Глава 19. Изменение служб

**Изменение служб**

Перевод пользователей с одной службы на другую – важная задача системных администраторов. Это может потребоваться по разным причинам: устаревание системы, прекращение поддержки, слияние компаний или разделение подразделений. Независимо от ситуации, изменение должно быть максимально плавным и незаметным для пользователей.

**Невидимое изменение**

Успех проекта зависит от минимального вмешательства в работу пользователей. Примером удачного перехода может служить разделение Bell Labs при отделении Lucent от AT&T. Исследователи даже не заметили изменений, что свидетельствует о грамотном планировании и исполнении.

**19.1Основы**

Ключ к успешному переходу – надежная инфраструктура и постепенное внедрение изменений. Начинать лучше с системных администраторов, затем переходить к более широкому кругу пользователей. Важно иметь план отката, чтобы в случае проблем быстро вернуться к предыдущему состоянию.

Автоматизированные системы обновления помогают упростить распространение изменений. Также необходимо заранее информировать пользователей, учитывать их мнения и графики работы. Грамотное планирование всех этапов позволит минимизировать негативное влияние на рабочие процессы.

### Минимизируйте вмешательство

При планировании изменений важно минимизировать их влияние на пользователей. Необходимо тщательно продумать, требует ли переход прерывания работы службы, и как можно сократить время недоступности. Также важно определить, нужно ли изменения на рабочих станциях пользователей и как сделать процесс перехода максимально удобным, чтобы вмешательство происходило только один раз. В случае необходимости изменения клиентского ПО стоит заранее подготовить обучение для пользователей и службу поддержки, чтобы они были готовы к новому программному обеспечению. Стремитесь выполнить переход без прерывания работы и изменения процессов, и обеспечьте поддержку до начала распространения изменений.

### Горизонтально или вертикально

При переходе задачи можно выполнять двумя способами: горизонтально или вертикально. Горизонтальный подход предполагает выполнение одной задачи для всех пользователей перед переходом к следующей, а вертикальный – выполнение всех задач для каждого пользователя по очереди. Задачи, не вмешивающиеся в работу пользователей, например создание учетных записей, можно выполнять горизонтально. Однако задачи, требующие вмешательства, такие как установка нового ПО, должны выполняться вертикально. В вертикальном подходе вмешательства происходят только один раз для каждого пользователя, что снижает количество неудобств.

### Распространение информации

Хотя переход должен быть как можно менее заметным для пользователей, важно заранее информировать их о предстоящих изменениях. Общение с пользователями позволяет выявить непредвиденные способы использования системы и учесть их потребности. Все пользователи, активно использующие систему, должны быть привлечены на раннем этапе проекта. Заранее планируйте все важные сроки, чтобы минимизировать влияние изменений на работу пользователей. Даже если переход проходит незаметно, пользователи должны быть осведомлены о его проведении и возможных последствиях.

### Обучение

Обучение пользователей — важная часть перехода. Если работа пользователей изменится, они должны получить соответствующую подготовку. В большинстве случаев достаточно уведомлений по электронной почте, но при введении новых крупных систем обучение становится критически важным. Чем меньше техническая подготовка пользователей, тем больше внимания нужно уделить обучению.

Обычно системные администраторы не проводят обучение, но могут поддерживать его организацию. Это включает взаимодействие с пользователями, разработчиками и руководством. Важно учитывать технические сложности подготовки учебного класса, такие как настройка оборудования и сетевой безопасности.

### Начинайте с небольших групп

Любое изменение должно вводиться постепенно. Сначала тестируйте новый процесс на собственных системах, исправляя возникающие проблемы. Затем привлекайте коллег-системных администраторов, расширяя тестовую группу. Далее переходите к пользователям, которые готовы столкнуться с возможными сложностями, и постепенно переводите всю компанию. Такой метод снижает риски и позволяет выявить проблемы до массового распространения.

### Мгновенные изменения: делать все сразу

По возможности избегайте одномоментного перехода всей компании на новую систему. Постепенный переход снижает вероятность крупных проблем. Однако иногда изменения необходимо внедрять сразу, и это требует дополнительного оборудования. В таких случаях стоит заранее предусмотреть бюджет на дублирующие ресурсы.

Если технические возможности позволяют, можно использовать параллельную работу старой и новой системы. Это даст пользователям время на адаптацию, возможность вернуться к старой системе при необходимости и сообщить о проблемах. Такой метод часто применяется в телефонных сетях, где после изменения номера некоторое время действует предупреждающее сообщение перед окончательным отключением старого номера.

План отмены

План отмены является важной частью процесса перехода на новую службу. Если новая система работает некорректно, пользователи могут потерять доступ к необходимым инструментам, что повлияет на их работу. Важно иметь возможность быстро вернуть систему в исходное состояние и исправить возможные проблемы. Одним из способов реализации плана отмены является параллельная работа старой и новой системы. Это позволяет быстро переключаться между ними при возникновении проблем. Сбой может проявиться не сразу, поэтому механизмы отмены должны быть готовы работать в течение некоторого времени, пока не будет уверенности в стабильности новой системы. Также необходимо установить заранее время, по истечении которого будет выполнен откат, например, если переход не завершится в течение двух часов рабочего дня.

Тонкости

Мгновенный откат играет важную роль в процессе перехода, позволяя быстро вернуть систему в исходное состояние при возникновении ошибок. Для этого можно перенаправлять трафик через DNS, чтобы быстро переключаться между старой и новой системой, либо использовать несколько версий программного обеспечения, переключая их с помощью символических ссылок. Хорошее планирование позволяет избежать частых изменений, например, выбор продуктов, которые легко масштабируются, чтобы избежать необходимости их обновления в будущем. Важно также использовать инфраструктурные методы, такие как автоматическая сетевая конфигурация и документация, чтобы избежать изменений в пользовательских конфигурациях при перемещении служб.

Изменения веб-служб

С каждым годом все больше служб становятся веб-службами. В таких случаях обновление сервера редко требует обновления клиентского программного обеспечения, так как служба работает через веб-браузер. Однако многие веб-службы до сих пор поддерживают только определённые браузеры, что является неудачным решением. Службы должны поддерживать работу с любыми браузерами, позволяя пользователю подключаться через различные устройства, такие как мобильные телефоны, игровые консоли или даже умные устройства. В случае использования неподдерживаемого браузера служба должна корректно снижать функциональность, не отказывая в доступе.

Поддержка разработчиков

При внедрении масштабных изменений важно заручиться поддержкой разработчика. Стоит заранее обсудить возможные препятствия, что позволит избежать крупных проблем. Хорошие отношения с разработчиком могут помочь в процессе планирования и даже в предоставлении дополнительной технической поддержки. Если такие отношения не налажены, стоит позаботиться о связи с технической поддержкой, которая может помочь в случае возникновения проблем. Рекомендуется заранее поделиться своими планами с разработчиком, чтобы он был лучше подготовлен к любым вопросам или проблемам, которые могут возникнуть во время перехода.

Заключение

Успешный переход в проекте требует тщательного планирования и надёжной инфраструктуры. Основной целью является минимизация воздействия изменений на пользователей. Переход должен быть плавным и безболезненным для работы пользователей. Ключевые принципы перехода — это хорошее планирование, постепенное внедрение изменений с проверками и готовность к отмене изменений в случае необходимости.

Глава 20. Технические перерывы

Если бы вам пришлось отключить целый вычислительный центр для масштабного технического обслуживания, смогли бы вы справиться с этим? Некоторые компании проводят такие мероприятия регулярно, чтобы минимизировать воздействие на пользователей. Системные администраторы часто откладывают задачи, которые требуют прерывания обслуживания, такие как модернизация оборудования или изменения в сети, до таких перерывов. Это может быть необходимо также из-за технических мероприятий, таких как строительство или аварии.

