В помощь системным и сетевым администраторам

2-е издание

Основы SNMP

СИМВОЛ®
O'REILLY®

Дуглас Мауро и Кевин Шмидт

16 лет вместе
с профессионалами

Essential SNMP

Second Edition

Douglas Mauro and Kevin Schmidt

O'REILLY®

Основы SNMP

Второе издание

Дуглас Мауро и Кевин Шмидт

Символ®

Санкт-Петербург — Москва
2012

Дуглас Мауро, Кевин Шмидт

Основы SNMP, 2-е издание

Перевод Р. Багаутдинова

Главный редактор	*А. Галунов*
Зав. редакцией	*Н. Макарова*
Научный редактор	*Ю. Семенов*
Редактор	*Е. Тульсанова*
Корректор	*С. Минин*
Верстка	*Д. Орлова*

Мауро Д., Шмидт К.

Основы SNMP, 2-е издание. – Пер. с англ. – СПб.: Символ-Плюс, 2012. – 520 с., ил.

ISBN 978-5-93286-203-2

Второе издание книги «Основы SNMP» – это практическое руководство для системных и сетевых администраторов, которые пользуются протоколом SNMP для управления своими серверами и маршрутизаторами. Книга начинается с объяснения основных принципов SNMP и его работы и охватывает такие технические элементы, как идентификаторы объектов (OID), базы MIB, строки сообщества и ловушки. Что более важно, эта книга показывает вам, как пользоваться SNMP для получения полной информации о функционировании вашей сети. Внимание авторов сосредоточено на *практическом* системном и сетевом администрировании, конфигурации SNMP-агентов и станций управления сетью, использовании SNMP для получения и изменения переменных на сетевых устройствах и конфигурации программ управления для реагирования на ловушки, отправляемые устройствами.

Главы второго издания были тщательно переработаны и дополнены, и теперь книга содержит ряд Perl-сценариев, которые помогут вам автоматизировать большее число задач по управлению. Вы найдете сценарии для мониторинга служб SMTP, POP3, HTTP и DNS, SNMP-агента на Perl, управления портами коммутатора, использования MIB Cisco Ping, а также раздел по мониторингу беспроводных точек доступа (WAP) и новую главу по Java и SNMP. Книга полна практических примеров использования различных инструментов, от популярных коммерческих продуктов, таких как HP OpenView и Castle Rock SNMPc, до разнообразного ПО с открытым исходным кодом.

ISBN 978-5-93286-203-2
ISBN 978-0-596-00840-6 (англ)

Издательство «Символ-Плюс». 199034, Санкт-Петербург, 16 линия, 7,
тел. (812) 380-5007, www.symbol.ru. Лицензия ЛП N 000054 от 25.12.98.
Подписано в печать 9.12.2011. Формат 70×100 1/16.
Печать офсетная. Объем 32,5 печ. л.

Оглавление

Предисловие

Протокол SNMP (Simple Network Management Protocol – простой протокол управления сетью) – это стандартизированный для Интернета протокол управления устройствами в IP-сетях. SNMP поддерживают многие устройства, такие как маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры, модемные стойки и источники бесперебойного питания. Способы применения SNMP разнообразны, от обыденных до экзотических. С помощью SNMP легко следить за состоянием маршрутизаторов, серверов и других элементов сетевого оборудования, но вы также можете применять его, чтобы управлять сетевыми устройствами, обмениваться сообщениями и автоматически предпринимать необходимые меры при возникновении проблем. Информация, которую вы можете отслеживать, охватывает широкий диапазон: от простых и стандартизированных элементов, например объема входящего и исходящего трафиков интерфейса, до более сложных объектов, специфичных для класса устройства или производителя, таких как температура внутри маршрутизатора.

Зачем писать еще одну книгу по SNMP, если их и так уже издано достаточно? Несмотря на то что книг по SNMP много, далеко не все из них ориентированы на практикующих системных или сетевых администраторов. Обычно рассматривается, как обеспечить работу SNMP, или ведется обсуждение протокола на достаточно абстрактном уровне, но фактически ни одна книга не отвечает на самые важные вопросы сетевого администратора: Как лучше всего применить SNMP в моей сети? Как я могу упростить управление своей сетью?

В главах 2 и 3 мы даем краткий обзор протокола SNMP, а затем последовательно рассматриваем такие темы, как аппаратные требования и виды инструментов, доступных для использования SNMP. Однако основная часть данной книги посвящена обсуждению использования SNMP для задач системного и сетевого администрирования.

Большинство из тех, кто не знаком с SNMP, обычно задают следующие вопросы:

- Что именно представляет собой SNMP?
- Какую пользу может SNMP принести мне как системному администратору?
- Что такое MIB?

- Что такое OID?
- Что такое строка сообщества (community)?
- Что такое ловушка?
- Я слышал, что SNMP небезопасен. Это правда?
- Поддерживают ли SNMP мои устройства? Если да, как я могу определить, правильно ли они настроены?
- Как мне заниматься сбором SNMP-информации с устройства?
- Мои средства на покупку программ для управления сетью ограничены. Какие имеются бесплатные программы и программы с открытым исходным кодом?
- Существует ли Perl-модуль SNMP, который можно использовать для написания хороших сценариев?
- Могу ли я использовать Java™ для работы с SNMP?

Книга отвечает на эти и другие вопросы. Наша задача – снять с SNMP покровы таинственности и сделать его доступным для более широкой аудитории.

Целевая аудитория

Эта книга предназначена для системных и сетевых администраторов, желающих применять SNMP для управления оборудованием, но без опыта или с небольшим опытом работы в этой области. Мы убеждены, что использование SNMP может быть полезно практически для любой сети, какой бы маленькой она ни была. Если вы программист Perl, эта книга даст вам ясное представление о том, как писать сценарии для SNMP, которые помогут вам управлять своей сетью. Если вы не знаток Perl, то можете воспользоваться многими другими инструментами, которые мы представим, от Net-SNMP (набор инструментов командной строки с открытым исходным кодом) до Hewlett-Packard OpenView (высококачественная дорогая платформа управления сетью).

Краткое содержание

В главе 1 «Введение в SNMP и управление сетями» представлен нетехнический обзор управления сетью при помощи SNMP. Мы поговорим о различных версиях SNMP, менеджерах и агентах, принципах сетевого управления и методах управления изменениями.

В главе 2 «SNMPv1 и SNMPv2» обсуждаются технические детали SNMP версий 1 и 2. Мы рассмотрим структуру информации управления (Structure of Management Information – SMI) и информационную базу управления (Managment Information Base – MIB), а также обсудим, как на самом деле работает SNMP – как отправляется и принимается в сети информация об управлении.

В главе 3 «SNMPv3» рассмотрен протокол версии 3, который на данный момент является полным стандартом, обеспечивающим устойчивую безопасность SNMP.

Глава 4 «Архитектуры NMS» поможет вам продумать стратегии развертывания SNMP.

Глава 5 «Настройка NMS» дает основное представление о том, чего ожидать при установке программного обеспечения NMS, на примере двух пакетов NMS: HP OpenView и CastleRock SNMPc.

Глава 6 «Настройка агентов SNMP» описывает, как настраивать некоторые SNMP-агенты для UNIX и Windows, в том числе агент Net-SNMP. В заключительной части главы мы рассмотрим, как настроить встроенные агенты на двух сетевых устройствах: Cisco и APC Symetra.

Глава 7 «Опрос и установка» показывает, как пользоваться инструментами командной строки и Perl для сбора SNMP-информации и изменения состояния управляемого устройства.

В главе 8 «Опрос и пороги» рассмотрено, как настроить OpenView и SNMPc для сбора SNMP-информации через опрос. Кроме того, здесь обсуждается настройка RMON в маршрутизаторе Cisco.

Глава 9 «Ловушки» объясняет, как отправлять и получать ловушки при помощи инструментов командной строки, Perl, OpenView и других приложений управления.

