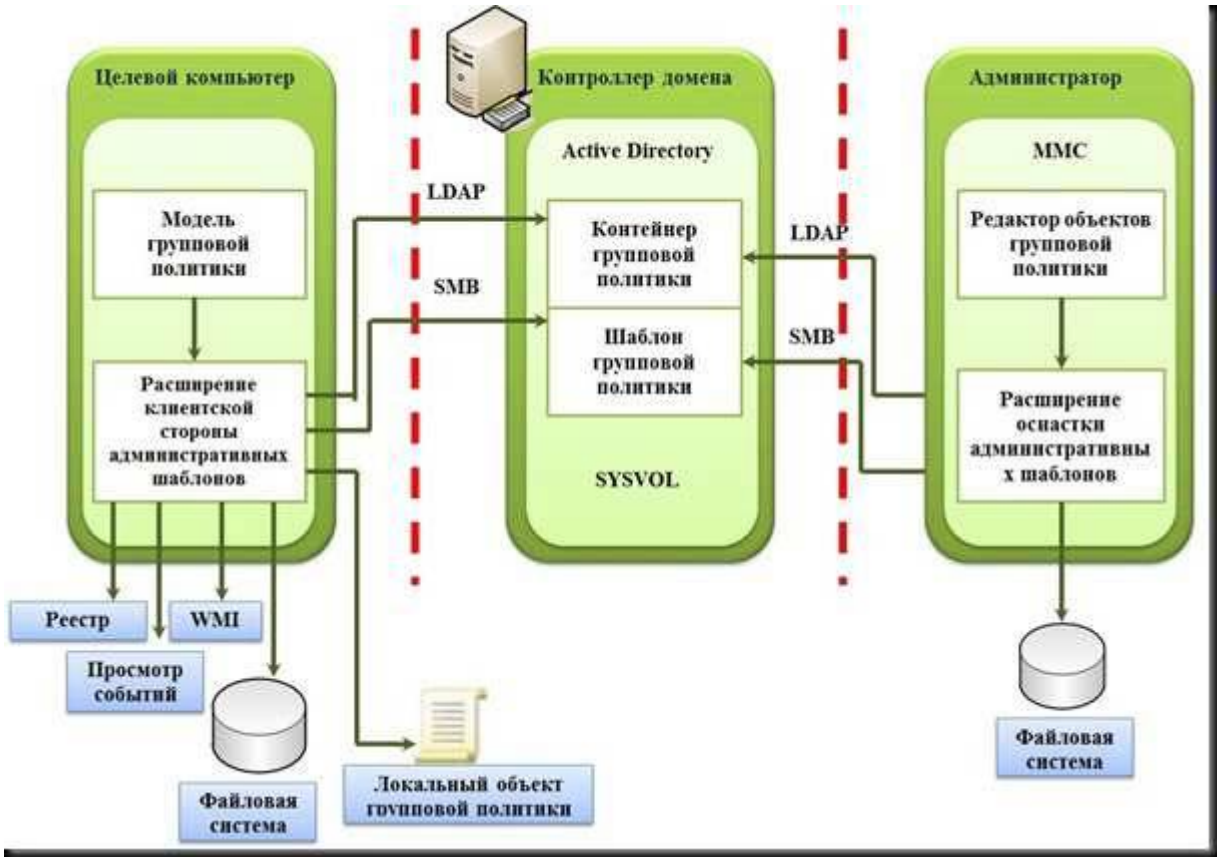

Рис. 2. Архитектура расширения административных шаблонов

Первое, что стоит рассматривать в архитектуре расширения административных шаблонов групповых политик, это работу, выполняемую системным администратором, которая в данной схеме отображена в самом правом блоке. Здесь под компонентом **«Администратор»** подразумевается компьютер, на котором системный администратор вносит изменения в административные шаблоны, используя оснастку **«Редактор управления групповыми политиками»**. В этой оснастке, в расширении серверной стороны администратор настраивает

параметры политик, основанные на административных шаблонах. Оснастка располагается в библиотеке userenv.dll, которую можно найти в папке WindowsSystem32. Настройки расширения административных шаблонов передаются в Active Directory на контроллер домена по протоколам LDAP и SMB. Протокол SMB (Server Message Block) считается основным методом, предназначенным для доступа к файлам и принтерам. Именно этот протокол используют административные шаблоны для доступа к папке SYSVOL, а также для резервного копирования и извлечения файлов удаленной файловой системы.

