Использование систем мониторинга для уменьшения числа человеческих ошибок в распределенных серверных залах и удаленных коммутационных узлах

Информационная статья № 103

Версия 0

Автор: Деннис Були

>Краткий обзор

Неожиданные вынужденные простои оборудования серверных залов и удаленных коммутационных узлов становились причиной бессонных ночей для многих ИТ-менеджеров. Многие из них могут рассказать ужасные истории о том, как их серверные залы отключались из-за стечения обстоятельств, ошибки оператора или простой некомпетентности. В данной статье рассматриваются несколько таких инцидентов и содержатся рекомендации об использовании простой системы мониторинга, которая позволяет уменьшить частоту возникновения подобных непредвиденных событий.

Содержание

Щелкните раздел, чтобы перейти к нему

Информационные статьи APC теперь входят в библиотеку информационных статей Schneider Electric, созданную **Научно-исследовательским центром по центрам обработки данных** компании Schneider Electric.
DCSC@Schneider-Electric.com

Schneider Electric

Введение

Многие ИТ-менеджеры могут рассказать о том, как распределенные серверные залы и удаленные коммутационные узлы неожиданно переставали работать. При анализе этих случаев у них обнаруживается одна общая черта — недостаток информации. Недостаток информации ведет к возникновению ошибок операторов, которые становятся причиной простоев. Уровень стресса очень высок, поскольку у операторов и администраторов нет данных, получаемых в режиме реального времени, и поэтому они не имеют возможности предотвратить возникающие ошибки.

Вот два факта:

- Согласно оценкам, только в США имеется 2,9 млн серверных залов и коммутационных узлов[1].
- Более 70 % простоев центров обработки данных связано с человеческими ошибками[2].

В этой статье рассматриваются типичные инциденты, ведущие к незапланированным простоям распределенных серверных залов и удаленных коммутационных узлов. Также предлагаются рекомендации по интеграции программного обеспечения для мониторинга и автоматизации с видеонаблюдением и датчиками для уменьшения числа ведущих к простоям человеческих ошибок в подобных небольших распределенных системах (см. **рисунок 1**).

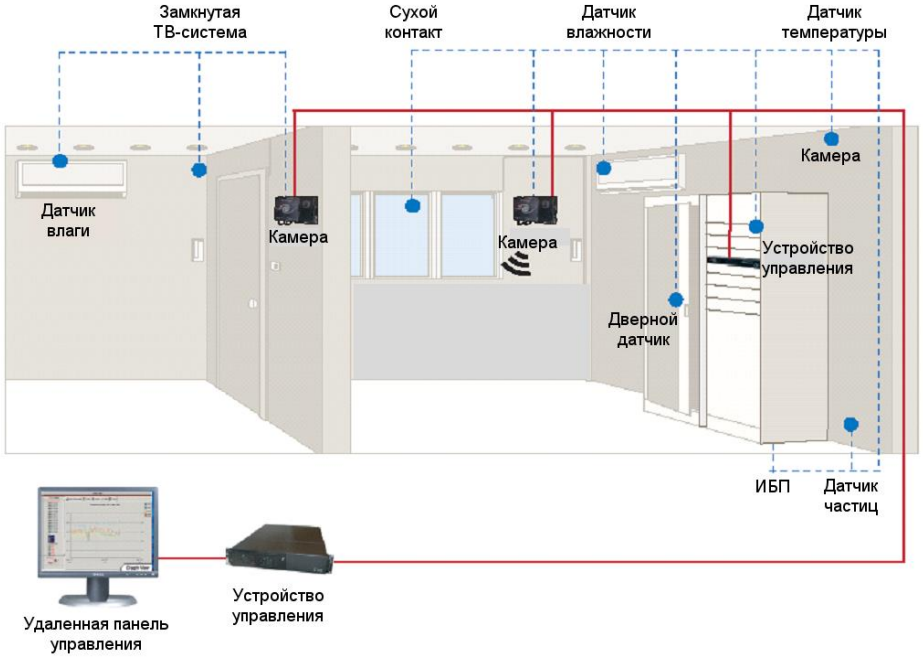


Рисунок 1

Интеллектуальный мониторинг на нескольких уровнях позволяет уменьшить число человеческих ошибок

[1] IDC, *Building, Planning, and Operating the Next-Generation Data Center*, Michelle Bailey, 2008

[2] Uptime Institute, *Data Center Site Infrastructure Tier Standard: Operational Sustainability*, 2010

Просто или сложно?