В главе 10 «Расширяемые SNMP-агенты» рассмотрено, как можно увеличить функциональность некоторых популярных SNMP-агентов. Обсуждаются средства для расширения работы агента без доступа к его исходному коду.

Глава 11 «Адаптация SNMP к вашей среде» ориентирована на системных администраторов, владеющих Perl. Мы приводим Perl-сценарии, которые позволяют при помощи SNMP решать некоторые распространенные задачи системного администрирования.

В главе 12 «MRTG» представлено одно из наиболее широко используемых SNMP-приложений с открытым исходным кодом, Multi Router Traffic Grapher (MRTG). MRTG предоставляет сетевым администраторам графики использования интерфейсов маршрутизаторов и может быть настроен для отображения многих других типов данных.

В главе 13 «Инструменты RRDtool и Cricket» описаны эти замечательные средства, которые при совместном использовании предоставляют возможности по графическому отображению, аналогичные MRTG, но с дополнительной гибкостью.

В главе 14 «Java и SNMP» рассмотрено, как использовать Java для создания SNMP-приложений.

В приложении A «Отображение входящего и исходящего трафиков» обсуждаются графики, построенные при помощи OpenView и показывающие количество входящих и исходящих октетов.

В приложении B «Подробнее об OpenView NNM» рассмотрено, как при помощи Network Node Manager (NNM) отображать на графике внешние данные, добавлять в NNM пункты меню, настраивать профили пользователей и использовать NNM как централизованный коммуникационный интерфейс.

Приложение C «Инструменты Net-SNMP» обобщает использование инструментов командной строки Net-SNMP.

В приложении D «RFC, определяющие SNMP» представлен официальный список различных RFC, которые так или иначе касаются SNMP.

Приложение E «Поддержка SNMP для Perl» является хорошим обобщением данных о Perl-модуле SNMP, который используется в примерах книги, а также представляет Perl-модуль Net-SNMP.

В приложении F «Программы управления сетью» представлен обзор программ для управления сетью по категориям.

В приложении G «Программы мониторинга с открытым исходным кодом» описаны наиболее распространенные средства сетевого управления и мониторинга с открытым исходным кодом.

В приложении H «Руководство по устранению неполадок в сети» речь идет об инструментах, которые могут помочь в случае сбоя.

Новое в этом издании

Второе издание было тщательно пересмотрено и расширено. Оно содержит новые данные:

- В главе 1 рассмотрены принципы, лежащие в основе управления сетью и управления изменениями.
- В главе 2 дана трассировка пакетов различных операций SNMP.
- В главе 3 обсуждается SNMPv3. В первом издании эта глава была приложением, здесь она значительно расширена.
- В главах 5 и 9 шире охвачен SNMPc.
- В главе 11 рассмотрено использование сценариев для различных задач. Размер этой главы вырос вдвое, и теперь она включает много новых сценариев. Вы найдете сценарии для мониторинга служб SMTP, POP3, HTTP и DNS, SNMP-агента на Perl, управления портами коммутатора, использования Cisco Ping MIB, а также раздел по мониторингу беспроводных точек доступа (WAP).
- В главе 13, появившейся в этом издании, обсуждаются RRDtool и Cricket.
- В главе 14, также новой в этом издании, показано, как можно использовать Java для создания SNMP-приложений.
- В приложении E дан краткий обзор Perl-модуля Net-SNMP.

- В приложении G рассмотрены детали наиболее распространенных инструментов с открытым исходным кодом для управления сетью и мониторинга сети.
- В приложении H представлены наиболее широко используемые средства устранения неполадок в сети.

Примеры программ

Примеры программ из этой книги доступны на ее веб-странице *http://www.oreilly.com/catalog/esnmp2/*.

Использование программного кода примеров

Эта книга призвана оказать помощь в решении ваших задач. Вы можете свободно использовать приведенные здесь примеры программного кода в своих приложениях и в документации. Вам не нужно обращаться в издательство за разрешением, если вы не собираетесь воспроизводить существенные части программного кода. Если вы, например, разрабатываете программу и используете в ней несколько фрагментов программного кода из книги, на это не требуется разрешения. Однако в случае продажи или распространения компакт-дисков с примерами из этой книги вам *необходимо* получить разрешение от издательства O'Reilly. Если вы отвечаете на вопросы, цитируя данную книгу или примеры из нее, разрешение также не требуется. Но при включении существенных объемов программного кода примеров из этой книги в вашу документацию вам *необходимо* получить разрешение издательства.

Мы приветствуем, но не требуем добавления ссылки на первоисточник при цитировании. Под ссылкой на первоисточник мы подразумеваем указание авторов, издательства и ISBN. Например: «Основы SNMP, второе издание. Дуглас Р. Мауро и Кевин Дж. Шмидт. 2005 O'Reilly Media, Inc., 978-0-596-00840-6».

За получением разрешения на использование значительных объемов программного кода из этой книги обращайтесь по адресу *permissions@oreilly.com*.

Типографские соглашения

В этой книге приняты следующие соглашения:

Курсив

Применяется для выделения адресов электронной почты, URL, имен файлов и каталогов, а также терминов, когда они упоминаются впервые. Кроме того, курсивом выделен перевод некоторых фрагментов листингов.

`Моноширинный шрифт`

Используется для представления содержимого файлов, а также для выделения в тексте названий методов, инструкций и команд из программного кода.

`Моноширинный полужирный`

Применяется для выделения команд или текста, который должен быть введен пользователем, а также для выделения новых или измененных фрагментов программного кода в листингах.

`Моноширинный курсив`

Обозначает замещаемые элементы в программном коде и комментарии.

`<Моноширинный курсив>`

Так выделяются синтаксические элементы, которые должны замещаться действительным программным кодом.

Так выделяются советы, предложения или примечания общего характера, имеющие отношение к расположенному рядом тексту.

Так выделяются предупреждения или предостережения, имеющие отношение к расположенному рядом тексту.

Как с нами связаться

С вопросами и предложениями, касающимися этой книги, обращайтесь в издательство:

O'Reilly Media, Inc.
1005 Gravenstein Highway North
Sebastopol, CA 95472
(800) 998-9938 (в США или Канаде)
(707) 829-0515 (международный/местный)
(707) 829-0104 (факс)

Список опечаток, отзывы и другую дополнительную информацию вы найдете на сайте книги

http://www.oreilly.com/catalog/esnmp2/

Свои пожелания и вопросы технического характера отправляйте по адресу

bookquestions@oreilly.com

Дополнительную информацию о книгах, обсуждения, Центр ресурсов издательства O'Reilly вы найдете на сайте

http://www.oreilly.com

Safari® Enabled

Если на обложке вашей любимой технической книги стоит значок Safari® Enabled, это означает, что книга доступна через O'Reilly Network Safari Bookshelf.

Система Safari лучше обычных электронных книг. Это целая виртуальная библиотека с возможностью поиска по тысячам лучших технических книг, копирования/вставки примеров кода, загрузки глав и быстрого поиска ответов, когда вам требуется самая точная и актуальная информация. Safari можно бесплатно опробовать на сайте *http://safari.oreilly.com*.

Благодарности ко второму изданию

Деб Кэмерон (Deb Cameron) заслуживает большой благодарности за контроль над вторым изданием от начала до конца. Ее усердие и инициатива помогли нам не сойти с пути. Доктор Роберт Минч (Robert Minch), профессор Государственного университета Бойсе, давал ценные советы для второго издания. Бобби Крупцак (Bobby Krupczak), Ph.D., снова предоставлял обратную связь по агенту Concord SystemEDGE. Фрэнк Фок (Frank Fock) любезно рецензировал главу о Java и SNMP. Макс Бейкер (Max Baker) предложил идею алгоритма установки каналов, представленного в главе 11. Джим Боуни (Jim Boney) великодушно предоставил нам в пользование свои маршрутизаторы Cisco. Castle Rock Computing снабдили нас копией SNMPc для второго издания этой книги; отдельное спасибо Джону Мэйтуму (John Maytum) из Castle Rock за координацию нашего доступа к SNMPc.