В средней части данной схемы расположен контроллер домена, который является связующим звеном между изменениями, внесенными в административные шаблоны системным администратором и целевым компьютером, который будет извлекать настройки параметров объектов групповой политики. Всем известно, что контроллером домена называется отдельный сервер, который играет роль доменных служб Active Directory и имеет права на запись в базу данных Active Directory, запускать службу центра распространения ключей Kerberos, контролировать доступ к сетевым ресурсам и выполнять много других задач. В этом случае, как видно на схеме, контроллер домена содержит **контейнер групповой политики**, который хранит информацию о настройках объектов групповых политик в Active Directory, а также **шаблон групповых политик**, который хранит данные объекта GPO в папке Sysvol.

Как и компьютер системного администратора, с контроллером домена по протоколам LDAP и SMB связывается целевой компьютер, на который и распространяются параметры политики измененного системным администратором объекта GPO. Прежде всего, на каждом целевом компьютере есть модуль групповых политик, вызывающий клиентское расширение административных шаблонов с полным перечнем всех объектов групповых политик, которые будут применяться на данную машину. Модель групповых политик вызывает расширение клиентской стороны административных шаблонов, реализованное в библиотеке userenv.dll, зарегистрированной в разделе HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindows NTCurrentVersionWinlogonGPExtensions, которое отвечает за внесение изменений в системный реестр операционной системы, согласно параметрам политики административных шаблонов, которые настраиваются при помощи соответствующей оснастки. Для выполнения настроек, указанных в параметрах групповой политики, расширение административных шаблонов изменяет конкретные параметры системного реестра. Изменяемые параметры указываются непосредственно в ADMX файле. Изменения, внесенные в системный реестр при помощи модуля групповых политик, записываются в журналы событий, которые можно просмотреть при помощи оснастки **«Просмотр событий»**. Во время обработки групповой политики, расширение клиентской стороны административных шаблонов записывает информацию об обработке данных в пространстве имен RSoP инструментария управления Windows.

Помимо выполнения объектов групповых политик, на каждом компьютере можно индивидуально настроить административные шаблоны в локальных объектах групповой политики. Эти объекты будут локально располагаться в скрытой папке %systemroot%System32GroupPolicy и, как всем вам известно, в среде Active Directory считаться наименее приоритетными, так как все объекты GPO, распространяемые на подразделение Active Directory, в котором расположен сам пользователь или его компьютер имеют более высокий приоритет.

Структура ADMX-файла (Файла, не зависящего от языка)

В ADMX-файле указано количество параметров политики и их тип данных, а также расположения в категориях, находящихся в оснастке **«Редактор управления групповыми политиками»**. ADMX-файл состоит из семи разделов, которые вы можете увидеть на следующей иллюстрации:

Рис. 2. Структура ADMX-файла

- XML-объявление. XML-объявлением является заголовок файла, который не рассматривается в качестве фрагмента ADMX-документа, но является его необходимой частью и помещается в начале всего файла для того, чтобы указать на то, что это XML-документ. Синтаксис следующий:

```
<?xml version="<placeholder for version number>" encoding="<placeholder for character
encoding"?>
```

где доступны два параметра:

- **Version**. Представляет собой версию языка XML, используемую в документе;
- **Encoding**. Предоставляет сведения о кодировке, используемые средствами синтаксического анализа XML-документов (в ADMX-файлах всегда должна быть задана кодировка UTF-8).

- **Элемент policyDefinitions**. Является элементом документа для ADMX-файла, который определяет набор параметров политики системного реестра. Данный элемент содержит все остальные элементы для ADMX-файла. Синтаксис этого элемента следующий:

```
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
revision="<MajorVerison.MinorVersion>" schemaVersion="<MajorVerison.MinorVersion>"
xmlns=" http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions" >
  <policyNamespaces> ... </policyNamespaces>
  <supersededAdm> ... </supersededAdm>
  <resources> ... </resources>
  <supportedOn> ... </supportedOn>
  <categories> ... </categories>
```

```
<policies> ... </policies>
    </policyDefinitions>
```

где присутствуют следующие основные и дополнительные параметры:

- **Xmlns:xsd и xmlns:xsi**. Это основные элементы, которые обозначают элементы и типы данных, используемые в схеме из пространства имен (параметр xmlns:xsd), а также обозначают пространства имен экземпляра XML-схемы, предоставленной в самом пространстве имен. Эти оба параметра всегда должны входить в состав ADMX-файла, так как, в противном случае, он может не пройти проверку на правильность формата XML-файла, они должны вводиться следующим образом:xmlns:xsd =»http://www.w3.org/2001/XMLSchema» и xmlns:xsi=»http://www.w3.org/2001/XMLSchema-instance»
- **Revision**. В этом параметре указывается версия ADMX-файла, которая в большинстве случаев предназначена для отслеживания внесенных изменений. Синтаксис этого параметра имеет следующий вид:revision=»<MajorVersion.MinorVersion>»где MajorVersion и MinorVersion являются номерами версии, и имеют формат XXXX, где X обозначает одиночную десятичную цифру, например **revision=»1.1”** или **revision=»1234.5678”**. Параметр является обязательным.
- **schemaVersion**. Данный параметр очень похож на revision, но его основное отличие в том, что при помощи него указывается версия схемы, используемая средствами работы с групповыми политиками для определения того, поддерживается ли ими формат конкретных ADMX-файлов. Синтаксис этой команды идентичен синтаксису revision. Обычно, данный параметр указывается следующим образом: **schemaVersion=»1.0”**. Параметр является обязательным.
- **policyNamespaces**. Этот элемент определяет уникальное пространство имен для данного ADMX-файла. Более подробно данный элемент будет рассмотрен ниже.
- **supersededAdm**. Данный элемент ссылается на имя ADM-файла, заменяемого ADMX-файлом. В этом случае, редактор управления групповой политикой не будет считывать любые ADM-файлы, обозначенные как заменяемые. Синтаксис данного элемента довольно простой:

  ```
  <supersededAdm fileName="<placeholder for ADM file name>" />
  ```

  где в параметре fileName должно быть указано имя ADM-файла, заменяемого ADMX-файлом. Например, <supersededAdm fileName=»oldadm.adm» />.

- **Resources**. Текущий элемент определяет требования для ресурсов определенного языка и минимальную необходимую версию связанного ADML-файла. Этот элемент более подробно будет рассмотрен ниже.
- **supportedOn**. Элемент, определяющий сопоставление ссылки на локализированные строки текста с операционными системами или приложениями, на которые влияют конкретные параметры политики. Более подробно будет рассмотрен ниже.
- **Categories**. Данный элемент содержит список категорий, в которых параметр политики текущего ADMX-файла будет отображаться в оснастке редактора управления групповыми политиками. Более подробно будет рассмотрено ниже.
- **Policies**. В этом элементе размещен список определений параметров политики. Также более подробно будет рассмотрен немного ниже.

- **Элемент policyNamespaces**. Как было указано выше, данный элемент определяет уникальное пространство имен для текущего ADMX-файла. Помимо этого, данный элемент обеспечивает сопоставление с пространствами имен во внешних файлах, то есть, в том случае, если ADMX-файл ссылается на элементы **category**, определенные в другом ADMX-файле. Синтаксис у этого элемента следующий:

```
<policyNamespaces>
  <target> ... </target>
  <using> ... </using>
      </policyNamespaces>
```

где:

- **target**. Текущий параметр определяет уникальное имя пространства имен политики в ADMX-файле;
- **using**. Этот параметр указывает ссылку на существующую категорию из другого элемента **policyNamespaces**;

- **Элемент resources**. Элемент ADMX-файла позволяет задавать минимальный уровень версии ADML-файла, а также позволяет указывать базовый язык. Текущий элемент включает в себя два вложенных атрибута, синтаксис которых можно увидеть ниже:

```
<resources minRequiredRevision="<MajorVersion.MinorVersion>"
fallbackCulture="<placeholder for culture/language name>"/>
```

где:

- **minRequiredRevision**. Атрибут позволяет указать минимальный уровень версии ADML-файла;
- **fallbackCulture**. При помощи текущего атрибута вы можете указать язык, который будет использоваться по умолчанию, если ни в одном расположении не будет найден соответствующий ADML-файл. Если вы не укажите текущий атрибут, то по умолчанию будет использоваться английский язык;