При рассмотрении вопроса об использовании систем мониторинга в небольших удаленных вычислительных средах, какими являются коммутационные узлы и серверные залы, всегда возникают две проблемы. Первая проблема связана с установкой. Насколько сложно установить систему мониторинга? То есть, сколько времени потребуется для сбора информации о характеристиках устройств, которые необходимо отслеживать, и сколько времени уйдет на ввод этих данных (при использовании сотен устройств на нескольких площадках)? Как система различает камеры, кондиционеры воздуха, ИБП, термодатчики и т.д., и как выдаются IP-адреса, чтобы устройства могли сообщать о своем состоянии? Вторая проблема связана с неясностью относительно объемов работы при изменении конфигурации оборудования для электропитания, охлаждения и мониторинга внешней среды, установленного на удаленной площадке. Например, как выполняется обновление микропрограмм и изменяется пороговое значение температуры?

Развитие программного обеспечения для мониторинга в последние несколько лет привело к ситуации, когда пользователи могут устанавливать его сами или заказать эту услугу на стороне. Привлечение сторонних поставщиков услуг обычно позволяет запустить систему в течение 1-2 дней.

Программное обеспечение для мониторинга может поставляться в виде дистрибутива или загружаемого кода либо в виде сервера для установки в стойку с уже загруженным ПО. Систему можно устанавливать удаленно или в главном центре обработки данных (например, если необходимо управлять несколькими десятками или сотнями коммутационных узлов). После того как сервер управления подключен, можно загрузить на ноутбук программный клиент, позволяющий оператору начать процедуру идентификации оборудования электропитания, охлаждения и мониторинга окружающей среды, а также действий пользователей, которые необходимо отслеживать. Большинство современных ИБП, систем охлаждения и камер наблюдения сразу оборудованы сетевыми картами, которые можно использовать для связи. Оператор задает IP-адрес или диапазон IP-адресов, который будет использоваться контролируемыми устройствами. Пример этого приведен на **рисунке 2**. Некоторые системы затем могут автоматически обследовать сеть и найти все устройства для электропитания, охлаждения и обеспечения безопасности, которые необходимо контролировать. Возможность автообнаружения устройств сильно упрощает установку и запуск системы. Обнаружив удаленные устройства, система начинает следить за ними.