Процесс управления техническими перерывами требует тщательного планирования, четкого исполнения и обширного тестирования. Важные изменения в системах, как очистка системы охлаждения или реорганизация данных, можно выполнить эффективно, если обеспечить согласие всех пользователей на длительный перерыв в работе. Подход руководителя полета, по аналогии с руководством при запуске космических аппаратов, включает планирование до перерыва, выполнение работ во время перерыва и действия после него.

В некоторых компаниях регулярные технические перерывы используются для обслуживания критических систем и сетей, что повышает их доступность в обычное время. Это может быть перерыв вечером или ночью раз в месяц или в конце недели раз в квартал. Системные администраторы часто предпочитают отключать все системы для упрощения обслуживания и тестирования, например, при переводе почтовых серверов на новую систему.

Однако необходимо учитывать выгоду для компании, а не только для удобства системных администраторов. Заблаговременное планирование и обеспечение высокой доступности служб в оставшееся время крайне важны. Также стоит разработать метрики для оценки доступности систем до и после запланированных технических перерывов.

20.1. Основы

Технический перерыв — это короткий промежуток времени, в течение которого выполняется большое количество работ по обслуживанию систем. Этот процесс неудобен для всей компании, и его время должно быть согласовано с пользователями. Группа системных администраторов выполняет различные задачи, и эта работа координируется руководителем полета.

Основы успешного выполнения технического перерыва включают координацию времени перерыва, создание общего плана, организацию подготовительных работ, общение с пользователями и выполнение тестов после завершения работы. В этой главе рассматривается роль руководителя полета и механизмы обеспечения работы во время перерыва.

20.1.1. Планирование времени

При планировании технических перерывов необходимо согласовывать даты с компанией. Важно избегать дней в конце месяца, квартала и финансового года, чтобы не нарушить работу группы продаж и бухгалтерии. Также нужно учитывать сезонные ограничения в разных отраслях. Желательно заранее опубликовать график перерывов, чтобы сотрудники компании могли планировать свою деятельность с учетом этих дат.

20.1.2. Планирование

Задачи должны планироваться системными администраторами, чтобы избежать нестандартных решений или проблем во время перерыва. Поскольку технические перерывы происходят редко, системные администраторы должны заблаговременно планировать задачи с достаточным запасом времени, чтобы успеть оформить заказы и получить оборудование, необходимое для работы. Планирование следующего перерыва должно начинаться сразу после завершения предыдущего.

20.1.3. Руководство

Руководитель полета отвечает за создание и рассылку объявлений, планирование запросов на выполнение работ, принятие решений о отключениях, мониторинг выполнения задач и сообщение о состоянии дел в конце перерыва. Руководитель полета должен быть старшим системным администратором, способным оценить предложения и увидеть зависимости, которые могут быть упущены. Этот человек не выполняет техническую работу во время перерыва, но координирует работу остальных членов группы.

В зависимости от структуры группы системных администраторов можно выделить нескольких руководителей полета, которые будут поочередно выполнять эту роль. Важно также учитывать личные качества руководителя полета, такие как способность соблюдать сроки, принимать решения в условиях давления и поддерживать нужный уровень ответственности.

20.1.4. Управление предложениями изменений

Все предложения изменений должны быть поданы за неделю до технического перерыва. Эффективным методом управления этим процессом является использование области с контролем версий, где каждый системный администратор редактирует документы в своей директории. За неделю до перерыва эта область блокируется, и все последующие изменения могут быть внесены только через руководителя полета.

Форма предложения изменения должна отвечать на следующие вопросы:

1. **Какие изменения планируется внести?**
2. **На каких машинах вы будете работать?**
3. **Какие условия должны быть выполнены до технического перерыва и какие сроки их выполнения?**
4. **Что должно работать, чтобы изменение было успешным?**
5. **Что будет затронуто изменением?**
6. **Кто выполняет работу?**
7. **Сколько времени займет изменение, включая тестирование, и сколько помощников нужно?**
8. **Каковы процедуры тестирования? Какое оборудование для них требуется?**
9. **Какова процедура отмены и сколько времени она займет?**

### Пример 1: Обновление программы сервера аутентификации SecurID

* **Изменение:** Обновление программы с версии 1.4 до 2.1.
* **Машины:** tsunayoshi и shingen.
* **Условия до перерыва:** Программа и лицензионные ключи должны быть доставлены к 14 сентября. Резервные копии должны быть сделаны в последний вечер перед перерывом.
* **Зависимости:** Сеть, служба командной строки, службы внутренней аутентификации (NIS).
* **Затронутые системы:** Удаленный доступ и защищенные области, требующие аутентификации.
* **Время работы:** 3 ч работы, 3 ч выделено.
* **Ответственный:** Джейн Смит.
* **Тестирование:** Проверка VPN-соединения, создание и удаление пользователей, изменение атрибутов.
* **Оборудование:** Ноутбук с модемом и программой VPN, аналоговая линия, ISDN-модем.
* **Процедура отмены:** Установка новой программы в параллельную директорию, копирование базы данных и изменение ссылок на старую программу.

### Пример 2: Перемещение директорий

* **Изменение:** Перемещение /home/de105 и /db/gene237 с anaconda на anachronism.
* **Машины:** anaconda, anachronism и shingen.
* **Условия до перерыва:** Диски для anachronism должны быть доставлены до 17 сентября и установлены к 21 сентября. Резервные копии должны быть сделаны в последний вечер перед перерывом.
* **Зависимости:** Сеть, служба командной строки, NIS.
* **Затронутые системы:** Сетевой трафик, учетные записи с домашними директориями в /home/de105.
* **Время работы:** 1 ч работы, 12 ч выделено.
* **Ответственный:** Грег Джонс.
* **Тестирование:** Подключение к директориям, создание базы данных, запуск тестов доступа.
* **Оборудование:** Доступ к узлу, не принадлежащему системному администратору.
* **Процедура отмены:** Удаление старых данных после успешного тестирования, восстановление старых директорий.

20.1.5. Разработка общего плана

За неделю до технического перерыва руководитель полета блокирует предложения изменений и начинает разрабатывать общий план. Этот план должен учитывать все условия, сроки и требования, а также время работы и тестирования. В результате составляется набор таблиц, где указывается, кто какую задачу выполняет и в какое время. Все задачи, исполнители, руководители и взаимосвязи должны быть четко определены.

Если предложений изменений слишком много, могут возникнуть конфликты, связанные с доступностью машин или необходимым персоналом. В таких случаях может понадобиться резервное время для решения непредвиденных проблем. Руководитель полета должен заранее принимать решения о приоритетах и помогать выбрать наиболее важные проекты для компании.

**20.1.6. Отключение доступа**

Первая задача в ходе технического перерыва — это отключение доступа к системе и уведомление всех пользователей о том, что перерыв начался. В зависимости от масштаба и возможностей компании этот процесс может включать:

* Размещение заметных объявлений на входных дверях комплекса зданий, с указанием времени начала и окончания технического перерыва.
* Отключение всех форм удаленного доступа, таких как VPN, модемные пулы, выделенные линии или беспроводной доступ.
* Объявление по системе оповещения комплекса зданий, напоминая всем сотрудникам, что системы будут отключены в ближайшее время.
* Изменение сообщения в голосовой почте службы поддержки с информацией о техническом перерыве и времени восстановления нормальной работы.

Эти меры помогут минимизировать попытки доступа к системе во время перерыва, что может привести к потере или повреждению данных, а также сократить вероятность того, что сотрудники службы поддержки будут получать запросы о недоступности системы.

Перед началом технического перерыва рекомендуется проверить консольные серверы и другие системы, которые будут использоваться во время перерыва. Эти средства могут не использоваться часто, и их неисправность может остаться незамеченной. Важно убедиться, что все системы работают должным образом до начала перерыва, чтобы избежать проблем во время его проведения.