- **Элемент supportedOn**. Данный элемент является опциональным элементом в структуре ADMX-файла, то есть включать его не обязательно. При помощи элемента supportedOn вы можете обеспечить сопоставление продуктов с их определениями, то есть, вы можете указать в каких версиях операционных систем или программных продуктов запрещается помечать параметры групповой политики как устаревшие в случае, если параметр больше не применяется к текущей версии. С этим элементом не связан ни один атрибут, но вы можете использовать дочерний элемент definitions, который является элементом, определяющим набор параметров политики реестра. Синтаксис данного элемента следующий:

```
<supportedOn>
  <definitions> ... </definitions>
      </supportedOn>
```

В следующей таблице указаны значения данного атрибута, определяющие операционные системы, на которые будет распространяться созданный вами параметр административного шаблона:

Значение SupportOn	Описание значения
SUPPORTED_AllowWebPrinting	Windows 2000 или более поздние операционные системой, с поддержкой служб IIS, но не поддерживается Windows Server 2003
SUPPORTED_IE6SP1	Не ниже Internet Explorer 6.0
SUPPORTED_Win2k	Не ниже Windows 2000
SUPPORTED_Win2kOnly	Только Windows 2000
SUPPORTED_Win2kSP1	Не ниже Windows 2000 SP1

SUPPORTED_Win2kSP3	Не ниже Windows 2000 SP3
SUPPORTED_Win2kSP3_Or_XPSP1	Не ниже Windows 2000 SP3 или Windows XP SP1
SUPPORTED_WindowsNET	Не ниже Windows Server 2003
SUPPORTED_WindowsNETOnly	Только Windows 2003
SUPPORTED_WindowsNET_XP	Только Windows 2003 и Windows XP
SUPPORTED_WindowsPreVista	Только Windows Server 2003, Windows XP или Windows 2000
SUPPORTED_WindowsUpdate	Не ниже Windows 2000 SP3, Windows XP SP1 или семейства Windows Server 2003
SUPPORTED_WindowsVista	Не ниже Windows Vista
SUPPORTED_WindowsXP	Не ниже Windows XP или семейства Windows Server 2003
SUPPORTED_WindowsXP_Or_Vista	Не ниже Windows XP или Windows Vista
SUPPORTED_WindowsXP_SP1_W2K_SP4_NETSERVER	Не ниже Windows 2000 SP4, Windows XP SP1 или семейства Windows Server 2003
SUPPORTED_WindowsXP_SP2_W2K_SP5_NETSERVER_SP1	Не ниже Windows 2000 SP5, Windows XP SP2 или семейства Windows Server 2003 SP1
SUPPORTED_WindowsXPOnly	Только Windows XP
SUPPORTED_WindowsXPSP1	Не ниже Windows XP SP1 или семейства Windows Server 2003
SUPPORTED_WindowsXPSP2	Не ниже Windows XP SP2
SUPPORTED_WindowsXPSP2_Or_WindowsNET	Не ниже Windows XP SP2 или семейства Windows Server 2003
SUPPORTED_WindowsXPSP2_Or_WindowsNETSP1	Не ниже Windows XP SP2 или семейства Windows Server 2003 SP1
SUPPORTED_WindowsXPOrServerOnly	Только Windows XP или Windows Server 2003
SUPPORTED_Windows7	Не ниже Windows 7

- **Элемент categories**. Используя этот элемент, вы можете указать таблицу элементов category, позволяющих задавать имя уникальной категории, которая будет отображаться в окне редактора объектов групповой политики. Этот элемент целесообразно использовать только в том случае, если элементы category указываются в ADML-файле. Элемент categories опасен тем, что из-за него вы случайно можете указать циклические ссылки, ссылаясь на элементы category других ADMX-файлов. Элемент category включает в себя следующий синтаксис:

```
<categories>
    <category ... </category>
      </categories>
```

- **Элемент policies**. Текущий элемент позволяет вам указать таблицу элементов policy, представляющих собой одиночный параметр групповой политики. Синтаксис этого элемента следующий:

```
<policies>
    <policy> ... </policy>
```

```
</policies>
```

Структура ADML-файла (файла языковых ресурсов)