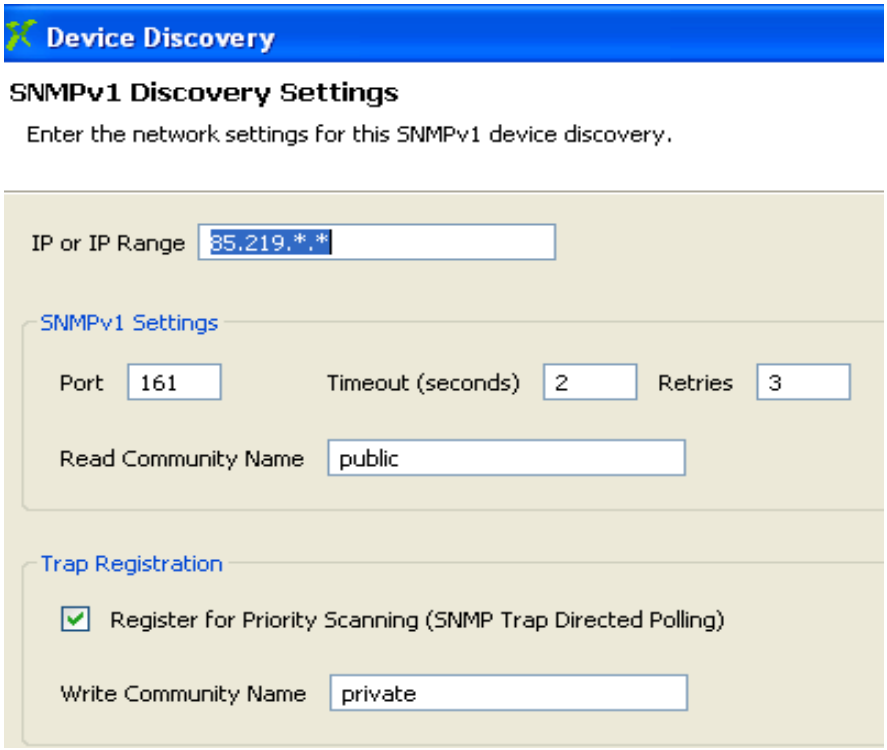


Рисунок 2

Чтобы задать IP-адреса для нескольких устройств, может быть достаточно ввести диапазон цифр (в качестве примера приведен экран приложения Schneider Electric Data Center Expert)

Некоторые системы мониторинга и автоматизации также позволяют группировать устройства по местоположению, по рядам или по типу (например, все устройства охлаждения, все БРП, все камеры и т.д.). Группировка дает пользователю возможность задавать политики и пороговые значения для каждой группы. Общими могут быть такие параметры как температура, влажность и закрытие или открытие (например, дверей шкафов).

При превышении порогового значения срабатывает сигнал тревоги, который передается системному администратору по электронной почте или в виде текстового сообщения. Следует следить за тем, чтобы сигналы тревоги срабатывали только при серьезных изменениях внешней среды. Если это не сделать, администратору будут приходить сигналы тревоги несколько раз в час. В такой ситуации он может стать безразличным к сигналам и начать игнорировать их. Поэтому необходимо найти точный баланс, чтобы каждый поступающий администратору сигнал был значимым и важным.

Наличие современной системы мониторинга также облегчает выполнение обновлений серверного зала или коммутационного узла, например обновлений встроенного ПО. Менеджеру больше не придется отправлять персонал на удаленные объекты для выполнения установки встроенного ПО. Многие системы мониторинга поддерживают возможность массовой настройки, позволяя централизованно рассылать изменения через сеть.

Природа простоев, связанных с человеческими ошибками

В распределенные серверные залы и удаленные коммутационные узлы вкладывается значительно меньше средств, чем в крупные ответственные центры обработки данных, и количество уделяемого им внимания также намного меньше. Крупные централизованные площадки укомплектованы штатом специалистов и зачастую могут похвастать новейшими системами безопасности и большим количеством встроенных резервных элементов. Распределенными серверными залами и удаленными коммутационными узлами обычно занимаются сотрудники, имеющие массу разных обязанностей, одна из

которых — приглядывать за коммутационным узлом или серверным залом. На этих объектах часто реализован лишь минимальный набор мер безопасности, и они подвержены более серьезным отключениям, чем крупные, более совершенные площадки. Как бы хорошо ни был спроектирован серверный зал или коммутационный узел, риск незапланированного простоя всегда имеется. Некоторые ИТ-менеджеры полагают, что они все предусмотрели. Они гордятся тем, как спроектирован их серверный зал. Но затем приходит кажущийся безобидным необученный техник или смотритель и за пять секунд нарушает все планы.

Рисунок 3

Фраза о «потенциальной угрозе» очень уместна для небольших и удаленных серверных залов.

Ниже приведен список происшествий, иллюстрирующий, как отсутствие простых систем мониторинга и автоматизации может привести к незапланированным простоям серверных залов и коммутационных узлов. В этих ситуациях персонал на площадке либо совсем отсутствовал, либо у него не было возможности сообщить системным администраторам о сбое. Обнаружив сбой системы охлаждения на час раньше, порой можно избежать полного отключения системы. Оперативное уведомление в режиме реального времени дает администраторам возможность организовать переключение на другой ресурс при сбое и избежать перебоев в обслуживании.

Непридуманные истории

Рассмотрим ряд происшествий, причиной которых стали человеческие ошибки.