Мы благодарны за замечания Джейсона Бриггса (Jason Briggs), Билла Хорсфолла (Bill Horsfall) и Джейсона Вайсса (Jason Weiss), которые, несмотря на большую загруженность работой, просматривали новый материал для второго издания.

Дуглас

Я много лет был системным и сетевым администратором и часто сталкивался с вопросом «Как это работает?». Именно он и привел меня к SNMP и в конце концов к идее этой книги. Конечно, я хотел бы поблагодарить Кевина за его усердие и преданность делу. Отдельное спасибо трем особенно любимым мною людям – моей жене Эми и нашим детям Кэри и Мэтью – за то, что терпели мое долгое отсутствие, когда я писал книгу в кабинете. Я также благодарен своей семье и друзьям за поддержку и ободрение.

Кевин

Работа над вторым изданием была очень приятной. После выхода первого издания прошло почти четыре года, и в это время я подумывал о том, что неплохо бы добавить в нее новый материал, если когда-нибудь O'Reilly вознамерится выпустить второе издание. Поэтому я благодарен O'Reilly за возможность обновить эту книгу. Я хотел бы поблагодарить Дугласа за то, что он снова позволил мне работать с ним над книгой. Наконец, я очень признателен Данетт, моей любящей и великодушной жене, за то, что дала мне время, необходимое для завершения этого проекта. Без ее поддержки я бы не справился.

Благодарности к первому изданию

Сказать, что выпуск этой книги занял много времени, было бы излишне скромным. Она никогда не была бы издана без терпения и поддержки Майкла Лукидеса (Mike Loukides). Спасибо, Майк! Еще мы хотели бы поблагодарить людей, которые предоставили нам ценную обратную связь в виде полезных технических обзоров, а также общую поддержку и указания: Майка ДеГро-Берча (Mike DeGraw-Bertsch) из O'Reilly, Дональда Кули (Donald Cooley) из Global Crossing, Джейкоба Кирша (Jacob Kirsch) из Sun Microsystems, Inc., Бобби Крапцака (Bobby Krupczak), Ph.D., из Concord Communications, Джона Рейнхардта (John Reinhardt) из Road Runner, Патрика Бэйли (Patrick Bailey) и Роба Свита (Rob Sweet) из Netrail, а также Юргена Шонвальдера (Jurgen Schonwalder) из Технического университета Брауншвейга. Роб Романо (Rob Romano), талантливый художник-график из O'Reilly, заслуживает благодарности за великолепные рисунки в книге. Наконец, спасибо Джиму Самсеру (Jim Sumser), который сопровождал проект на завершающих этапах, и Рэйчел Уилер (Rachel Wheeler), техническому редактору, за компоновку этой книги.

1

Введение в SNMP и управление сетями

В современной комплексной сети из маршрутизаторов, коммутаторов и серверов задача управления всеми устройствами и обеспечения того, чтобы они не просто функционировали, а работали оптимально, может показаться обескураживающей. Вот где может помочь SNMP (Simple Network Management Protocol) – простой протокол управления сетью. SNMP был введен в 1988 году с целью удовлетворить растущую потребность в стандарте для управления устройствами, поддерживающими интернет-протокол IP (Internet Protocol). SNMP предоставляет пользователям «простой» набор операций, позволяющий управлять этими устройствами удаленно.

Эта книга будет полезна системным администраторам, которые хотели бы начать использовать SNMP для управления своими серверами или маршрутизаторами, но не имеют для этого достаточных знаний или понимания. Мы постараемся дать вам базовое представление о том, что представляет собой SNMP и как он работает; кроме того, мы покажем вам, как применять SNMP на практике, используя ряд широко доступных инструментов. Прежде всего, мы хотим, чтобы эта книга была полезной на практике – помогала отслеживать, что происходит в вашей сети.

В этой главе обсуждаются протокол SNMP, управление сетями и управление изменениями. Очевидно, основной темой этой книги является SNMP, но понимание общих принципов управления сетями лучше подготовит вас к использованию SNMP для нужд своей сети.

Что такое SNMP

Основа SNMP[1] – простой набор операций (и информации, собираемой посредством этих операций), который предоставляет администраторам возможность изменять состояние какого-либо устройства, поддерживающего SNMP. Например, вы можете использовать SNMP, чтобы отключить интерфейс на маршрутизаторе или проверить скорость, с которой работает интерфейс Ethernet. SNMP позволяет даже отслеживать температуру коммутатора и предупреждать вас, когда она слишком высока.

Обычно SNMP ассоциируется с управлением маршрутизаторами, но важно понимать, что его можно использовать для управления устройствами различных типов. Хотя предшественник SNMP, простой протокол управления маршрутизаторами SGMP (Simple Gateway Management Protocol), разрабатывался для управления интернет-маршрутизаторами, SNMP может использоваться для управления UNIX- и Windows-системами, принтерами, модемными блоками, источниками питания и другими устройствами. Можно управлять любым устройством, на котором запущено программное обеспечение, позволяющее получать информацию SNMP. Это справедливо не только для физических устройств, но и для программ, например веб-серверов и баз данных.

Другой аспект управления сетью – мониторинг сети, то есть мониторинг всей сети, а не отдельных маршрутизаторов, узлов и других устройств. Чтобы помочь нам понять, как работает сама сеть, а также как отдельные ее устройства влияют на сеть в целом, был разработан модуль удаленного мониторинга (RMON – Remote Network Monitoring). Он может использоваться для мониторинга не только трафика в локальной сети (LAN – Local Area Network), но и интерфейсов WAN. Мы рассмотрим RMON более подробно далее в этой главе и в главе 2.

RFC и версии SNMP

За стандартные протоколы, регулирующие трафик Интернета, в том числе SNMP, отвечает Группа по стандартам для сети Интернет IETF (Internet Engineering Task Force). IETF публикует документы RFC (Request for Comments), которые представляют собой спецификации для многих протоколов, существующих в мире IP. Сначала документы представляются в рабочей версии как *предлагаемые* стандарты, затем получают *временный* статус. Когда наконец утверждается последняя версия, RFC получает статус *стандарта* – хотя полностью утвержденных

[1] Протокол SNMP уникален тем, что использует управление не с помощью команд, а посредством информации. Субъект не может ожидать немедленной реакции от объекта управления, поскольку такая реакция возникает лишь тогда, когда внесенная субъектом информация будет использована объектом. – *Прим. науч. ред.*

стандартов меньше, чем вы можете подумать. Два других статуса стандартов, *исторический* и *экспериментальный*, определяют соответственно документы, замещенные более новой версией (с новым номером) и еще не готовые стать стандартом. В следующем списке приведены все текущие версии SNMP и статус каждой из них в IETF (полный список RFC, связанных с SNMP, приведен в приложении D):

- SNMP версии 1 (SNMPv1) – первоначальная версия протокола SNMP. Она определена в RFC 1157 и является историческим стандартом IETF. Безопасность SNMPv1 основана на строках community (поле «пароль»), которые представляют собой просто пароли. Они позволяют любому SNMP-приложению, которое их знает, получать доступ к информации об управлении устройством. Обычно в SNMPv1 используются три значения community: *read-only* (*только чтение*), *read-write* (*чтение и запись*) и *trap* (*ловушка* – уведомление). Следует отметить, что, хотя SNMPv1 стал историческим стандартом, он все еще является основной реализацией SNMP, поддерживаемой многими производителями.
- SNMP версии 2 (SNMPv2) часто называют SNMPv2 с поддержкой строк community. Технически эта версия SNMPv2 называется SNMPv2c, но в этой книге мы будем называть ее просто SNMPv2. Она определена в RFC 3416, RFC 3417 и RFC 3418.
- SNMP версии 3 (SNMPv3) – последняя версия SNMP. Ее главный вклад в управлении сетями заключается в безопасности. В ней добавлена поддержка сильной аутентификации и закрытой связи между управляемыми объектами. В 2002 году она наконец перешла из разряда временного стандарта в разряд полного стандарта. Этот стандарт определяется следующими документами: RFC 3410, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3415, RFC 3416, RFC 3417, RFC 3418 и RFC 2576. В главе 3 представлен подробный разбор SNMPv3, а в главе 6 рассмотрена настройка агента SNMPv3 для Net-SNMP и Cisco. И хотя SNMPv3 уже является утвержденным стандартом, производители, как обычно, медленно принимают новые версии протокола. Несмотря на то что SNMPv1 стал историческим стандартом, подавляющее большинство реализаций производителями SNMP являются версиями SNMPv1. Некоторые крупные производители сетевой инфраструктуры, такие как Cisco, уже начали поддерживать SNMPv3, и мы, несомненно, будем наблюдать, как все больше производителей станут переходить на SNMPv3 по мере того, как покупатели будут настаивать на более безопасных средствах управления сетями.