Как я уже говорил во введении этой статьи, в файлах ADML указываются языковые ресурсы, привязывающиеся к определенному языку, без которых ADMX-файл не будет корректно работать. Основная задача этого файла – обеспечение корректного отображения описания параметра политики, который можно будет найти в оснастке редактора управления групповыми политиками. Структура этого файла намного проще структуры ADMX-файла и ее вы можете увидеть на следующей иллюстрации:

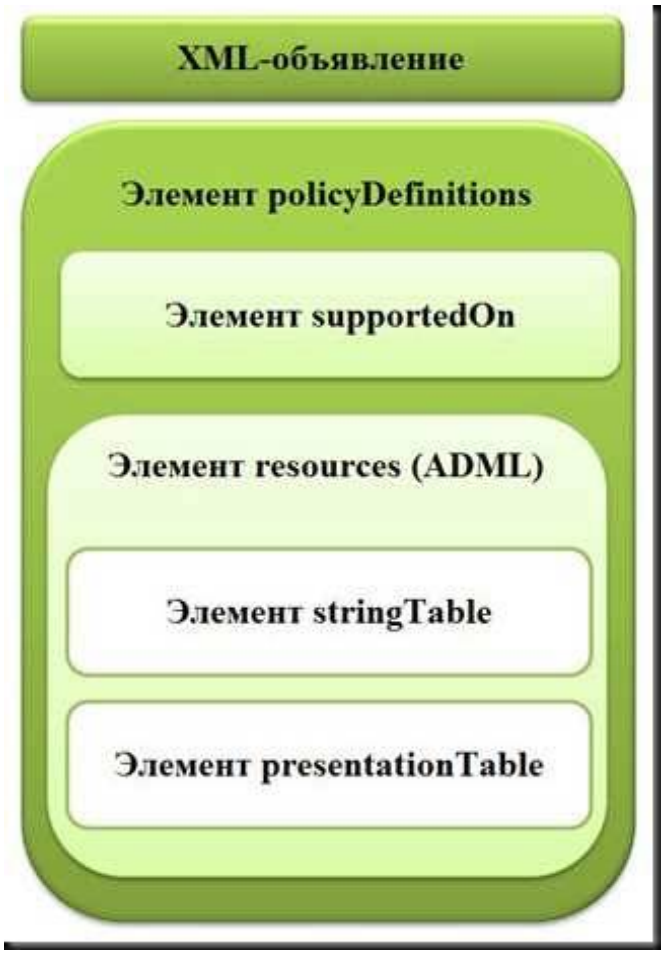

Рис. 3. Структура ADML-файла

- **XML-объявление**. Так же как и в случае с файлом ADMX, в этом файле XML-объявлением является заголовок файла, который не рассматривается в качестве фрагмента ADML-документа, но является его необходимой составляющей и помещается в начале всего файла для того, чтобы указать на то, что это XML-документ. О данном элементе вы можете прочитать в предыдущем разделе данной статьи;
- **Элемент PolicyDefinitionResources**. Этот элемент определяет сведения всех локализованных ресурсов с одним языком или набором региональных параметров в файле для каждого поддерживаемого языка или набора региональных параметров и содержит объявление пространства имен по умолчанию для всех элементов ADML-файла. Этот элемент включает в себя пять атрибутов: xmlns:xsd, xmlns:xsi, revision, schemaVersion и xmlns. Обо всех этих элементах уже говорилось ранее. Помимо этого, данный элемент содержит до четырех возможных дочерних элементов, которые вкратце описаны далее:
    - **Элемент displayName**, в котором указывается локализованное и понятное имя ADML-файла;

- **Элемент description**, позволяющий указать описание параметров политики, которые включены в соответствующий файл;
- **Элемент annotation**, в котором указывается локализованный комментарий;
- **Элемент resources**, считающийся родительским элементом для элементов stringTable и presentationTable, о которых речь пойдет немного ниже.