**20.1.7. Обеспечение механизмов и координации**

Для успешного проведения технического перерыва критически важна координация и использование ключевых технологий. Важными аспектами являются:

**20.1.7.1. Последовательность отключения/загрузки**

Во время перерыва важно правильно планировать порядок отключения и загрузки систем, чтобы избежать проблем с зависшими машинами или некорректной работой. Некоторые системы или серверы могут зависеть от других, и их отключение или загрузка должны происходить в определенной последовательности. Например:

* Машины, которые пытаются загрузиться, когда нужные службы или серверы недоступны, могут не загрузиться корректно. Это может привести к зависанию системы или проблемам с запуском программ.
* При отключении серверов важно, чтобы они могли правильно завершить соединение с необходимыми ресурсами, такими как файловые серверы, базы данных или серверы лицензий. Если связь с ними будет потеряна, процесс отключения может затянуться.

Важно понимать взаимосвязи между машинами, чтобы избежать сбоев в процессе отключения. Например, наиболее важные системы, такие как серверы аутентификации, серверы приложений и данные, должны загружаться до вычислительных серверов и рабочих станций. Это обеспечит корректное завершение всех процессов.

Каждая система должна быть загружена в правильном порядке, начиная с самых критичных (например, серверы аутентификации и лицензий) и заканчивая менее важными системами. Также стоит учитывать взаимосвязи между критически важными серверами и правильно формировать список последовательности загрузки всех машин.

**20.1.7.2. КВМ и служба консоли**

Для эффективного управления вычислительным центром во время технических перерывов полезными могут быть следующие устройства:

* **Коммутатор КВМ (Keyboard, Video, Mouse)**: Этот коммутатор позволяет нескольким компьютерам использовать одну клавиатуру, монитор и мышь. Он экономит место в серверных, упрощая доступ к консоли. Некоторые более сложные системы КВМ позволяют удаленный доступ из любой точки сети, что особенно полезно во время технических перерывов.
* **Последовательный консольный сервер**: Это устройство подключает различные системы без видеовыхода (например, маршрутизаторы, коммутаторы или UNIX-серверы) к центральному серверу, который может управлять несколькими последовательными входами. Это позволяет удаленно подключаться к консольным интерфейсам этих устройств. Все оборудование, поддерживающее последовательные консоли, должно быть подключено к консольному концентратору (например, терминальному серверу).

Использование этих устройств помогает избежать физической перегрузки серверных и повышает удобство работы, так как системные администраторы могут работать из своих рабочих мест. Это также позволяет уменьшить затраты на дополнительные мониторы, электричество и охлаждение.

**20.1.7.3. Радиостанции**

Во время технических перерывов, когда работа требует координации большого числа операций и взаимодействия между различными группами, системные администраторы должны иметь возможность быстро обмениваться информацией. Важно, чтобы они могли своевременно сообщать руководителю о выполнении задач и убедиться, что предыдущие этапы завершены, прежде чем переходить к следующему.

Для этой цели рекомендуется использовать **портативные радиостанции**, которые позволяют быстрее наладить связь между членами команды. Радиостанции особенно полезны, так как они не требуют оплаты за разговоры, работают в условиях ограниченного покрытия и имеют возможность переключаться между несколькими каналами. Важно, чтобы такие радиостанции имели дальность действия, подходящую для размеров вашего комплекса зданий.

* **Радиосвязь прямой видимости** обычно работает на расстоянии до 25 км, в зависимости от ландшафта и зданий.
* **Ретрансляторы** могут увеличивать дальность связи, особенно если передача сигнала блокируется природными или искусственными препятствиями, такими как горы или высокие здания.

При использовании радиостанций важно помнить о безопасности: не стоит передавать важную информацию, такую как пароли, по рациям, сотовым телефонам или пейджерам, так как это может быть подслушано.

Если вам нужно использовать ретрансляторы для увеличения дальности, важно убедиться, что установка будет соответствовать местному законодательству, особенно если потребуется лицензия радиолюбителя для эксплуатации такого оборудования.

**20.1.8. Предельные сроки завершения изменения**

Руководитель полета играет критическую роль в управлении процессом выполнения задач во время технического перерыва. Он отслеживает прогресс и принимает решения о том, когда нужно завершить задачу или перейти к ее отмене.

* Для задач, не зависящих от других, в случае технического перерыва, проводимого в выходные, предельный срок завершения может быть установлен на 23:00 в субботу, за вычетом времени, необходимого для отмены задачи.
* Важно учитывать уровень усталости и производительности группы. Если сотрудники перегружены, можно дать им перерыв или заранее начать выполнение плана отмены, если они не смогут продолжить эффективно.
* Когда одна задача зависит от другой, особенно важно заранее определить критические временные границы. Например, проблемы с обновлением консольного сервера могут повлиять на другие задачи, такие как перемещение больших файлов. Задержки на одной задаче могут вызвать цепную реакцию, которая потребует решения только во время следующего перерыва.

**20.1.9. Полное тестирование системы**

После завершения технического перерыва проводится полное тестирование системы, чтобы убедиться в ее работоспособности.

* **Начало тестирования**: Все машины в вычислительном центре отключаются, после чего следует последовательность загрузки.
  + Каждому системному администратору назначается ответственность за отключение и загрузку отдельных машин. После завершения каждого этапа руководитель полета объявляет следующий.
  + Если на каком-то этапе возникают проблемы, процесс приостанавливается, пока неисправности не будут устранены.
* **Группы системных администраторов**:
  + После завершения загрузки машины разделяются на группы, каждая из которых отвечает за тестирование в определенной области.
  + Группы выполняют перезагрузку машин, проверку сервисов и приложений, чтобы удостовериться в правильности работы.
  + В процессе тестирования используется система цветных наклеек, чтобы отметить исправные и проблемные машины.
  + После завершения своей работы группа помогает другим, переходя к следующей области.
* **Решение проблем**:
  + Руководитель полета и старшие администраторы отслеживают возникшие проблемы и назначают ответственных за их устранение.
  + В идеале тестирование должно быть завершено к воскресенью днем, чтобы дать возможность системным администраторам отдохнуть перед началом следующей недели.

**20.1.10. Общение после обслуживания**

После завершения работ по техническому обслуживанию и тестированию системы, руководитель полета должен отправить информационное сообщение по компании, сообщая о восстановлении работоспособности всех сервисов.

* Сообщение должно включать:
  + Краткое описание выполненных задач.
  + Список служб, которые все еще не работают, с указанием времени, когда они будут исправлены.
* Это сообщение должно быть подготовлено заранее, чтобы избежать ошибок и усталости руководителя полета в конце напряженных выходных.

### 20.1.11. Возобновите удаленный доступ

После завершения технического перерыва важно вернуть удаленный доступ и восстановить сообщение на автоответчике службы поддержки в нормальное состояние. Это действие следует включить в общий план, а также в индивидуальные планы ответственных сотрудников. Очень важно не забыть о данном шаге, так как его нельзя исправить удаленно, если удаленный доступ был отключен. Это должно стать последним действием перед уходом из здания, чтобы обеспечить нормальную работу после завершения перерыва.

### 20.1.12. Будьте на виду следующим утром

После завершения технического перерыва вся группа системных администраторов должна прийти на работу рано на следующий день и быть на виду в компании. Это важно, чтобы показать готовность к решению возможных проблем. В идеале все должны носить футболки с логотипом компании или группы, чтобы сотрудники сразу видели, кто ответственен за решение технических проблем.

Руководитель полета и старшие системные администраторы должны находиться в помещении службы поддержки, отслеживая звонки и выявляя проблемы, которые могут быть связаны с перерывом. Это помогает быстро обнаружить и устранить проблемы, не прибегая к помощи обычного персонала службы поддержки.

Визуальное присутствие этих сотрудников после технического перерыва символизирует готовность решать проблемы и позволяет быстро исправить все неисправности, поскольку нужные специалисты уже на месте.

### 20.1.13. Обсуждение итогов

Приблизительно к обеду следующего дня после технического перерыва следует обсудить оставшиеся проблемы. Руководитель полета и старшие системные администраторы должны собраться для анализа того, что прошло не так, почему это произошло и как можно улучшить процесс. Это обсуждение помогает выявить ошибки, такие как чрезмерная нагрузка, недостаточная предварительная подготовка или недооценка времени, необходимого для выполнения различных задач.