Официальный сайт RFC – *http://www.ietf.org/rfc.html*. Впрочем, одна из самых серьезных проблем с RFC – найти нужный вам документ. На сайте Университета штата Огайо ориентироваться в указателе RFC чуть проще (*http://www.cse.ohio-state.edu/cs/Services/rfc/index.html*).

Менеджеры и агенты

В предыдущих разделах мы вскользь упомянули о поддерживающих SNMP устройствах и станциях управления сетями. Теперь пора объяснить, что это на самом деле. В мире SNMP существует два вида объектов: менеджеры и агенты. *Менеджер* – это сервер, на котором запущена какая-либо программная система, имеющая возможность выполнять задачи по управлению сетью. Менеджеры часто называют станциями управления сетью (NMS – Network Management Stations)[1]. NMS отвечает за опрос и получение ловушек от агентов в сети. *Опрос* в контексте управления сетью – это действие по запросу у агента (маршрутизатора, коммутатора, UNIX-сервера и т. п.) какой-либо информации. В дальнейшем эта информация может быть использована, чтобы определить, не произошло ли какое-нибудь катастрофическое событие. *Ловушка* – это способ для агента сообщить NMS о каком-то событии. Далее NMS отвечает за действие[2] в соответствии с информацией, полученной от агента. Например, маршрутизатор может отправить NMS ловушку, когда интернет-канал T1 отключается. NMS, в свою очередь, может выполнить какое-то действие, например сообщить вам о произошедшем событии.

Второй тип объекта, *агент*, – это программный элемент, запущенный на управляемом сетевом устройстве. Это может быть отдельная программа (демон в терминологии UNIX) или элемент операционной системы (например, Cisco IOS для маршрутизатора или операционной системы низкого уровня, управляющей источником бесперебойного питания). В настоящее время в большинстве IP-устройств есть какой-либо встроенный SNMP-агент. То, что производители охотно реализуют агенты во многих своих продуктах, упрощает работу системного или сетевого администратора. Агент предоставляет NMS информацию для управления, отслеживая различные рабочие параметры устройства. Например, агент на маршрутизаторе может отслеживать состояние каждого интерфейса: какие работают, какие отключены и т. д. NMS может запрашивать состояние каждого интерфейса и принимать соответствующие меры, если какие-либо из них отключаются. Когда агент замечает, что произошел какой-то сбой, он может отправить NMS ловушку. Эта ловушка исходит от агента и отправляется NMS, где она соответствующим образом обрабатывается. При переходе из аварийного состояния в нормальное некоторые устройства отправляют соответствующую ловушку[3] «все в порядке». Это может быть полезно для определения того,

---

[1] Список некоторых популярных приложений NMS приведен в приложении F.

[2] Имейте в виду, что NMS предварительно настроена для выполнения этого действия.

[3] Протокол SNMP является управляющим, а управление не может быть эффективным без обратной связи. Функцию обратной связи и выполняет операция `trap` – ловушка. – *Прим. науч. ред.*

что проблемная ситуация разрешена. На рис. 1.1 показана связь между NMS и агентом.

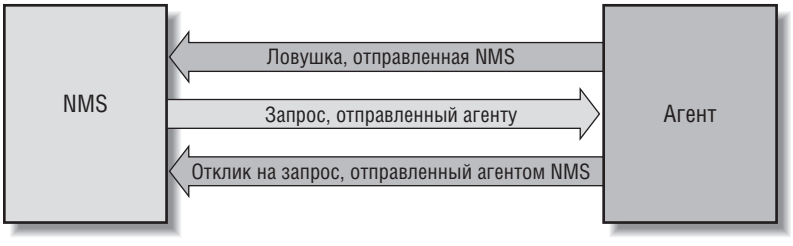

Рис. 1.1. *Связь между NMS и агентом*

Важно иметь в виду, что запросы и ловушки могут отправляться одновременно. Для времени, когда NMS может опросить агента или когда агент может отправить ловушку, ограничений нет.

Структура информации для управления и MIB

Структура информации для управления (SMI – Structure of Management Information) предоставляет способ определения управляемых объектов и их поведения. У агента есть список отслеживаемых им объектов. Один из таких объектов – состояние работы интерфейса маршрутизатора (например, *работает*, *не работает* или *тестируется*). Этот список собирает информацию, которой NMS может воспользоваться для определения общего состояния того устройства, на котором работает агент.

База управляющей информации (MIB – Management Information Base) может рассматриваться как база данных управляемых объектов, которые отслеживает агент. Все данные о состоянии или статистическая информация, к которой есть доступ у NMS, определены в MIB. SMI предоставляет способ определения управляемых объектов, тогда как MIB – это определение (в терминологии SMI) самих объектов. Как словарь, в котором показывается написание слова, а затем приводится его толкование, MIB определяет текстовое имя управляемого объекта и объясняет его значение. В главе 2 приведено больше технических подробностей о MIB и SMI.

В агенте может быть реализовано много MIB, но во всех агентах реализована конкретная MIB, которая называется MIB-II[1] (RFC 1213). Этот стандарт определяет переменные для таких параметров, как статистика интерфейса (скорость интерфейса, MTU, количество отправленных

[1] Первоначальная версия – это MIB-I, но на нее больше не ссылаются, потому что MIB-II ее расширяет.

октетов[1], количество принятых октетов и т. д.), а также различных параметров, относящихся к самой системе (местоположение системы, контактные сведения и т. д.) Основная цель MIB-II – предоставить общую управляющую информацию TCP/IP. Она не охватывает все возможные объекты, которыми производителю может потребоваться управлять в конкретном устройстве.

Какая еще информация может оказаться полезной? Во-первых, было разработано много временных и предлагаемых стандартов для управления сетями Frame Relay, ATM, FDDI и службами (почта, доменная система имен (DNS – Domain Name System)). Вот примеры этих MIB и номеров их RFC:

- ATM MIB (RFC 2515)
- MIB для интерфейса DTE Frame Relay (RFC 2115)
- MIB для BGP версии 4 (RFC 1657)
- RDBMS MIB (RFC 1697)
- MIB сервера аутентификации RADIUS (RFC 2619)
- MIB мониторинга почты (RFC 2789)
- MIB DNS-сервера (RFC 1611)

Но этот список далек от полного, вот почему производители и отдельные пользователи могут определять переменные MIB для своих нужд[2]. Например, рассмотрим производителя, который выводит на рынок новый маршрутизатор. Агент, встроенный в маршрутизатор, будет отвечать на запросы NMS (или отправлять NMS ловушки) для переменных, определенных стандартом MIB-II; возможно, в нем также будут реализованы MIB для используемых им типов интерфейсов (например, RFC 2515 для ATM и RFC 2115 для Frame Relay). Кроме того, в маршрутизаторе могут быть новые важные функции, которые стоит отслеживать, но они не охватываются никакими стандартными MIB. Поэтому производитель определяет собственную MIB (иногда называемую *проприетарной MIB*), в которой реализованы управляемые объекты для информации о состоянии и статистической информации его нового маршрутизатора.