Синтаксис данного элемента следующий:

```
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
revision="<MajorVerison.MinorVersion>"
schemaVersion="<MajorVerison.MinorVersion>" xmlns=
"http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions" >
  <displayName> ... </displayName>
  <description> ... </description>
  <annotation> ... </annotation>
  <resources> ... </resources>
</policyDefinitionResources>
```

- **Элемент stringTable**. Используя этот элемент ADML-файла, вы можете указать сам заголовок параметра групповой политики, текст с описанием, текст со ссылкой на поддержку, названия категорий, а также подписи для параметров. Стоит обратить внимание на то, что элемент **stringTable**нельзя объявлять более одного раза. Данный элемент включает в себя вложенные элементы string, позволяющие определить все указанные выше данные. Синтаксис данного элемента следующий:

```
<stringTable>
    <string> ... </string>
      </stringTable>
```

- **Элемент presentationTable**. Последний элемент представляет собой целую структуру дочерних элементов управления параметрами отдельных параметров групповой политики, включая в себя всевозможные флажки, переключатели, подписи, подсказки и прочее. Дочерними элементами являются элементы **presentation**, которые представляют собой отображаемые сведения параметров для параметров политики. Синтаксис для этого элемента имеет следующий вид:

```
<presentationTable>
    <presentation> ... </presentation>
      </presentationTable>
```

Создание своего административного шаблона

На первый взгляд все эти XML файлы со множеством родительских и дочерних элементов могут показаться очень сложными при создании своего собственного административного шаблона. Чтобы соответствующий материал вам было проще усвоить, в этом разделе я покажу, как можно создать свои ADMX и ADML файлы, предназначенные для управления двумя параметрами антивирусного программного обеспечения Microsoft Security Essentials. Сразу хотелось бы обратить ваше внимание на то, что данный антивирусный продукт можно использовать в SOHO компаниях, то есть там, где развертывается не более 10 компьютеров. Мы рассмотрим только три параметра, которые позволяют вам указывать тип проверки, а также ее периодичность. Для начала, перед созданием ADMX-файла, вам нужно узнать какие именно параметры в каких разделах системного реестра должны изменяться. При помощи программы ProcessMonitor от Марка Руссиновича или программы RegMon можно быстро отследить изменения в реестре и узнать, что при изменении опций в самом Microsoft Security Essentials, меняются следующие параметра реестра:

1. Для того чтобы выполнять запланированную проверку, только когда компьютер включен, но не используется, в системный реестр вносятся следующие изменения:

```
[HKEY_LOCAL_MACHINESoftwareMicrosoftMicrosoft AntimalwareScan]
“ScanOnlyIfIdle”=dword:00000001
;Опция включена
“ScanOnlyIfIdle”=dword:00000000
;Опция отключена
```

- Для того чтобы ограничить использование ЦПУ при проверке, в реестре изменяется значение следующего параметра:

```
[HKEY_LOCAL_MACHINESoftwareMicrosoftMicrosoft AntimalwareScan]
“AvgCPULoadFactor”=dword:00000000
;Опция отключена
“AvgCPULoadFactor”=dword:0000000a
;10%
“AvgCPULoadFactor”=dword:00000014
;20%
“AvgCPULoadFactor”=dword:0000001e
;30%
“AvgCPULoadFactor”=dword:00000028
;40%
“AvgCPULoadFactor”=dword:00000032
;50%
“AvgCPULoadFactor”=dword:0000003c
;60%
“AvgCPULoadFactor”=dword:00000046
;70%
“AvgCPULoadFactor”=dword:00000050
;80%
“AvgCPULoadFactor”=dword:0000005a
;90%
“AvgCPULoadFactor”=dword:00000064
      ;100%
```

После того как вы узнали нужные параметры и значения реестра, можно приступать к созданию ADMX-файла.

Первым делом в ADMX-файле вам нужно указать XML-объявление и элемент policyDefinitions. Практически во всех случаях эти строки создаваемого вами XML-файла одинаковые. У вас они должны получиться примерно следующими:

```
<?xml version="1.0" encoding="utf-8"?>
<!--  Dmitry Bulanov, 2011 (c)  -->
<policyDefinitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
schemaVersion="1.0"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions">
```

После этого необходимо заполнить элемент policyNamespaces, где нужно будет указать уникальное имя пространства имен, а также ссылку на существующую категорию из другого элемента policyNamespaces. Так как создается ADMX-файл для Microsoft Security Essentials, укажем префикс mse и назовем пространство имен Microsoft.Policies.MicrosoftSecurityEssentials, а также элемент resources, где зададим минимальный уровень версии ADML-файла 1.0, как показано ниже:

```
  <policyNamespaces>
    <target prefix="mse" namespace="Microsoft.Policies.MicrosoftSecurityEssentials "
/>
    <using prefix="windows" namespace="Microsoft.Policies.Windows" />
  </policyNamespaces>
  <supersededAdm fileName="mse" />
```

```
  <resources minRequiredRevision="1.0" />
```