Обсуждение итогов помогает улучшать проведение технических перерывов, делая их более эффективными и менее стрессовыми.

### 20.2. Тонкости

Для повышения эффективности технических перерывов полезно учитывать некоторые тонкости:

#### 20.2.1. Обучение нового руководителя полета

Обучение новых руководителей полета важно для обеспечения преемственности. Новый руководитель может заранее ознакомиться с планом и учиться у текущего руководителя. Обучаемый руководитель полета может создать первый набросок плана, обсудить его с наставником и внести изменения в зависимости от выявленных взаимосвязей и нужд.

#### 20.2.2. Анализ тенденций в данных истории

Полезно анализировать данные с предыдущих технических перерывов, чтобы улучшить планирование будущих. Это включает в себя отслеживание времени выполнения различных задач, таких как перемещение данных между машинами или обновление программного обеспечения, и использование этих данных для более точного прогнозирования времени на выполнение таких задач в будущем.

Анализ тенденций помогает новым сотрудникам быстро адаптироваться и учитывать возможные сложности при планировании. Важно записывать фактическое время выполнения задач, чтобы использовать эту информацию для улучшения процесса в дальнейшем.

**20.2.3. Предоставление ограниченной доступности**  
На некоторых этапах может возникнуть необходимость поддерживать доступность служб для определенной группы пользователей во время технического перерыва. Это может быть связано с непредвиденными ошибками или изменением графика работы, например, переходом на круглосуточное обслуживание. Для этого может потребоваться изменение архитектуры службы или добавление уровней избыточности.

**20.2.4. Компании высокой доступности**  
Компании, которые требуют высокой доступности, не могут позволить себе крупные запланированные отключения и должны обеспечить наличие избыточных систем. Чем выше требования по доступности, тем больше систем требуется для обеспечения бесперебойной работы. Высокая доступность достигается через множество избыточных компонентов.

**20.2.4.1. Сходства с другими компаниями**  
Большинство принципов проведения технических перерывов актуальны для компаний высокой доступности. Эти компании должны планировать перерывы так, чтобы они минимально влияло на пользователей. Важным аспектом является предварительное информирование клиентов и быстрое выполнение всех работ. Для эффективного управления перерывами необходим руководитель, координирующий задачи и следящий за соблюдением сроков.

**20.2.4.2. Различия**  
Технические перерывы в компаниях высокой доступности имеют несколько отличий. Они требуют наличия избыточных систем и не предполагают полного отключения доступа, так как службы должны оставаться доступными. Также нет необходимости в полном списке отключений/перезагрузок, но при наличии зависимостей между машинами требуется учитывать эти зависимости. Физическая доступность на следующий день не критична, но важно обеспечить видимость и помощь пользователям. После обслуживания не требуется массовая рассылка сообщений, если нет оставшихся проблем. Главное отличие – учет избыточной архитектуры при планировании перерыва, чтобы работа службы не была нарушена.

**20.3. Заключение**  
Основные аспекты успешного проведения технического перерыва — это подготовка, выполнение и работа с пользователями после завершения работ. Заблаговременная подготовка, правильное планирование и выполнение большинства работ заранее способствуют успешному проведению перерыва. Назначение руководителя для координации действий и создание общего плана являются важными шагами. Во время перерыва важна инфраструктура, такая как консольные серверы и радиосвязь. Хорошая работа с пользователями после перерыва и распространение информации о проведенных изменениях также играют важную роль. Правильное планирование и тестирование системы помогут предотвратить проблемы.

**Глава 21. Централизация и децентрализация**  
Эта глава помогает системным администраторам определить, какая степень централизации подходит для конкретной компании или службы, а также как изменять степень централизации. Централизация означает наличие единой точки управления, где различные элементы компании контролируются одним объектом, в то время как децентрализация распределяет контроль по нескольким элементам. Примером может служить распределение контроля за DNS-серверами в разных подразделениях.

Централизация направлена на повышение эффективности через экономию масштаба и снижение ошибок, а децентрализация улучшает гибкость и скорость за счет локализации контроля. Оба подхода имеют свои преимущества в разных ситуациях и могут быть реализованы с элементами другого подхода.

Централизация помогает организовать порядок и снизить избыточность, делая процессы более эффективными, например, через внедрение централизованных систем для обработки данных. В то же время, новые технологии могут обеспечить как централизацию, так и высокую степень местной автономии.

**21.1. Основы**  
Организации часто меняют степень централизации и децентрализации в зависимости от внутренних изменений, слияний или расширения, особенно в крупных компаниях. В этом разделе рассматриваются принципы, которые следует учитывать при проведении таких изменений, а также примеры служб, которые могут быть кандидатами для централизации или децентрализации.

**21.1.1. Руководящие принципы**  
При решении о централизации или децентрализации следует учитывать несколько принципов, аналогичных тем, что применяются при любых крупных структурных изменениях:

1. **Решение проблем:** Четко определите, какую проблему вы хотите решить. Например, проблемы с нестабильной системой, если каждое подразделение использует оборудование разных марок, или с отказами служб при отключении сетевых соединений с офисами. Важно не потерять цель из виду в процессе работы над проектом.
2. **Мотивация:** Понимание своей мотивации для внесения изменений важно для правильного управления процессом. Будьте честны с собой о том, почему вы решаете провести централизацию или децентрализацию: возможно, вы хотите сэкономить деньги, улучшить скорость или гибкость, или просто улучшить рабочие процессы.
3. **Опыт имеет значение:** Используйте здравый смысл и опыт. Например, опыт показал, что для малых компаний достаточно одного сервера электронной почты на несколько отделов, в то время как для крупных компаний требуется больше серверов, а для очень крупных — отдельные шлюзы.
4. **Участие:** Прислушивайтесь к мнению пользователей, чтобы понимать их ожидания. Не всегда то, что они просят, можно реализовать напрямую, но важно понять принципы их запросов и сохранить их в новой системе.
5. **Будьте реалистом:** Избегайте нереальных обещаний. Например, будьте осторожны с утверждениями, что централизация или децентрализация легко решат все проблемы. Также важно помнить, что продукт может не решить проблему, если сама структура организации требует изменений.
6. **Баланс:** Найдите оптимальный баланс между централизацией и децентрализацией с учетом текущих потребностей и перспектив. Например, если компания планирует расти, важно строить систему, которая будет масштабироваться в будущем.
7. **Доступ:** Чем больше система централизована, тем выше вероятность, что потребуются индивидуальные настройки для некоторых пользователей. Найдите способы обеспечить гибкость, чтобы удовлетворить различные потребности пользователей.
8. **Отсутствие давления:** Проекты по централизации и децентрализации требуют внимательной координации и планирования, подобно запуску новой службы. Успех зависит от понимания потребностей пользователей и четкого планирования.
9. **110%:** Уделите внимание первому впечатлению от новой системы. Сделайте все правильно с первого раза, даже если это потребует больше времени или денег на тестирование. Хорошее начало поможет создать доверие к системе.
10. **Право вето:** Слушайте пользователей, но учитывайте решения руководства. Иногда для успешной централизации необходима поддержка руководства, а без этого изменения могут стать невозможными.

21.1.2. Кандидатуры для централизации

Системные администраторы ищут способы централизации процессов и служб для достижения экономии масштаба и повышения эффективности через стандартизацию. Централизация помогает снизить накладные расходы, делая управление более простым и эффективным. Однако она может вызвать сопротивление у сотрудников, которые теряют контроль. Важно заранее учитывать психологическую реакцию и способы убедить сотрудников, что новая система будет лучше.