Простая загрузка новой MIB в вашу NMS необязательно позволит вам получать данные/значения/объекты и т. д., определенные в этой MIB. Вам нужно загружать только те MIB, которые поддерживаются опрашиваемыми агентами (например, `snmpget`, `snmpwalk`). Вы можете свободно загружать дополнительные MIB для поддержки будущих устройств, но не паникуйте, когда ваше устройство не отвечает (а возможно, возвращает ошибки) на запросы по этим неподдерживаемым MIB.

---

[1] Октет – это 8 бит, основная единица передаваемой информации в сетях TCP/IP.

[2] Эта тема будет рассмотрена в следующей главе.

Управление узлом

Управление ресурсами узла (дисковым пространством, использованием памяти и т. д.) – важный элемент управления сетью. Грань между традиционным системным администрированием и управлением сетью в течение последних десяти лет стиралась и в настоящее время практически отсутствует. Как утверждают в Sun Microsystems, «сеть – это компьютер». Если отказал ваш веб-сервер или почтовый сервер, то неважно, правильно ли работают ваши маршрутизаторы, – вы все равно будете получать жалобы. MIB ресурсов узла (RFC 2790) определяет набор объектов, которые помогают управлять критическими аспектами UNIX- и Windows-систем[1].

Среди объектов, поддерживаемых MIB ресурсов узла, – емкость диска, количество пользователей системы, количество запущенных процессов и установленное в данный момент программное обеспечение. В настоящее время все больше людей пользуются сервис-ориентированными вебсайтами. Обеспечение правильного функционирования внутренних серверов так же важно, как мониторинг маршрутизаторов и других коммуникационных устройств.

К сожалению, для некоторых агентов на этих платформах такая MIB не реализована, так как это не требуется.

Краткое введение в удаленный мониторинг

Стандарт удаленного мониторинга Remote Monitoring версии 1 (RMONv1, или RMON) определен в RFC 2819; расширенная версия стандарта, называемая RMON версии 2 (RMONv2), определена в RFC 2021. RMONv1 предоставляет NMS статистику обо всей локальной или глобальной сети на уровне пакетов. RMONv2 надстраивается над RMONv1, предоставляя статистику на сетевом и прикладном уровнях. Эту статистику можно собирать различными способами. Один из них – разместить датчик RMON на каждом сегменте сети, за которым вы хотите наблюдать. В некоторых маршрутизаторах Cisco есть ограниченные возможности удаленного мониторинга, поэтому вы можете использовать их функции для второстепенных задач удаленного мониторинга. Подобным образом в некоторых коммутаторах 3Com реализована полная спецификация RMON и их можно использовать как полнофункциональные датчики RMON.

База RMON MIB была создана, чтобы позволить самому датчику RMON работать в оффлайновом режиме (не в реальном времени), который позволяет датчику собирать статистику о наблюдаемой им сети, не требуя от NMS постоянного опроса. Через какое-то время NMS может запросить у датчика собранную им статистику. Другая функция, реализо-

[1] Реализация базы ресурсов узла возможна в любой операционной системе, использующей SNMP; она не ограничена агентами UNIX- и Windows-систем.

ванная в большинстве датчиков, – возможность устанавливать пороговые значения для различных аварийных состояний и при превышении порога сообщать об этом NMS SNMP-уведомлением. В следующей главе технические детали RMON рассмотрены более подробно.

Принципы управления сетями

Фактически SNMP используется для управления сетями. Управление сетями – отдельная дисциплина, но, прежде чем приступить к подробному изучению SNMP в главе 2, полезно получить достаточно ясное представление о том, что такое управление сетями.

Что такое управление сетями? Это общая концепция, предполагающая использование различных инструментов, методов и систем для помощи людям в управлении различными устройствами, системами или сетями. Давайте пока отвлечемся от SNMP и рассмотрим модель управления сетями, называемую *FCAPS*, которая включает управление обработкой отказов (Fault Management), конфигурацией (Configuration Management), учетными записями (Accounting Management), рабочими характеристиками (Performance Management) и безопасностью (Security Management). Эти смысловые области были созданы Международной организацией по стандартизации ISO для помощи в изучении основных функций систем управления сетями. Теперь давайте кратко рассмотрим каждую из них.

Управление обработкой отказов

Цель управления обработкой отказов – обнаруживать и фиксировать проблемы, а также уведомлять о них пользователей систем или сетей. Во многих средах неприемлемы никакие отказы.

Управление обработкой отказов предписывает выполнение следующих этапов решения проблем:

1. Выделить проблему, используя инструменты определения симптомов.
2. Разрешить проблему.
3. Записать процесс, использованный для обнаружения и разрешения проблемы.

Хотя этап 3 важен, часто он пропускается. Пренебрежение этим этапом ведет к тому, что приходится вновь и вновь выполнять этапы 1 и 2 вслепую, тогда как можно было бы обратиться к базе данных или советам по устранению неполадок.

Управление конфигурацией

Цель управления конфигурацией – наблюдать за информацией о конфигурации сетей и систем, чтобы можно было отслеживать и контроли-

ровать воздействие на работу сети различных версий аппаратных и программных элементов.

В любой системе имеется ряд интересных и важных параметров конфигурации, в отслеживании которых технические специалисты могут быть заинтересованы, в том числе:

- Версия операционной системы, фирменной реализации и т. п.
- Количество сетевых интерфейсов, скорости и т. п.
- Количество жестких дисков
- Количество процессоров
- Объем оперативной памяти

Обычно эта информация хранится в какой-либо базе данных. По мере обновления параметров конфигурации систем модифицируется и эта база данных. Дополнительное преимущество хранения этих данных заключается в том, что они могут помочь в решении проблем.

Управление учетом

Цель управления учетом – обеспечить, чтобы вычислительные и сетевые ресурсы были должным образом распределены между всеми группами или индивидуумами, осуществляющими к ним доступ. Благодаря такому регулированию можно минимизировать проблемы сети, так как ресурсы распределяются в зависимости от нагрузки.

Управление производительностью

Цель управления производительностью – измерять различные аспекты производительности сети или системы и сообщать о них.

Рассмотрим этапы управления производительностью:

1. Сбор данных о производительности.
2. Определение базовых уровней на основании анализа собранных данных.
3. Установка пороговых значений производительности. Достижение этих порогов является признаком проблемы, которая требует внимания.

Один из примеров управления производительностью – мониторинг служб. Например, интернет-провайдера может интересовать мониторинг времени реакции его службы электронной почты, в том числе при отправке сообщений через SMTP и получении почты через POP3. Примеры того, как это сделать, рассмотрены в главе 11.

Управление безопасностью

Цель управления безопасностью двояка. Во-первых, нам нужно контролировать доступ к некоторому ресурсу, например к сети и ее узлам.

Во-вторых, нам нужна помощь в обнаружении и предотвращении атак, которые могут скомпрометировать сети и узлы. Атаки против сетей и узлов могут привести к отказу в обслуживании или, что еще хуже, позволить хакерам получить доступ к жизненно важным системам, содержащим данные об учете, платежах либо исходные коды.

Управление безопасностью охватывает не только сетевые системы безопасности, но и физическую безопасность. Физическая безопасность включает системы контроля доступа и видеонаблюдения. Их задача в том, чтобы обеспечить физический доступ к уязвимым системам только для авторизованного персонала.

В настоящее время управление безопасностью сетей осуществляется путем использования различных инструментов и систем, специально спроектированных для этой цели. Они включают:

- Брандмауэры
- Системы обнаружения вторжений (IDS – Intrusion Detection System)
- Системы предотвращения вторжений (IPS – Intrusion Prevention System)
- Антивирусные системы
- Системы управления политикой доступа и контроля за ее выполнением

Большинство современных систем сетевой безопасности, если не все, могут быть интегрированы с системами управления сетями посредством SNMP.

Применение принципов управления сетями

Умение применять принципы управления сетями так же важно, как изучение возможностей SNMP. В этом разделе рассмотрены некоторые вопросы, связанные с управлением сетями.