Так как элемент supportedOn является опциональным элементом, в нашем случае мы опустим использование этого элемента. Поскольку для нашей группы административных шаблонов нужно указать группу, в которой будут расположены административные шаблоны антивирусного программного обеспечения, нужно добавить элемент categories, как показано в следующем листинге:

```
  <categories>
    <category name="MicrosoftSecurityEssentials"
displayName="$(string.MicrosoftSecurityEssentials)"
explainText="$(string.MicrosoftSecurityEssentials_Help)">
    </category>
  </categories>
```

Вот мы и дошли до самого интересного момента, когда нужно добавлять разделы и параметры системного реестра, которые будут использоваться как основа параметров групповых политик. На этом шаге стоит обратить внимание на то что, так как параметры реестра для Microsoft Security Essentials расположены только в разделе HKLM, в классе политики необходимо указать **Machine**. Эти параметры можно увидеть в следующем листинге, причем, что самое интересное, в данном листинге вы можете найти как переключатели, так и раскрывающиеся меню:

```
<policies>
    <policy name="SchedScanCheck" class="Machine"
displayName="$(string.SchedScanCheck)" explainText="$(string.SchedScanCheck_Help)"
key="SoftwareMicrosoftMicrosoft AntimalwareScan" valueName="ScanOnlyIfIdle">
      <parentCategory ref="MicrosoftSecurityEssentials" />
      <supportedOn ref="windows:SUPPORTED_WindowsXPSP2" />
          <enabledValue>
        <decimal value="1" />
      </enabledValue>
      <disabledValue>
        <decimal value="0" />
      </disabledValue>
    </policy>
    <policy name="ScanSch" class="Machine" displayName="$(string.LimitCPUUsage)"
explainText="$(string.LimitCPUUsage_Help)"
presentation="$(presentation.LimitCPUUsage)" key="SoftwareMicrosoftMicrosoft
AntimalwareScan">
      <parentCategory ref="MicrosoftSecurityEssentials" />
          <supportedOn ref="windows:SUPPORTED_WindowsXPSP2" />
          <elements>
        <enum id="LimitCPUUsageMode" valueName="AvgCPULoadFactor" required="true">
          <item displayName="$(string.10perc)">
            <value>
              <decimal value="10" />
            </value>
          </item>
          <item displayName="$(string.20perc)">
            <value>
              <decimal value="20" />
            </value>
          </item>
          <item displayName="$(string.30perc)">
            <value>
              <decimal value="30" />
            </value>
          </item>
          <item displayName="$(string.40perc)">
            <value>
              <decimal value="40" />
            </value>
          </item>
          <item displayName="$(string.50perc)">
            <value>
```

```
            <decimal value="50" />
          </value>
        </item>
        <item displayName="$(string.60perc)">
          <value>
            <decimal value="60" />
          </value>
        </item>
        <item displayName="$(string.70perc)">
          <value>
            <decimal value="70" />
          </value>
        </item>
        <item displayName="$(string.80perc)">
          <value>
            <decimal value="7" />
          </value>
        </item>
               <item displayName="$(string.90perc)">
          <value>
            <decimal value="90" />
          </value>
        </item>
               <item displayName="$(string.100perc)">
          <value>
            <decimal value="100" />
          </value>
        </item>
      </enum>
    </elements>
  </policy>
 </policies>
</policyDefinitions>
```

После того как ADMX-файл будет окончательно завершен, вам еще предстоит написать сам ADML-файл. Как вы уже знаете, структура этого файла намного проще. В этом файле следует оставить XML-объявление и элемент policyDefinitions такими же, как вы указывали в самом ADMX-файле. Обязательно обратить внимание на то, что весь текст в этом файле должен быть в кодировке UTF-8. В элементах displayName и description укажем, что данный административный шаблон создается для антивирусного программного обеспечения Microsoft Security Essentials. В элементе stringTable следует указать идентификаторы и описания для каждого уникального объекта, который был создан в ADMX-файле.