- Системный администратор серверного зала в удаленном офисе приехал, чтобы выяснить причину отключения серверов. Он обнаружил, что ремонтные рабочие на время проведения работ обернули стойки пленкой, чтобы в серверы не попадала пыль. Они не проинформировали о своих действиях ИТ-отдел, поэтому все серверы, которые они обернули, продолжали работать. В результате серверы перегрелись и отключились.
- У высокопоставленного менеджера возникли проблемы с доступом в Интернет, и он захотел решить их самостоятельно. Он пошел в серверный зал, вытащил кабель из маршрутизатора и подключил напрямую к своему ноутбуку. Таким образом он обошел все брандмауэры и службы шифрования, сделав всю систему уязвимой для вирусов и прочего вредоносного ПО.
- При выполнении ремонтных работ сантехник просверлил отверстие в потолке прямо над сервером Exchange. Он также некачественно выполнил соединение труб. Ночью из трубы потекла вода. Она дотекла до дырки в потолке и полилась на стоявший внизу сервер Exchange, полностью выведя его из строя.
- В серверную отправили уборщиков. Они увидели хлопья пыли не только вокруг стоек с серверами, но и внутри. Дверцы стоек при этом были приоткрыты. Убор-

щики сделали свою работу: они помыли стойки и сами серверы изнутри, используя средство для мойки окон. Никто не дал им четких указаний о том, что можно и чего нельзя делать при уборке.

- Подрядчик работал в помещении, оборудованном галоновой системой пожаротушения. Он зажег факел газосварочного аппарата, никого не предупредив и не отключив систему пожаротушения.
- Подрядчик отключил БРП, чтобы поставить в него предохранитель. Этот БРП подавал питание на главный сервер филиала. Многие посетители серверных залов могут не знать, что можно и чего нельзя делать на определенном объекте.

Компоненты системы мониторинга

При разработке системы мониторинга, главная задача которой — уменьшить число человеческих ошибок в удаленных серверных залах, необходимо помнить о четырех ее компонентах: видеонаблюдении, датчиках, интеллектуальных стоечных системах питания и программном обеспечении для мониторинга и автоматизации. В **таблице 1** содержится сводка решений, описанных в данном разделе.

Видеонаблюдение и датчики

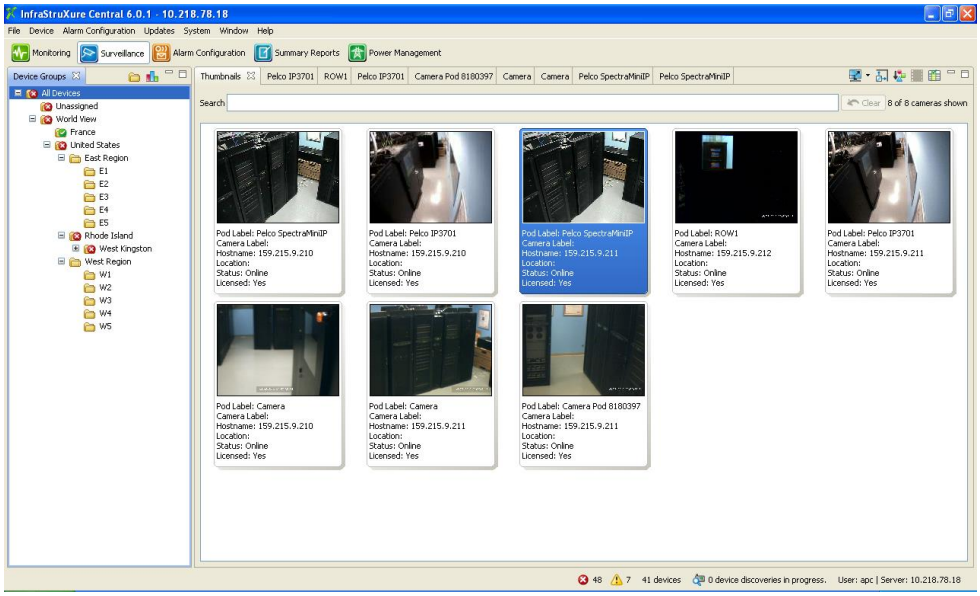
Что может помочь в подобной ситуации? На рынке имеются масштабируемые системы мониторинга и наблюдения, позволяющие собирать, сортировать и распространять критически важные оповещения и видеозаписи системы наблюдения. Пример такой системы показан на **рисунке 4**. Отслеживая состояние электропитания и охлаждения, контролируя передние и задние поверхности стоек, а также внешнюю среду, эти системы могут мгновенно выдавать уведомления о сбоях, позволяют быстро оценивать ситуацию и устранять серьезные инфраструктурные проблемы, которые могут негативно сказаться на доступности системы.