Для централизации подходящими кандидатурами являются:

1. **Распределенные системы**: Например, веб-серверы могут быть централизованы для обеспечения единообразной конфигурации и улучшения безопасности. Это также позволяет снизить потребность в высококвалифицированных специалистах и упростить управление.
2. **Консолидация служб**: Объединение служб на меньшем количестве узлов снижает эксплуатационные расходы, такие как потребление энергии и охлаждение. Мотивация заключается в снижении стоимости и улучшении эксплуатации через объединение служб на более мощных машинах.
3. **Консолидация хранилищ информации**: Переход на Storage Area Network (SAN) для хранения данных улучшает производительность и надежность за счет более эффективного использования ресурсов.

21.1.3. Кандидатуры для децентрализации

Децентрализация не всегда автоматически снижает время реакции, но при правильной организации она может создать предпосылки для этого. Люди часто более терпимы к неэффективным процессам, если чувствуют, что они под контролем. Децентрализация жертвует эффективностью ради других ценностей, таких как демократизация контроля, устойчивость к ошибкам, создание индивидуальных решений и отделение от центральных органов.

Подходящие кандидатуры для децентрализации:

1. **Устойчивость к отказам**: Дублирование работы помогает устранить одиночные точки отказа, что повышает надежность. Например, установка локальных серверов электронной почты в разных местах позволяет пользователям иметь доступ к почте даже при отключении сети.
2. **Индивидуализация**: Некоторые группы пользователей требуют доступа к новейшим технологиям, чтобы поддерживать конкурентоспособность. В таких случаях можно создать специализированные подразделения системных администраторов, которые могут работать с технологиями, отличающимися от корпоративных стандартов, обеспечивая гибкость и инновации.
3. **Удовлетворение потребностей пользователей**: Иногда централизованные службы не могут удовлетворить все требования пользователей, и в этом случае может понадобиться децентрализация. Важно понимать причину неудовлетворенности и совместно искать решение, которое устроит как пользователей, так и системных администраторов.

Децентрализация может привести к множеству точек отказа, распределенных по компании, что снижает избыточность. Однако правильно организованная централизация, наоборот, может повысить устойчивость за счет профессионализма и выполнения стандартов, таких как SLA. Также разнообразие систем (например, разных операционных систем) может быть преимуществом, так как это снижает риски, связанные с безопасностью.

21.2. Тонкости

Переход к централизованной или децентрализованной системе часто требует серьезной перестройки. Если вы просите людей потерпеть временные неудобства из-за перехода на новую систему, то необходимо предложить решение, которое не только дешевле, но и лучше для них.

**Пример: Объединение закупок**

В этом примере централизованная закупка привела к более быстрой доставке лучших продуктов за меньшие деньги. Группа системных администраторов смогла контролировать все закупки, что позволило им заблаговременно взаимодействовать с пользователями, выясняя их специфические требования. Это помогло избежать неожиданных требований на этапе реализации крупных проектов.

Основные преимущества централизованных закупок:

1. **Лучшее управление активами**: Все закупки отслеживаются через одну систему, и теперь есть единое место для хранения серийных номеров оборудования. Это обеспечило лучшую управляемость активами и позволило избегать потерь из-за несогласованности.
2. **Оптовые скидки**: Центральная закупка позволила получать скидки при заказе большого объема продукции, что снижало расходы.
3. **Снижение времени ожидания**: Ранее процесс доставки компьютеров занимал несколько недель, включая время на сборку и установку ОС. Централизованная система закупок позволила значительно сократить это время, установив стандартные конфигурации, которые можно было быстро развернуть.
4. **Привлекательность стандарта**: Несмотря на стандартизацию, группа закупок предложила конфигурации, которые были достаточно мощными и качественными, чтобы удовлетворить потребности большинства пользователей, что снизило желание заказывать индивидуальные конфигурации.
5. **Ускоренная доставка**: Время на получение нового компьютера сократилось с 6 недель до 6 минут. Это повысило моральный дух сотрудников и повысило эффективность компании.

Таким образом, централизованные закупки с правильно спланированными процессами и выгодными стандартами могут значительно повысить эффективность компании, сэкономить время и деньги, а также повысить удовлетворенность пользователей.

21.2.2. Аутсорсинг

Аутсорсинг — это процесс, при котором сторонним компаниям платят за выполнение определенных технических услуг, таких как организация корпоративной поддержки, обслуживание сетей, установка компьютеров и даже создание инфраструктуры для конкретных приложений. Этот процесс часто является формой централизации, направленной на снижение избыточного обслуживания и стандартизацию процессов.

**Преимущества аутсорсинга:**

1. **Снижение внутренних конфликтов**: Привлечение сторонних исполнителей помогает избежать политических конфликтов внутри компании, которые часто мешают достижению высокой эффективности.
2. **Сфокусированность на основном бизнесе**: Аутсорсинг позволяет компании сосредоточиться на своих основных задачах, а не на поддержке технологической инфраструктуры, что часто занимает много времени и ресурсов.
3. **Экономия и стандартизация**: Аутсорсинг может привести к экономии за счет стандартизации процессов и использования лучших практик со стороны сторонних исполнителей.

**Проблемы при аутсорсинге:**

1. **Неопределенность в требованиях**: Проблема возникает, если компании не понимают точно, что им нужно, или не могут точно прописать требования в контракте. Это связано с тем, что сторонний исполнитель обладает большим техническим опытом и может доминировать в переговорах.
2. **Неопытность при экстренных решениях**: Компании часто обращаются к аутсорсингу в экстренных ситуациях, когда их инфраструктура уже находится в плохом состоянии. В такой ситуации компании часто торопятся заключить контракт, что приводит к недостаточной подготовленности и потере контроля над переговорами.
3. **Скрытые расходы**: Аутсорсинговые контракты могут включать скрытые расходы, такие как работы, не включенные в основной объем обязательств. Эти работы выполняются по высоким стандартным расценкам, и компании, часто не оговаривая их, могут столкнуться с дополнительными затратами.

**Рекомендации по аутсорсингу:**

1. **Тщательно прописывайте требования в контракте**: Убедитесь, что контракт включает все этапы жизненного цикла услуг (проектирование, установка, обслуживание и поддержка, вывод из эксплуатации, аварийное восстановление). Важно также предусмотреть санкции за несоответствие требованиям по производительности.
2. **Консультанты по аутсорсингу**: Использование консультантов для переговоров по аутсорсингу может помочь избежать ошибок. Однако стоит выбирать консультантов, которые не имеют финансовых связей с потенциальными исполнителями.
3. **Осторожность с низкими расценками**: Некоторые аутсорсинговые компании могут предложить низкие расценки на проект, чтобы привлечь клиентов, но эти расценки могут скрывать дополнительные расходы на работы, не входящие в контракт.

Аутсорсинг может быть эффективным инструментом для оптимизации процессов и сокращения избыточных затрат, но важно внимательно подходить к его организации и заключению контрактов, чтобы избежать скрытых рисков и дополнительных расходов.

**21.3. Заключение**

Централизация и децентрализация — это сложные концепции, и ни одна из них не является универсально правильным решением. Эти процессы могут быть применены как к техническим задачам, например, администрированию серверов, так и к нетехническим вопросам, таким как организационная структура.

При внесении изменений важно понимать, какую проблему вы хотите решить и что вами движет. Централизация должна происходить только в том случае, если это имеет смысл и приносит пользу на данный момент. Все изменения требуют внимательного и продуманного подхода, и важно всегда прислушиваться к мнению пользователей, для которых эти изменения будут реализованы.

Учиться на опыте других людей, изучая материалы конференций и работы известных экспертов, полезно для успешного внедрения изменений. Централизованные закупки, как показано в примере, могут быть отличным инструментом для контроля расходов, если правильно организовать процесс, не ограничивая выбор людей, а наоборот, помогая им делать покупки более эффективно.

Аутсорсинг, как форма централизации, также становится важной частью системного администрирования. Внешние исполнители могут значительно помочь в оптимизации процессов, и это влияние будет сохраняться долго. В конечном счете, выбор между централизацией и децентрализацией зависит от конкретных условий, и главное — это тщательно анализировать потребности, вовлекать пользователей в процесс изменений и подходить к организации изменений с ответственностью и планированием.