Требования экономической модели

Работа по управлению сетями предполагает поиск эффективных решений для задач бизнеса. Разработанная экономическая модель позволяет лучше понять, насколько хорошо выполняется та или иная задача или функция. Например, это может касаться повседневной работы сетевых администраторов. Основной смысл заключается в снижении расходов и повышении эффективности. Если нововведение не приведет к экономии денег компании при обеспечении более эффективного обслуживания, в реализации данного решения практически нет необходимости[1].

[1] Это утверждение может быть несправедливым по отношению к безопасности, которую трудно оценить в деньгах, пока все в порядке. Но в случае сетевого вторжения фирма может быть разорена. – *Прим. науч. ред.*

Уровни активности

Прежде чем управлять конкретной службой или устройством, вы должны знать о четырех возможных уровнях активности и решить, какой из них подходит для этой службы или устройства.

Неактивный

Мониторинг не ведется, и, если бы вы получили в этой области сигнал тревоги, вы бы его проигнорировали.

Реактивный

Мониторинг не ведется; в случае возникновения проблемы вы на нее реагируете.

Интерактивный

Вы наблюдаете за компонентами и должны в интерактивном режиме устранять неполадки для исключения побочных сигналов тревоги и выявлять их основные причины.

Предупреждающий

Вы наблюдаете за компонентами, а система обеспечивает сигнал тревоги при возникновении проблемы и по возможности запускает предопределенные автоматические процессы по восстановлению, чтобы минимизировать время отказа.

Анализ тенденций

Возможность мониторинга службы или системы с упреждением начинается с анализа тенденций и сообщения о них. В главах 12 и 13 описаны два инструмента, которые могут здесь помочь. В принципе, цель анализа тенденций – выявить, когда загрузка системы, службы или сети приближается к максимальной, но при этом еще есть достаточный запас времени, чтобы принять какие-то меры, прежде чем это станет реальной проблемой для конечных пользователей. Например, вы можете обнаружить необходимость увеличить объем памяти сервера базы данных или перейти на более новую версию какого-либо приложения сервера, которая повышает производительность. Принятие этих мер прежде, чем проблема станет реальной, может помочь вашим пользователям избежать раздражения, а вам, возможно, увольнения.

Время реакции

Если вы отвечаете за управление каким-либо сервером (HTTP, SMTP и т. д.), то знаете, как могут раздражать жалобы пользователей на слишком медленную работу веб-сервера или загрузку интернет-страниц. Время реакции позволяет оценить, как работают различные элементы вашей сети (в том числе системы) в смысле скорости отклика. В главе 11 рассмотрено, как при помощи SNMP вести мониторинг сервисов.

Корреляция предупреждений

Корреляция аварийных сигналов связана с объединением большого количества сигналов и событий в один сигнал или несколько событий, отражающих реальную проблему. Другое ее название – анализ основной причины. Идея проста, но ее реализация на практике обычно сложная. Например, когда в сети отключается веб-сервер, а вы управляете всеми устройствами между вами и сервером (в том числе и коммутатором, к которому сервер подключен, и маршрутизатором) то можете получить любое количество предупреждений, например, об отказе сервера, коммутатора или маршрутизатора, в зависимости от того, где на самом деле произошел сбой.

Допустим, проблема в маршрутизаторе (например, вышла из строя карта сетевого интерфейса). На самом деле вам нужно знать только то, что маршрутизатор отказал. Системы управления сетями часто могут обнаруживать, когда какое-либо устройство или сеть недостижимы в силу различных причин. Ключевым действием в этой ситуации является объединение сигналов сервера, коммутатора и маршрутизатора в единое событие высокого уровня, уточняющее, что отказал маршрутизатор. Это событие высокого уровня может состоять из всех затронутых отказавшим маршрутизатором объектов и их предупреждений, но вам нужно оградить оператора от них, пока он сам ими не заинтересуется. Реальная проблема, которую нужно решить, – это отказ маршрутизатора. Исключение этой кучи предупреждений и сигналов из поля зрения оператора повышает общую эффективность и расширяет способности персонала по устранению неполадок.

Удаление предупреждений также важно. Например, когда маршрутизатор снова заработает, то предположительно он должен отправить об этом SNMP-уведомление или система управления сетью обнаружит, что устройство возобновило свою работу, и сформирует об этом предупреждение. Такое сообщение об изменении состояния со сбойного на нормальное является обычным. Оно помогает операторам узнать, что что-то действительно заработало. Оно также помогает в выявлении тенденций. Если вы будете видеть, что определенное устройство постоянно отказывает, вы можете захотеть разобраться, почему.

Устранение неполадок

Ключ к устранению неполадок – знание о том, что данные, предоставляемые вам, являются ценными и могут помочь вам решить проблему. Например, когда отказывает маршрутизатор, загадочное сообщение «маршрутизатор отказал» бесполезно. По возможности предупреждения и сигналы должны предоставлять оператору достаточно подробностей, чтобы он мог эффективно выявить и устранить проблему.

Управление изменениями

Управление изменениями касается, как ни странно, управляемых изменений. Другими словами, вам нужно планировать как плановые, так и экстренные изменения в своей сети. Если этого не делать, сети в лучшем случае могут быть ненадежными, а в худшем – приносить неприятности тем людям, на которых вы работаете. В следующих разделах дан общий обзор методов управления изменениями. Эти методы рекомендованы Cisco. В конце данного раздела приведены URL этого и других документов по управлению сетями.

Планирование изменения

Планирование изменения – это процесс, который определяет уровень риска изменения и устанавливает требования, чтобы обеспечить успех выполняемой задачи. Основные этапы планирования изменения следующие:

- Перед планированием изменения присвойте всем потенциальным изменениям уровень риска.
- Задокументируйте как минимум три уровня риска с соответствующими требованиями к планированию изменений. Определите уровни риска для обновлений программного и аппаратного обеспечения, изменений топологии, маршрутизации и конфигурации, а также введения новых систем. Нестандартным действиям по добавлению, перемещению или изменению присваивайте более высокие уровни риска.
- Документируемый вами процесс изменения с высоким риском должен включать лабораторное тестирование, обзор поставщиками, обсуждение коллегами и подробную документацию по конфигурации и проектированию.
- Создайте шаблоны решений для введения новых систем, затрагивающих несколько местоположений. Включите информацию о физической компоновке, логической структуре, конфигурации, версиях программного обеспечения, приемлемых аппаратных платформах и модулях и указания по введению в эксплуатацию.
- Документируйте свои сетевые стандарты по конфигурации, версиям программного обеспечения, поддерживаемым аппаратным средствам и DNS. Кроме того, вам может потребоваться документировать такие аспекты, как правила именования устройств, детали проектирования сети и поддерживаемая сетью пропускная способность.

Управление изменением

Управление изменением – это процесс, который подтверждает изменение и составляет его график, чтобы обеспечить подходящий уровень уведомления с минимальным влиянием на пользователей. Вот ключевые этапы управления изменением:

- Назначьте ответственного за изменения, который сможет проводить собрания по управлению изменением, получать и рассматривать запросы на изменения, контролировать улучшение процесса изменения и действовать как связующее звено для групп пользователей.
- Проводите периодические собрания по рассмотрению изменения с группами системного администрирования, разработки приложений, эксплуатации сети, материально-технического обеспечения, а также основными пользователями.
- Документируйте начальные требования к изменению, в том числе владельца изменения, значение для бизнеса, уровень риска, причину изменения, факторы успеха, план отмены и требования по тестированию.
- Документируйте конечные требования к изменению, в том числе изменения в DNS, карте сети, маске, IP-адресации, управлении каналами связи и управлении сетью.
- Определите процесс утверждения изменения, в котором проверяются этапы подтверждения изменений с более высоким риском.
- Проводите собрания по разбору неудачных изменений для определения исходной причины неудачи.
- Разработайте процедуру экстренного изменения, обеспечивающую поддержание или быстрое восстановление оптимального решения.