Посмотрим, как подобная система мониторинга и автоматизации могла бы помочь в описанных выше случаях, где причиной проблем стало отсутствие понимания между людьми.

- Система автоматизации и мониторинга инженерной инфраструктуры в сочетании с системой видеонаблюдения, контролирующей действия сотрудников, включает видеозапись при срабатывании датчиков движения. Поэтому даже если бы на объекте не было ИТ-специалиста, действия подрядчиков, заворачивающих серверы, были бы записаны, а администратор получил бы сигнал тревоги. Увидев, что происходит, администратор мог бы остановить подрядчиков и избежать простоя.

Рисунок 4

Пример включаемой датчиком движения системы видеомониторинга, которая помогает уменьшить число человеческих ошибок (пример экрана из приложения APC by Schneider Electric Data Center Expert)



- Система мониторинга и автоматизации также может включать и выключать устройства при помощи сигнальных контактов низкого напряжения. Такой подход может использоваться для управления замками на стойках (см. **рисунок 5**). Действия выходного реле можно выполнять в ручном режиме или настроить для автоматического срабатывания при оповещении о превышении порогового значения или другом сигнале тревоги. Если было известно, что после окончания рабочего дня придут уборщики, систему можно было бы запрограммировать на запирание всех стоек после 18.00. Сотрудник, имеющий необходимый допуск, мог бы открыть их вручную или удаленно, но для всех остальных они были бы закрыты до следующего утра.

Камеры наблюдения особенно полезны, если серверный зал обслуживает приложения, в которых выполняются операции с пластиковыми картами. Выполнение требований индустрии платежных карт в последнее время стало очень важным фактором. Правительства некоторых государств требуют, чтобы компании уведомляли клиентов обо всех случаях утечки данных. Со временем понятие персональных данных расширится и будет включать в себя номера кредитных карт. Как только это произойдет, компании, в которых процедуры защиты таких данных недостаточно эффективны или отсутствуют, будут подвергаться санкциям. Компаниям, которые обеспечивают высокий уровень защиты, соответствующий требованиям индустрии платежных карт, в будущем может также предлагаться прямое финансовое поощрение. Видеонаблюдение является одним из компонентов соответствия требованиям индустрии платежных карт.

Система управления камерами обычно позволяет отслеживать персонал объекта, подрядчиков, сотрудников служб безопасности, смотрителей и других посетителей, входящих в серверный зал или удаленный коммутационный узел. Система может определить, кто находился в комнате в определенный момент времени, а также выявить отключение или подключение посетителем какого-либо оборудования. Такую систему также можно запрограммировать на запись данных при обнаружении движения. Кроме того, администратор может удаленно войти в систему, активировать ближайшую к посетителю камеру и наблюдать за его действиями. Некоторые подобные системы оборудуются динамиками, чтобы администратор мог со своего ноутбука давать указания посетителю или выдавать ему предупреждения (например, «Ни в коем случае не трогайте эту красную кнопку!»).