**Глава 22. Мониторинг служб**

Мониторинг является важным элементом обеспечения надежного и профессионального обслуживания. Существует два основных типа мониторинга: мониторинг в реальном времени и исторический мониторинг. Каждый из этих типов имеет свое назначение и применяется в разных случаях. Как говорилось в разделе 5.1.13, мониторинг является ключевым элементом при создании службы и поддержании требуемого уровня обслуживания.

В бизнесе существует аксиома: «Если вы не можете что-то измерить, вы не можете этим управлять». В контексте системного администрирования эта аксиома превращается в: «Если вы не наблюдаете за чем-то, вы не управляете этим». Мониторинг необходим для успешной работы любой компании, однако это может быть проектом, который со временем будет расширяться. Эта глава поможет вам подготовиться к разработке системы мониторинга и улучшению её эффективности.

Для некоторых компаний, например тех, которые предоставляют услуги через Интернет, полный мониторинг является обязательным для нормального функционирования. Такие компании должны следить за всем, чтобы избежать потерь прибыли из-за незамеченных сбоев. Особенно это важно для сайтов электронной коммерции, которые наверняка потребуют реализации мониторинга, как описано в данной главе.

**22.1. Основы**

Мониторинг систем используется для обнаружения и устранения неполадок, определения источников проблем, предотвращения будущих сбоев и предоставления данных о достижениях системных администраторов. Существует два основных способа мониторинга: (1) сбор исторических данных о доступности и использовании систем и (2) мониторинг в реальном времени для оперативного оповещения о сбоях.

Исторический мониторинг используется для записи статистических данных о длительной работе, использовании и производительности систем. Он включает два компонента: сбор данных и их анализ. Результатами исторического мониторинга могут быть, например, такие выводы: «Веб-служба работала в прошлом году 99,99% времени, что выше 99,9% в позапрошлом году». Данные об использовании также важны для планирования ресурсов. Например, график использования пропускной способности канала может показать, что через четыре месяца соединение с Интернетом будет перегружено. Для исторического мониторинга распространены такие системы, как Cricket и Orca.

Мониторинг в реальном времени предупреждает команду системных администраторов о сбоях сразу после их возникновения. Он состоит из двух элементов: мониторинга, который обнаруживает сбой, и предупреждения, которое оповещает кого-то о проблеме. Мониторинг системы имеет смысл только в том случае, если информация о сбое будет передана ответственным лицам. Задача системных администраторов заключается в том, чтобы обнаруживать сбои до того, как они станут заметными для пользователей. Это снижает время простоя и позволяет устранить проблемы до того, как они окажут влияние на пользователей, что создает впечатление высококачественного обслуживания. Примеры популярных систем мониторинга в реальном времени включают Nagios и Big Brother.

Обычно два типа мониторинга осуществляются различными системами. Задачи, выполняемые при каждом типе мониторинга, значительно различаются, и по завершении этой главы вы должны четко понимать их отличия и знать, на что обращать внимание при выборе программ для каждой задачи.

Однако стоит отметить несколько важных предупреждений. Мониторинг использует пропускную способность сети, поэтому необходимо следить за тем, чтобы он не потреблял слишком много ресурсов. Также мониторинг может расходовать процессорные и памятьные ресурсы, что может негативно сказаться на общей производительности системы. Поэтому важно следить за тем, чтобы мониторинг не ухудшал качество обслуживания. Еще одним важным аспектом является безопасность в системах мониторинга.

**22.1.1. Исторический мониторинг**

Системы опроса с заранее заданными интервалами используются для сбора данных об использовании различных компонентов системы и для оценки эффективности работы служб, предоставляемых системой. Эти данные обычно сохраняются и применяются для построения временных графиков производительности, которые помогают выявить или локализовать проблемы, произошедшие в прошлом. В средах с установленными нормами SLA исторический мониторинг используется для наблюдения за выполнением этих норм.

Сбор исторических данных часто требуется для системных администраторов, которым важно узнать, необходимо ли модернизировать сеть, добавить серверу больше памяти или установить более мощный процессор. Также их может интересовать, когда потребуется заказать дополнительные диски для группы, быстро заполняющей дисковое пространство, или когда нужно расширить емкость системы резервного копирования. Для этого администраторы должны собирать данные об использовании системы за определённый период, чтобы выявить тенденции и пики в использовании. Исторические данные также могут применяться для тарификации, обнаружения аномалий или для предоставления отчетности руководству.

Однако хранение исторических данных может занимать большое количество дискового пространства. Для уменьшения объема данных можно применить их сокращение или установить сроки хранения. Сокращение данных означает замену детализированных данных средними значениями. Например, можно собирать данные о пропускной способности каждые 5 минут, но заменять их на средние значения за час, что позволяет сэкономить до 90% места на диске. Обычно подробные данные хранятся в течение недели, а для более старых данных детализация уменьшается до почасовых средних значений.

Установка сроков хранения данных помогает управлять объемом хранимой информации. Например, можно решить, что данные старше двух лет не должны храниться. В качестве альтернативы такие данные могут быть перенесены на съемные носители, такие как DVD или магнитные ленты, если они могут понадобиться в будущем. Однако сокращение данных и установка сроков их хранения влияет на уровень детализации, который вы можете поддерживать. Следует учитывать это соотношение при выборе системы для сбора исторических данных.

Кроме того, необходимо учитывать, как система мониторинга собирает данные. Обычно система, осуществляющая сбор исторических данных, будет опрашивать наблюдаемые системы с регулярными интервалами. Интервал опроса должен быть изменяемым. Механизм опроса должен поддерживать стандартные методы связи, такие как SNMPv2, а также стандартные IP-механизмы, включая эхо-сообщения (ping) и открытие TCP-соединений. Также полезно иметь систему мониторинга, которая фиксирует информацию о задержке, поскольку задержка тесно связана с пользовательским восприятием. Когда служба отвечает медленно, это может восприниматься как отсутствие ответа.

Хорошая система мониторинга должна поддерживать максимальное количество механизмов опроса, предпочтительно позволяя добавлять свои собственные тесты, особенно в сильно индивидуализированных системах. Важно также наличие множества заранее определенных тестов, чтобы избежать необходимости писать их с нуля.

Результаты, которые обычно необходимы от систем исторического мониторинга, включают графики с четкими единицами измерения по каждой оси. Эти графики можно использовать для анализа тенденций использования, а также для выявления неожиданных пиков или провалов в интенсивности использования. Графики помогут прогнозировать, когда потребуется увеличить какой-либо ресурс сети, и послужат полезным инструментом при планировании бюджета, более подробно рассмотренного в главе 34. Также графики могут стать удобной формой документации для передачи информации руководству. Они четко отображают данные и могут служить надежной основой для обоснования запросов на увеличение пропускной способности, памяти, дискового пространства и других ресурсов.

**22.1.2. Мониторинг в реальном времени**

Системы мониторинга в реальном времени предназначены для немедленного уведомления о проблемах, таких как отключение узла, сбой службы или другие неисправности. Эти системы должны обеспечивать постоянное наблюдение за всеми аспектами системы, которые могут указывать на возникновение проблемы. В отличие от исторического мониторинга, который используется для анализа данных в прошлом, мониторинг в реальном времени ориентирован на оперативное реагирование и предотвращение сбоев.

Система мониторинга в реальном времени должна не только опрашивать состояние систем и приложений, но и получать сообщения напрямую от них, если они обнаружат проблему. Это может быть реализовано с использованием стандартных механизмов мониторинга, таких как SNMPv2, эхо-сообщения ICMP, TCP, а также через возможность добавления других форм мониторинга.

Система должна поддерживать отправку уведомлений нескольким получателям через различные каналы связи — например, электронную почту, пейджинговую связь, телефонные звонки или открытие заявок на устранение неисправности. Это важно, так как сообщение, отправленное одному человеку, может не дойти до него из-за проблем с его устройством (например, разряженная батарея на пейджере или телефон был вне зоны действия).