Общая структура процесса управления запланированным изменением

Этапы, которые вам потребуется пройти при изменении в сети, представлены на рис. 1.2[1]. В следующих разделах кратко рассматривается каждый блок схемы.

Охват

Охват – это ответ на вопросы «кто», «что», «где» и «как». Другими словами, вам нужно подробно описать все возможные последствия изменения, особенно его влияние на людей.

Оценка риска

Все, что вы делаете в сети, когда дело касается изменений, связано с определенным риском. Тот, кто запрашивает изменение, должен установить для него уровень риска. По возможности лучше всего экспериментировать в лаборатории, прежде чем вносить изменение в рабочую систему. Это может помочь в выявлении проблем и оценке риска.

---

[1] Рис. 1.2 и 1.3 перепечатаны с разрешения правообладателя, Cisco «Change Management: Best Practices White Paper», Document ID 22852, *http://www.cisco.com/warp/public/126/chmgmt.shtml*.

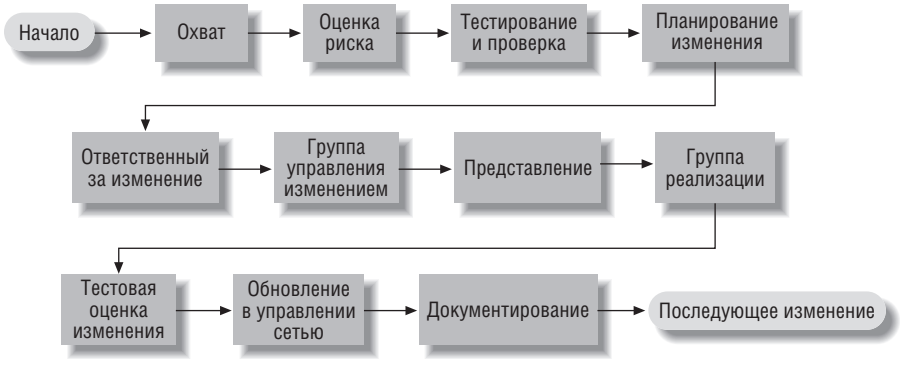

Рис. 1.2. *Структура процесса управления запланированным изменением*

Тестирование и проверка

В случае с любым предлагаемым изменением вам потребуется убедиться, что приняты все меры предосторожности. Здесь могут помочь строгое тестирование и проверка. В зависимости от уровня риска может потребоваться выполнить различные уровни проверки. Например, если изменение затронет большое количество систем, вам может потребоваться проверить его в лабораторной среде. Если изменение не работает, также может возникнуть необходимость задокументировать процедуры отмены.

Планирование изменения

Чтобы изменение было успешным, вы должны составить его план. Планирование включает сбор требований, заказ программных или аппаратных средств, создание документации и координацию персонала.

Ответственный за изменение

В сущности, ответственный за изменение – это человек, который отвечает за координацию всех деталей процесса изменения.

Группа управления изменением

Вам нужно создать группу управления изменением, включающую представителей от подразделений эксплуатации сети, эксплуатации сервера, поддержки приложения и групп пользователей вашей организации. Группа должна рассматривать все запросы на изменение и одобрять или отклонять каждый из них в зависимости от полноты, готовности, влияния на бизнес, потребности бизнеса и любых возможных конфликтов.

Группа управления изменением не проверяет техническую корректность изменений; этот этап процесса изменения должны выполнять технические эксперты, которые лучше понимают область и технические детали.

Представление

Многие организации, даже небольшие, не оповещают сотрудников о своих намерениях. Убедитесь, что вы держите в курсе состояния изменений людей, которых они могут затронуть.

Группа реализации

Вам нужно создать группу реализации из специалистов с техническими знаниями для проведения изменения. Группа реализации также должна участвовать в этапе планирования, чтобы внести свой вклад в разработку контрольных точек проекта, тестирование, определение критериев отмены и временных рамок отмены. Эта группа должна гарантировать соблюдение стандартов организации, обновлять DNS и инструменты управления сетью, а также поддерживать и расширять инструментарий, используемый для проверки и подтверждения изменения.

Тестовая оценка изменения

После реализации изменения вы должны приступить к его проверке. Хорошо, если у вас уже есть документированный набор тестов, которым можно воспользоваться для проверки изменения. Убедитесь, что у вас достаточно времени на проведение тестов. Если вы должны отменить изменение, убедитесь, что этот сценарий вы тоже проверили.

Обновление в управлении сетью

Будьте готовы обновить все системы, такие как инструменты по управлению сетью, конфигурации сети, записи DNS и т. д., в соответствии с изменением. Это может включать изъятие устройств из систем управления, которых больше не существует, изменение адреса получателя SNMP-уведомлений, используемого маршрутизаторами, и т. д.

Документирование

Всегда обновляйте документацию, которая после изменения устаревает или становится недостоверной. Может оказаться, что документация будет использоваться администратором сети для решения проблем. Если она неактуальна, он не сможет эффективно выполнять свои обязанности.

Общая структура процесса управления экстренным изменением

В реальной жизни изменение часто происходит в 2 часа ночи, когда отказывает какая-нибудь критическая система. Но, приложив некоторые усилия в процессе изменения «на лету», вы избежите стрессов и недовольства других сотрудников компании. При экстренных изменениях документация имеет гораздо большее значение, чем при запланированных. В экстренной ситуации что-то может потеряться или забыться.

Точная запись выполняемых шагов и процедур обеспечит возможность решения подобных проблем в будущем. При необходимости ведите короткие заметки по ходу процесса. В дальнейшем составьте из них формальную докуметацию, важно не забыть это сделать.

На рис. 1.3 показан процесс экстренного изменения.

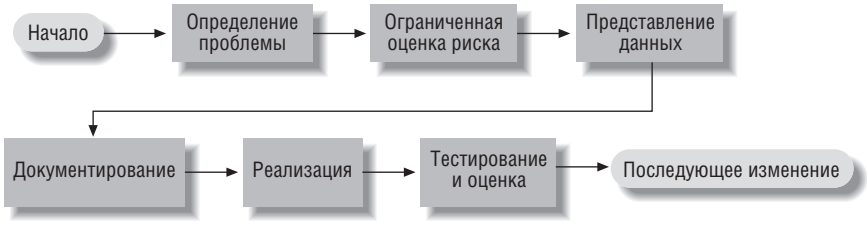

Рис. 1.3. *Процесс экстренного изменения*

Определение проблемы

В экстренной ситуации обычно несложно определить, что нужно изменить. Главное – делать все вовремя и не спешить. Да, время очень важно, но спешка может вызвать ошибки или даже привести к решению, которое не исправит проблемы. В некоторых случаях время отказа может излишне затянуться.

Ограниченная оценка риска

Оценка риска проводится дежурным сетевым администратором при содействии остального персонала поддержки. Классификация изменения с точки зрения риска определяется его опытом. Например, изменение версии программного обеспечения маршрутизатора имеет гораздо больший эффект, чем изменение IP-адреса устройства.

Взаимодействие и документирование

Пользователям нужно сообщить об изменении, если это вообще возможно. В экстренной ситуации это возможно не всегда. Кроме того, обязательно обсуждайте все изменения с ответственным за них руководителем. Он захочет уточнить, что именно следует документировать. Обеспечение актуальности документации нельзя переоценить. Наличие неактуальной документации означает, что в будущем персонал не сможет безошибочно устранять сетевые и системные проблемы.

Реализация

Если перед реализацией были выполнены оценка риска и документирование, сама по себе реализация должна быть простой. Остерегайтесь внесения возможных изменений различными сотрудниками поддержки,

не знающими об изменениях друг друга. Такая ситуация может привести к увеличению времени простоя и неправильному пониманию проблемы.

Тестирование и оценка

Обязательно протестируйте изменение. Обычно изменение тестируется и оценивается тем же человеком, который его выполнял. Основная цель заключается в том, чтобы определить, принесло ли изменение желаемый эффект. Если не принесло, процесс экстренного изменения нужно начать заново.