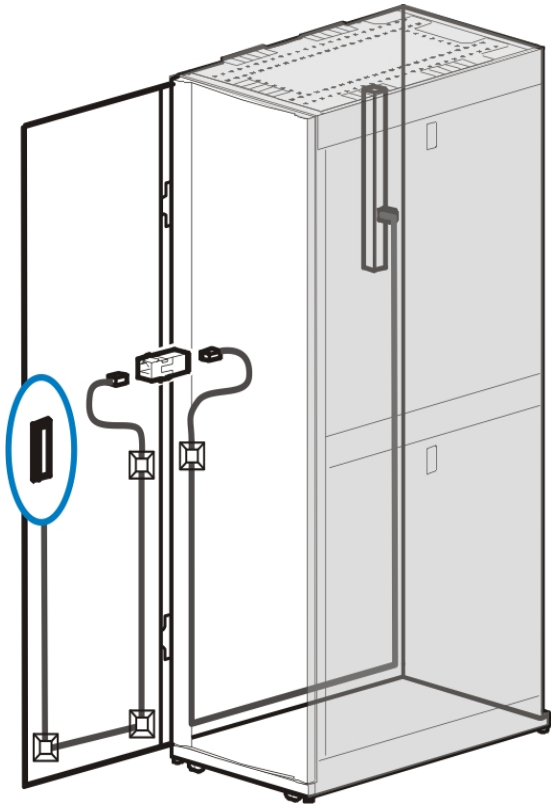


Рисунок 5

Удаленное управление безопасностью стоек позволяет предотвратить нежелательное проникновение

Интеллектуальные стоечные розетки

Интеллектуальные стоечные розетки представляют собой длинную тонкую панель с набором электрических розеток, закрепленную изнутри на задней стенке стойки (см. **таблицу 1**). Этими устройствами, известными также под названием «стоечные БРП», можно управлять, давая пользователям возможность удаленно включать и выключать питание находящегося под замком оборудования. Это сильно сокращает простои, позволяя быстро перезапускать оборудование и не тратить время на поездки на удаленные объекты.

Данные устройства также позволяют настраивать последовательность, в которой выключается или включается подача питания в каждую розетку. Это позволяет пользователям заранее определить, какое оборудование необходимо включать раньше, чтобы обеспечить корректную работу зависящего от него оборудования. При включении стойки интеллектуальное распределение питания помогает избежать начальной перегрузки из-за броска мощности — перегрузка цепей в этом случае может привести к потере нагрузки.

Также система мониторинга помогает предотвратить перегрузку, выводя графическое представление среднего и пикового потребления энергии и измеряя реальное потребление при помощи стоечных БРП с функцией мониторинга (интеллектуальных стоечных розеток). Таким образом, системный администратор имеет возможность контролировать потребление энергии каждой стойкой и принимать обоснованные решения о том, где разместить дополнительное оборудование, которое необходимо установить.

Программное обеспечение для мониторинга и автоматизации

Система управления и автоматизации предоставляет в распоряжение администратора огромный объем данных, позволяющих сократить время непродуктивных простоев из-за человеческих ошибок. Ниже перечислены некоторые функции предлагаемых на рынке систем мониторинга и автоматизации серверных залов и удаленных коммутационных узлов.

Таблица 1

Общие сведения о решениях

Компонент решения	Роль	Преимущество	Образец
Мониторинг и автоматизация	Оповещение Состояние оборудования Отчеты Настройка Управление	Пользователь может задавать пороговые значения для отправки текстовых сообщений, электронных писем или системных сообщений при выходе за установленные рамки определенных параметров, таких как температура и влажность. Создание многоуровневых отчетов на основе собранных за длительное время данных позволяет заблаговременно выявлять тенденции, ведущие к появлению проблем. Возможность массовой настройки сходных системных характеристик (таких как замки стоек и пороговые значения температуры) сразу для всех устройств этого типа. Возможность перезагрузки зависшего оборудования с удаленного ноутбука.	 
Оборудование для видеонаблюдения	Наблюдение за действиями людей	Запись видео по движению или сигналу тревоги Обнаружение и фиксация движений позволяет сопоставлять визуальные данные с данными о доступе или сигналами об изменении состояния внешней среды, ускоряя причинно-следственный анализ Сохранение данных об ошибках или обнаружении нарушений защиты предотвращает рецидивы	 
Интеллектуальные стоечные розетки	Удаленный запуск и выключение серверов Рациональное потребление электроэнергии	Сохранение целостности данных при длительных отключениях энергии Удаленное управление розетками позволяет отключать розетки, которые не используются (предотвращение перегрузки) или снова подавать питание на зависшее оборудование (сокращение до минимума дорогостоящих простоев и избавление от необходимости ездить на место размещения оборудования) Позволяет настраивать последовательность включения и выключения питания каждой розетки, помогая избегать бросков мощности при запуске, которые могут привести к перегрузке цепей и потере нагрузки	