Наверное, самой сложной частью ADML-файла считается определение структуры элементов управления отдельных параметров групповой политики в элементе **presentationTable**. Так как в нашем случае только в одном параметре политики есть раскрывающиеся списки, необходимо указать дочерние элементы **dropdownList** с идентификаторами и описанием данных элементов управления. В итоге должен получиться следующий XML-файл:

```
<?xml version="1.0" encoding="utf-8"?>
<!--  Dmitry Bulanov, 2011 (c)  -->
<policyDefinitionResources xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" revision="1.0"
schemaVersion="1.0"
xmlns="http://schemas.microsoft.com/GroupPolicy/2006/07/PolicyDefinitions">
  <displayName>Microsoft Security Essentials</displayName>
  <description>Microsoft Security Essentials</description>
   <resources>
    <stringTable>
      <string id="MicrosoftSecurityEssentials">Политики Microsoft Security
Essentials</string>
          <string id="MicrosoftSecurityEssentials_Help">Настройка различных
параметров антивирусного программного обееспечения Microsoft Security
Essentials</string>
```

```
          <string id="SchedScanCheck">Выполнять запланированную проверку, только
когда компьютер включен, но не используется</string>
          <string id="SchedScanCheck_Help">Этот параметр позволяет выполнять
запланированную проверку только в том случае, когда вы не пользуетесь компьютером.
```
При выборе параметра "Включить" будет включена данная опция.
```
          Если вы выберите опцию "Отключить", то проверка будет выполняться в строго
отведенное вами время</string>
          <string id="ScanSchDayMode">Настройка периодичности сканирования Microsoft
Security Essentials</string>
          <string id="LimitCPUUsage">Ограничить использование ЦПУ при
проверке</string>
          <string id="LimitCPUUsage_Help">При помощи текущего параметра групповой
политики вы можете ограничить использование ЦПУ при проверке. Значение по умолчнаию -
50%</string>
          <string id="10perc">10%</string>
          <string id="20perc">20%</string>
          <string id="30perc">30%</string>
          <string id="40perc">40%</string>
          <string id="50perc">50%</string>
          <string id="60perc">60%</string>
          <string id="70perc">70%</string>
          <string id="80perc">80%</string>
          <string id="90perc">90%</string>
          <string id="100perc">100%</string>
    </stringTable>
    <presentationTable>
      <presentation id="LimitCPUUsage">
            <text>Укажите лимит использования ЦПУ в процентах</text>
            <dropdownList refId="LimitCPUUsageMode" defaultItem="0">Ограничить
использование ЦПУ до: </dropdownList>
      </presentation>
    </presentationTable>
  </resources>
</policyDefinitionResources>
```

После того как вы поместите созданные файлы в папку Policy Definitions на локальном компьютере или в папку SYSVOL на контроллере домена, данные политики будут отображаться в оснастке редактора управления групповыми политиками.

Заключение

Из этой статье вы узнали о параметрах групповой политики, основанных на данных системного реестра, которые называются административными шаблонами. Вкратце была рассмотрена история развития административных шаблонов, структура ADMX-файла – файла, не зависящего от языка, структура ADML-файла – файла языковых ресурсов. Также, в данной статье был написан административный шаблон для управления антивирусным программным обеспечением – Microsoft Security Essentials.

Комментарии

Применительно обновлений ADML/ADMX до уровня Windows 8.1/Windows Server 2012 R2

здесь: http://blog.it-kb.ru/2013/10/22/update-admx-adml-gpo-templates-upgrade-domain-policies-policy-definitions-for-windows-8-1-and-windows-server-2012-r2/

Если у вас пропали из оснастки сами параметры политик административных шаблонов

Смотрите, если у вас пропали из оснастки сами параметры политик административных шаблонов, скорее всего, они подтерлись физически. То есть, скопируйте стандартный набор параметров политик в соответствующее расположение.
Если политики хранятся локально, их расположение должно быть: %SystemRoot%\PolicyDefinitions
Если же они «живут» в центральном хранилище — \\контроллер_домена\sysvol\%userdomain%\policies\PolicyDefinitions
Ну а сами файлы можно взять отсюда: http://www.microsoft.com/en-us/download/details.aspx?id=41193