Хранение информации в системе мониторинга в реальном времени ограничено. Обычно система сохраняет предыдущие результаты запросов и время, прошедшее с момента последнего изменения состояния. Иногда сохраняются скользящие средние значения или метки для высоких и низких значений, но объем информации, как правило, минимален. Это отличается от исторического мониторинга, где данные хранятся для анализа на более длительный период.

При выборе системы мониторинга необходимо учитывать два типа мониторинга: **мониторинг доступности** и **мониторинг ресурсов**. Мониторинг доступности ориентирован на обнаружение сбоев узлов, приложений, сетевых устройств и других элементов инфраструктуры. Мониторинг ресурсов, в свою очередь, помогает выявить, когда какие-либо компоненты системы перегружены или приближаются к этому состоянию, например, процессор, память, дисковое пространство, сетевые соединения и другие ресурсы.

Система мониторинга должна быть гибкой, чтобы можно было легко добавлять собственные тестовые модули. Предпочтительно, чтобы система поддерживала одни и те же модули для мониторинга как в реальном времени, так и для исторического мониторинга.

**22.1.2.1. SNMP (Simple Network Management Protocol)**

SNMP — это стандартный протокол для управления сетью, который используется для мониторинга устройств в сети. Протокол позволяет отправлять запросы к устройствам, например маршрутизаторам, и получать информацию о состоянии различных переменных (например, количество переданных байтов по интерфейсу).

Протокол включает два типа пакетов: **GET** (для запроса значения переменной) и **PUT** (для изменения значения переменной). В SNMP также существуют **ловушки** (или прерывания), которые позволяют устройствам отправлять уведомления при изменении состояния переменной.

Однако использование SNMP в сложных сетях может быть проблематичным. Во-первых, протокол имеет сложную структуру, и каждый запрос запрашивает одну переменную. Это может привести к большому количеству запросов, особенно если нужно отслеживать несколько переменных для большого числа устройств. Во-вторых, SNMP имеет проблемы с безопасностью: многие устройства используют стандартные пароли (например, "public" для GET и "private" для PUT), что может быть уязвимостью. Более поздние версии SNMP (v2 и v3) улучшили безопасность, зашифровав пароли, но важно правильно настроить доступ и периодически менять пароли.

Рекомендации для повышения безопасности использования SNMP:

1. **Ограничьте доступ** к SNMP-пакетам только для определённых диапазонов IP-адресов.
2. **Используйте SNMPv3**, когда это возможно, для шифрования паролей.
3. **Меняйте пароли SNMP** раз в год и предусмотрите переходный период.
4. **Автоматизируйте проверку** сетевых устройств на наличие уязвимых паролей.
5. Следите за **бюллетенями безопасности** разработчиков оборудования, чтобы своевременно обновлять настройки и устранять уязвимости.

Эти меры помогут повысить безопасность и эффективность использования SNMP в вашей сети.

**22.1.2.2. Механизм оповещения**

Механизм оповещения в системе мониторинга играет ключевую роль в сообщении о возникших проблемах, требующих вмешательства человека. Даже если система обнаруживает проблему, без надлежащего оповещения администратор не будет вовремя реагировать. Поэтому важно, чтобы механизм оповещения был независим от компонентов, которые находятся под наблюдением. Если система мониторинга не может отправить уведомление о сбое, необходимо пересмотреть структуру механизма оповещения.

Электронная почта является популярным средством оповещения, но не должна быть единственным. Она может быть ненадежной или замедленной. Предупреждения должны быть быстрыми и надежными. Также следует учитывать, что каналы оповещения, такие как беспроводная связь, могут быть подвержены перехвату третьими сторонами, что делает передачу критически важной информации, например, паролей, через такие каналы небезопасной.

Для эффективного мониторинга необходимо разработать политику обработки сообщений, которая будет определять, как и кому отправляются уведомления. Важно ответить на несколько ключевых вопросов:

* Сколько человек получат предупреждения?
* Отправляются ли предупреждения в службу поддержки или ответственным сотрудникам по конкретным компонентам, или в оба места?
* Как координируется работа получателей уведомлений, чтобы избежать дублирования усилий?
* Если проблема не решена в заранее определенный срок, передается ли она на более высокий уровень, и если да, то каким образом?
* Как часто и каким образом вы хотите получать информацию о проблеме?
* Какова степень серьезности каждой проблемы и как это влияет на политику реагирования?

В случае реализации механизма раннего оповещения о проблемах с ресурсами, вам может понадобиться интеграция с системой управления заявками для автоматического открытия тикетов. Например, уведомление будет создавать заявку только в случае, если параметр изменяется с приемлемого на неприемлемое состояние, а не каждый раз, когда он фиксируется как неприемлемый. Также можно настроить обновление существующей заявки, если проблема сохраняется после определенного интервала времени.

Если система мониторинга обнаруживает сбой критически важного компонента, важно, чтобы она непрерывно сообщала об этом дежурному персоналу. В таком случае оповещения должны быть частыми, с обновлениями о том, сколько времени ошибка продолжается.

Система мониторинга должна быть гибкой в плане оповещений и позволять использовать различные механизмы оповещения для разных типов проблем. Это может включать использование нескольких каналов связи, таких как электронная почта, SMS, звонки и т.д.

Кроме того, уведомления должны быть ясными и легко понятными. Предупреждения, которые требуют дополнительных объяснений или обращения к другим источникам информации, не являются достаточно эффективными. Например, вместо сообщения "SNMP запрос на 10.10.10.1 для 1.2.3.4.5.6.7.8.9.10 не прошел", более понятным будет сообщение: "Интерфейс Hssi4/0/0 на маршрутизаторе wan-router-1 не работает". Такие ясные и четкие уведомления помогут быстрее определить проблему и начать ее устранение.

Также важно избегать слишком категоричных заявлений в сообщениях, таких как "Веб-сервер на www-20 не работает", если не уточняется, что он "не отвечает". Это поможет избежать ложных тревог и гарантировать, что администратор будет проверять проблему более тщательно, а не решать, что сервер просто временно не доступен.

**22.1.2.3. Передача на более высокий уровень**

Политика передачи на более высокий уровень является важной частью системы мониторинга и оповещения, и она предписывает, как долго проблема может оставаться без решения, прежде чем будет передана другому человеку, обычно руководителю. Эта политика гарантирует, что даже если человек, получающий предупреждения, находится в отпуске или не реагирует, проблема будет передана на более высокий уровень. Важно описать разные пути передачи для различных типов предупреждений, чтобы избежать задержек и обеспечить оперативное решение.

Пример процедуры передачи показывает, как система может быть настроена с помощью таблиц ответственности, которые распределяют обязанности по различным сотрудникам или группам. Для разных типов служб, таких как электронная почта, веб-сайт, DNS и другие, могут быть настроены отдельные пути передачи, а критически важные системы (например, прокси-сервер генерального директора или веб-сайт электронной коммерции) могут быть перенаправлены быстрее. Такая настройка системы помогает эффективно оповещать соответствующих людей.

Также полезной функцией является возможность подтверждения получения экстренного сообщения. Это предотвращает повторную отправку сообщений и позволяет людям работать над решением проблемы, не получая лишних уведомлений. Подтверждение помогает показать, что работа над проблемой ведется, и временно прекращает поступление уведомлений, что снижает неудобства.

**22.1.2.4. Системы активного мониторинга**

Системы активного мониторинга способны не только обнаружить проблемы, но и активно устранять некоторые из них. Например, если система обнаруживает неисправность порта модема, она может сбросить порт или отключить модем из пула. Однако системы активного мониторинга имеют ограничения. Хотя они реагируют быстрее, чем люди, их возможности ограничены временными мерами. Эти системы могут устранять проблемы только временно, не решая коренную причину.