Датчики	Дверные замки, замки стоек, обнаружение протечек, мониторинг температуры, мониторинг качества воздуха	Дверной переключатель позволяет обнаруживать доступ не имеющего допуска персонала Обнаружение воды и повышенной влажности Обнаружение в воздухе дыма и взвесей Мониторинг температуры в ключевых точках	

Сигнальные механизмы и уведомления — Настроенные в системе сигнальные механизмы выступают в качестве пускового устройства. Если, например, пороговое значение температуры в нижней части стойки составляет 16 °C, превышение этого порогового значения приведет к созданию сигнального механизма. Этот сигнальный механизм затем рассылает оповещения, используя указанные пользователем способы. Оповещение может представлять собой сообщение электронной почты, текстовое сообщение, публикацию на веб-сайте или звонок на телефон. Формат оповещений может быть достаточно сложным — вплоть до почтового сообщения на устройство Blackberry с графиком температуры в серверном зале за последние четыре часа. Он может быть также очень простым, например, иметь вид электронного письма, сообщающего о том, что дверца стойки, которая должна быть закрыта, находится в открытом состоянии более двух минут.

Состояние оборудования — Простейшая конфигурация системы мониторинга включает в себя программное обеспечение и выделенный физический сервер. Сервер выступает в качестве центрального хранилища журналов данных обо всем настроенном оборудовании серверного зала. Помимо данных с датчиков и камер производится также сбор и систематизация всех системных профилей и пороговых значений. Уровень мониторинга может быть достаточно подробным. Например, каждая стойка может содержать три датчика температуры (внизу, в середине и в верхней части), поскольку температура на этих уровнях может быть совсем разной.

Оповещения о состоянии также полезны для мониторинга батарей. Отказ одной батареи может привести к потере критически важной нагрузки. Неисправные батареи необходимо заменять как можно быстрее, однако зачастую никто не следит за возрастом батарей ИБП на удаленных объектах. Расходы на замену одной-двух батарей меркнут по сравнению с перспективой сбоя, приводящего к отключению серверного зала. Избежать таких ситуаций поможет простейший мониторинг.

Анализ отчетов — Данные, собираемые системой мониторинга, можно преобразовывать в отчеты с заданными параметрами, которые будет просматривать ИТ-администратор. В прошлом для определения температуры в нерабочее время администраторам приходилось прибегать к услугам охранников или других посторонних лиц, которые считывали и вручную записывали показания термометров на стенах. Сейчас администратор может проверить историю и увидеть, что температура ночью колебалась в пределах 12° С. Проверив отчеты за 48 часов, недельные отчеты или отчеты за более длительный период времени, администратор может заметить наличие проблемы и обратиться в отдел, занимающийся инфраструктурой здания, с просьбой помочь в ее решении (если для частичного или полного охлаждения комнаты используется система кондиционирования воздуха здания). Данные, собираемые системой мониторинга помещения для ИТ-оборудования, позволяют документально подтвердить наличие проблемы, которая может быть симптомом более серьезной неисправности. Отчеты системы также полезны с точки зрения безопасности, поскольку помогают ИТ-

> “Затем администратор может сразу определить, какие ИБП поддерживают «лишнюю» нагрузку, и выдать команду об остановке, прежде чем какой-нибудь из розничных торговых терминалов отключится.”

администратору быстро определить, кто был у определенной стойки и сколько времени он провел у нее.

Если взять в качестве примера используемые в розничной торговле терминалы, система мониторинга может проверять ИБП на местах и выдавать отчеты о том, сколько нагрузки приходится на каждый отдельный ИБП. Если ИТ-администратор определяет, что нагрузка на все ИБП должна составлять 50%, он легко может выявить те из них, для которых нагрузка выше. Затем администратор может сразу определить, какие ИБП поддерживают «лишнюю» нагрузку, и выдать команду об остановке, прежде чем какой-нибудь из розничных торговых терминалов отключится.