До и после применения SNMP

Теперь, когда у вас есть представление о том, что такое SNMP и управление сетями, мы поговорим о практической пользе применения этих принципов и технологий. Допустим, у вас есть сеть из 100 машин с различными операционными системами. Несколько машин являются файловыми серверами, несколько других – серверы печати, еще на одной запущена программа проверки транзакций по кредитным картам (скорее всего, из веб-системы заказа), а остальные – персональные рабочие станции. Кроме того, работа сети поддерживается несколькими коммутаторами и маршрутизаторами. Компания подключена к Интернету по каналу T1, к системе проверки кредитных карт идет защищенное соединение.

Что происходит при сбое одного из файловых серверов? Если это случается в середине рабочей недели, его пользователи заметят сбой и вызовут системного администратора, чтобы исправить проблему. Но что если это произойдет, когда все, в том числе администраторы, уже ушли домой или в выходные?

Что если защищенное соединение с системой проверки кредитных карт отключилось в 22 часа в пятницу и не работало до утра понедельника? Проблема может заключаться в аппаратном сбое, для устранения которого требуется лишь замена карты или маршрутизатора, а тысячи долларов от продаж на веб-сайте будут безвозвратно потеряны. Отключение интернет-канала T1 также может негативно повлиять на объемы продаж, обеспечиваемые людьми, которые посещают ваш веб-сайт и размещают там заказы.

Очевидно, что это серьезные проблемы, которые могут повлиять на процветание вашего бизнеса. Вот здесь-то и появляется SNMP. Вместо того чтобы ждать, пока кто-то заметит неполадку и найдет человека, ответственного за решение проблемы (что может затянуться до утра понедельника, если проблема возникла в выходные), SNMP позволяет вам постоянно наблюдать за своей сетью, даже когда вас нет рядом. Например, он заметит, что если количество сбойных пакетов, проходящих через один из интерфейсов вашего маршрутизатора, постепенно растет, то

маршрутизатор, возможно, скоро откажет. Вы можете настроить автоматическое уведомление о ситуациях, когда сбой кажется неизбежным, чтобы иметь возможность исправить маршрутизатор, прежде чем он действительно выйдет из строя. Вы также можете установить отправку уведомления, если отказало устройство обработки кредитных карт, – возможно, вы даже сможете исправить его из дома. И если все пройдет нормально, в понедельник утром вы сможете вернуться в офис, зная, что никаких сюрпризов не будет.

Конечно, устранение проблем до их появления – это незаметный труд, но вы и ваше руководство будете спокойнее спать. Мы не можем сказать вам, как перевести это в более высокую зарплату, – иногда лучше быть тем, кто врывается и все исправляет в самый разгар критической ситуации, чем тем, кто исключает возникновение критических ситуаций. Но SNMP позволяет вам вести журнал регистрации, который доказывает, что ваша сеть работает надежно, и показывает, когда и какие меры вы приняли, чтобы отвести неизбежный кризис.

Советы по набору персонала

Реализация системы управления сетью может означать расширение штата, чтобы справиться с повышенной нагрузкой по поддержке и эксплуатации такой среды. В то же время внедрение мониторинга в большинстве случаев должно снизить нагрузку вашего персонала по системному администрированию. Вам потребуется:

- Персонал для обслуживания станции управления. Сюда входит обеспечение настройки станции управления для правильной обработки событий от устройств, поддерживающих SNMP.
- Персонал для обслуживания устройств, поддерживающих SNMP. Это предполагает обеспечение возможности связи рабочих станций и серверов со станцией управления.
- Персонал по наблюдению за сетью и устранению неисправностей. Обычно эта группа называется центром управления сетью (Network Operations Center – NOC) и работает в режиме 24/7. Альтернатива работе в режиме 24/7 – реализовать попеременное дежурство по вызову, когда один человек все время находится на телефоне, но необязательно присутствует в офисе. Дежурство по вызову подходит только для небольших систем, в которых в случае отказа сети можно подождать, пока кто-то доедет до офиса и устранит проблему.

Невозможно заранее предсказать, сколько сотрудников вам потребуется для поддержки системы управления. Количество персонала будет изменяться в зависимости от размера и сложности управляемой вами сети. В NOC некоторых крупных магистральных интернет-провайдеров работают 70 и более сотрудников, а в других компаниях – только один.

Получение дополнительной информации

Овладение SNMP может показаться непосильной задачей. RFC предоставляют официальное определение протокола, но они были написаны для разработчиков программного обеспечения, а не сетевых администраторов, поэтому последним может быть трудно найти необходимую информацию. К счастью, есть много сетевых ресурсов. Хорошим источником является SimpleWeb (*http://www.simpleweb.org*). Еще один хороший информационный сайт – SNMP Link (*http://www.SNMPLink.org*). *The Simple Times*, сетевое издание, посвященное SNMP и управлению сетями, также полезно. Все вышедшие[1] выпуски можно найти по адресу *http://www.simple-times.org*. SNMP Research – коммерческий поставщик SNMP-продуктов. Помимо коммерческих продвинутых SNMP-решений на веб-сайте компании *http://www.snmp.com* можно найти приличное количество бесплатной информации об SNMP.

Еще один замечательный источник – новости Usenet. Наибольшей популярностью пользуется новостная группа *comp.dcom.net-management*. Еще одна хорошая новостная группа – *comp.protocols.snmp*. Такие группы развивают сообщество обмена информацией, позволяя опытным профессионалам взаимодействовать с теми, кто не так хорошо владеет SNMP или управлением сетями. Прекрасный интерфейс для поиска по новостным группам Usenet есть у Google по адресу *http://groups.google.com*.

Существует SNMP FAQ, доступный в двух частях по адресам *http://www.faqs.org/faqs/snmp-faq/* и *http://www.faqs.org/faqs/snmp-faq/part2/*.

Ряд очень хороших документов по управлению сетями есть у Cisco, в том числе «Network Management Basics» (*http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/nmbasics.htm*) и «Change Management», из которого были взяты рис. 1.2 и 1.3. Кроме того, важный базовый материал для всех, кто изучает управление сетями, представлен в статье Дугласа У. Стивенсона «Network Management: What It Is and What It Isn't», доступной по адресу *http://www.itmweb.com/essay516.htm*.

Итак, здесь были изложены основы, а в главе 2 мы поговорим о SNMP более подробно.

---

[1] На момент написания книги последний выпуск довольно старый, опубликован в декабре 2002 года.

2

SNMPv1 и SNMPv2

В этой главе мы начнем подробное рассмотрение SNMP, в частности разбирая особенности SNMPv1 и SNMPv2 (мы будем периодически упоминать SNMPv3, но более детально его особенности обсудим в главе 3). Прочитав эту главу, вы должны будете понимать, как SNMP отправляет и получает информацию, что такое SNMP-сообщества и как читать файлы MIB. Мы также более подробно рассмотрим три MIB, представленных в главе 1, а именно MIB-II, Host Resources и RMON.

SNMP и UDP

В качестве транспортного протокола для передачи данных SNMP применяет протокол датаграмм пользователя UDP (User Datagram Protocol). UDP, определенному в RFC 768, было отдано предпочтение перед протоколом управления передачей TCP (Transmission Control Protocol), так как UDP – протокол без установления соединения, то есть при передаче датаграмм (пакетов) туда и обратно между агентом и NMS не создается соединения из конца в конец. Из-за этого аспекта UDP является ненадежным, потому что на уровне протокола нет подтверждения доставки датаграмм. SNMP-приложение само определяет, потеряны ли датаграммы, и при необходимости передает их повторно. Обычно это достигается путем простого ожидания в течение определенного интервала времени. NMS отравляет агенту UDP-запрос и ожидает ответа. Интервал времени, в течение которого NMS его ожидает, зависит от ее конфигурации. Если интервал времени ожидания превышен, а NMS не получила от агента ответа, она считает пакет потерянным и повторно передает запрос. Количество повторных передач пакетов также настраивается.