Важно, чтобы системы активного мониторинга не только устраняли временные проблемы, но и сообщали об этом, открывая заявки для принятия постоянных мер. Системные администраторы должны быть внимательными и не полагаться исключительно на автоматические решения, иначе они рискуют столкнуться с системными сбоями и ухудшением надежности. В конечном итоге важно переходить от временных решений к постоянным, чтобы поддерживать систему в стабильном состоянии.

**22.2. Тонкости**

Когда система мониторинга начнёт расширяться и покрывать большее количество устройств, важно обеспечить доступность этой системы для всех системных администраторов компании. Это позволит каждому администратору обслуживать свои списки устройств и своевременно вносить изменения. Важно также отметить, что со временем могут появиться дополнительные задачи, такие как мониторинг транзакций в полном объёме, а не только проверка работы отдельных компонентов, и обнаружение новых устройств, подключаемых к сети.

**22.2.1. Доступность**

На первых этапах системы мониторинга устанавливаются одним или двумя админами, которые полностью контролируют процесс. Но со временем нагрузка на систему растет, и важно сделать её доступной для всей команды администраторов. Каждый администратор должен иметь возможность самостоятельно добавлять объекты для наблюдения, а не обращаться к тем, кто установил систему. Это повышает гибкость и эффективность.

Обеспечение доступности требует хорошей документации, которая должна описывать:

* Какие данные потребуются для добавления объекта в систему.
* Как эти данные можно найти.
* Как вносить изменения в конфигурацию мониторинга.
* Предпочтительные настройки по умолчанию (например, частота опроса, уровни тревоги, приоритеты проблем).

Таким образом, если система мониторинга требует внесения изменений от одного или двух человек, это создаст неудобства. Без должной доступности система не будет использоваться эффективно, и команда не получит максимальную пользу от её внедрения.

**22.2.2. Тотальный мониторинг**

Идеальная система мониторинга должна охватывать все устройства и службы в компании, особенно в тех организациях, где важна высокая доступность (например, для сайтов электронной коммерции). Когда системы и службы добавляются в мониторинг вручную, есть риск забыть о некоторых объектах. Чтобы избежать этого, добавление новых объектов в список для наблюдения должно быть автоматизированным процессом.

Для этого можно использовать автоматизированную установку новых машин, как описано в главе 3. Когда машины устанавливаются с использованием такого процесса, можно автоматически внести их в систему мониторинга. Кроме того, можно установить на устройства специальное средство, которое при подключении сообщает системе мониторинга, что устройство работает и за ним нужно следить. В идеале процесс установки должен автоматически создавать заявку в службу поддержки для внесения устройства в мониторинг.

**22.2.3. Обнаружение устройств**

Система мониторинга, которая обнаруживает новые устройства, подключаемые к сети, также является полезным инструментом. Это особенно важно для тотального мониторинга, поскольку позволяет обнаружить устройства, которые могли быть пропущены при ручном добавлении в систему.

Кроме того, такой механизм полезен, если устройство вызывает проблемы в сети. Знание того, когда и какое устройство было подключено, может существенно сократить время на отладку и решение проблем.

**22.2.4. Сквозное тестирование**

Сквозное тестирование — это процесс проверки всей транзакции, как если бы её выполнял пользователь, чтобы удостовериться, что транзакция успешно завершена. Это может быть как простая проверка, например отправка письма через почтовый сервер, так и более сложная проверка, такая как имитация покупательского процесса на сайте электронной коммерции.

Пример из практики: в AT&T и Lucent был разработан инструмент для проверки электронной почты (mailping), который отправляет сообщения на почтовые серверы и измеряет время доставки. Это позволяло не только отслеживать скорость доставки сообщений, но и оперативно реагировать на возможные проблемы с почтовыми серверами.

Сквозное тестирование помогает выявить проблемы, которые могут быть не замечены в процессе обычного мониторинга. Например, если транзакция зависит от корректной работы нескольких компонентов (например, почтового сервера), система мониторинга может не обнаружить проблему, если она не настроена на проверку всех этапов транзакции. Имитация действий пользователя, таких как отправка сообщений, проверка статуса оплаты, может выявить ошибки, которые в противном случае были бы обнаружены только после жалоб пользователей.

**22.2.5. Мониторинг времени ответа приложений**

Мониторинг времени ответа приложений является важным аспектом, особенно в среде электронной коммерции и корпоративных приложений. Даже если все компоненты системы работают, высокое время отклика может привести к плохому пользовательскому опыту, потерям в бизнесе или снижению производительности.

Для предотвращения таких ситуаций важно отслеживать время отклика приложения, чтобы убедиться, что оно не превышает установленных порогов. Это может быть дополнением к сквозному тестированию, если тестирование предполагает проверку не только функциональности, но и времени отклика на каждом этапе процесса. Такие данные можно использовать для улучшения производительности и оптимизации работы приложения, а также для создания предупреждений, когда время ответа превышает допустимый предел.

**22.2.6. Расширение**

Когда вы начнете расширять мониторинг на большее количество объектов, столкнетесь с проблемами масштабируемости. При увеличении числа наблюдаемых объектов и частоты сборов данных (например, каждые 5 минут) система может испытывать трудности с обработкой данных, так как каждый новый сеанс может начинаться до того, как предыдущий завершится. Это требует значительных ресурсов, что усложняет работу системы мониторинга.

Примером таких проблем служит опыт WebTV Networks, где при увеличении сети возникли проблемы с производительностью, так как обработка данных требовала слишком много времени. Решением стало использование более эффективной системы — Cricket.

Для улучшения масштабируемости могут быть использованы удаленные зонды, которые собирают данные и отправляют только результаты на центральную станцию. Это снижает нагрузку на сеть и улучшает общую эффективность. В таком подходе главная станция управляет конфигурацией и поддерживает доступ к данным.

Системы мониторинга в реальном времени также сталкиваются с трудностями расширения. Когда количество объектов увеличивается, необходимо эффективно управлять большим количеством предупреждений. Система должна выделять наиболее критичные проблемы, чтобы администраторы могли оперативно реагировать.

Одной из возможных проблем является избыточное количество уведомлений о сбоях, которое может затруднить выявление настоящей причины проблемы. Система должна поддерживать механизм цепочек взаимосвязей, чтобы ошибки одного объекта не приводили к множеству уведомлений.

**22.2.7. Метамониторинг**

Метамониторинг — это мониторинг самой системы мониторинга, что позволяет удостовериться, что она не вышла из строя. Если система мониторинга не присылает уведомлений в течение длительного времени, это может означать, что система сама не работает корректно.

Простой способ реализации метамониторинга — это наблюдение за несколькими внутренними параметрами системы мониторинга, такими как заполняемость диска. Для более крупных систем можно использовать вторичную систему мониторинга, которая отслеживает только работу основной системы.

Метамониторинг также должен быть основан на SLA (соглашении об уровне обслуживания). Например, если система должна обрабатывать запросы каждые 10 минут, метамониторинг должен предупреждать, если это не происходит.

**Заключение**

Мониторинг систем может быть разделен на два типа: исторический и мониторинг в реальном времени. Исторический мониторинг включает сбор данных о доступности и использовании для последующего анализа, в то время как мониторинг в реальном времени фокусируется на немедленном обнаружении и оповещении о проблемах.

Обе формы мониторинга важны для поддержания работоспособности систем, особенно в таких областях, как электронная коммерция, где пользователи могут быстро покинуть сайт, если обнаружат проблемы. Мониторинг в реальном времени помогает быстро обнаружить и устранить проблемы, а исторический мониторинг предоставляет ценную информацию для анализа и прогнозирования.

Однако и тот, и другой тип мониторинга сталкиваются с проблемами масштабируемости. Чтобы решить эти проблемы, важно правильно спроектировать систему мониторинга, включая удаленные сборщики данных, эффективное управление приоритетами и метамониторинг для контроля за состоянием самой системы мониторинга.

Как только система мониторинга развернута, важно интегрировать дополнительные функции, такие как сквозное тестирование и мониторинг времени отклика приложений, чтобы поддерживать качество обслуживания пользователей на высоком уровне.