Массовая настройка — После первоначальной установки для всех устройств, подключенных к системе централизованного мониторинга и автоматизации, создаются журналы и профили. Это позволяет администратору впоследствии настраивать или запускать массовые изменения (одно изменение, затрагивающее несколько устройств). Рассмотрим для примера дверные замки на стойках в серверном зале. Каждый замок не надо настраивать отдельно. Если администратор захочет что-то сделать, ему необходимо будет передать на все 50 дверей в стойках (передних и задних) лишь одну конфигурацию системы безопасности.

Управление — Администраторам психологически гораздо легче работать при наличии доступа к подробным данным системы мониторинга и автоматизации. Например, система может составить схему распределения питания и физическое взаимоотношение и зависимость систем. Это помогает избежать судорожных поисков источника проблемы при ее возникновении. Некоторые системы также могут порекомендовать лучшее место для размещения нового оборудования с учетом свободной мощности и сетевых портов. Таким образом можно избежать проблем с неожиданной нехваткой мощности в определенной стойке. Кроме того, система может наглядно продемонстрировать последствия отказа определенного устройства в стойке — это помогает выявить воздействия таких отказов на работу критически важных бизнес-приложений. Данная возможность позволяет администратору заранее сформулировать план на случай возникновения проблемы и свести к минимуму время простоя.

Более полный контроль над средой, лучшее оповещение и более полные исторические данные облегчают управление системой. Если системы видеонаблюдения и централизованного управления и автоматизации уже имеются, на добавление средств контроля температуры и влажности, данных о температуре конденсации и других оповещений о состоянии внешней среды потребуется потратить совсем немного средств. Оценка тенденций состояния рабочей среды и проверка данных видеонаблюдения помогают администратору обнаруживать проблемы в зародыше и сводить к минимуму число человеческих ошибок.

Еще несколько «боевых историй»

Системы электропитания и охлаждения особенно уязвимы к человеческим ошибкам ввиду отсутствия у сотрудников знаний об этих системах. Ниже приведены примеры случаев, иллюстрирующих некоторые связанные с этими системами опасности.

- В одном из случаев ИБП перегрелся, поскольку на устройство поставили упаковки с туалетной бумагой, нарушив циркуляцию воздуха.
- На верхней лестничной площадке офисного здания был устроен небольшой серверный зал для временного проекта. Группа, занимавшаяся установкой оборудования, выбирала дешевые, но соответствующие спецификации устройства. Для охлаждения использовался домашний кондиционер воздуха, мощность которого вполне соответствовала количеству тепла, выделяемого оборудованием в зале. Однако вскоре пришлось обратиться в службу поддержки из-за аппаратного сбоя. На место был отправлен инженер, который обнаружил, что температура в помещении составляла около 43° С. К сожалению, кондиционер установили так, что и

воздухозаборник, и вывод воздуха находились у него в одном и том же маленьком помещении.

- Свободная розетка действует как магнит на всех, кто заходит в серверный зал или коммутационный узел. Множество серверных залов отключались из-за проблем с оборудованием, несанкционированно подключенным к розеткам. Примерами оборудования, которое НЕЛЬЗЯ подключать к розеткам ИБП, могут служить пылесосы и дрели. В одном из случаев короткое замыкание в дрели вызвало срабатывание автомата защиты ввиду пробоя на землю и привело к отключению значительного части оборудования в серверном зале.
- В магазине крупной розничной сети не было ни одного сотрудника, разбирающегося в работе серверного зала или коммутационного узла. Кассиры, придя на работу, обнаружили, что кассы отключены. Головной офис посоветовал им подключить систему в обход ИБП к электросети общего пользования, пока не будут доставлены новые батареи. Когда батареи доставили, для их установки пришлось отправлять квалифицированного специалиста. В итоге в этот день были потеряны тысячи долларов из-за несостоявшихся покупок, а если бы произошло отключение электроэнергии, потери могли бы быть еще больше.
- Другая розничная сеть постоянно сталкивались с проблемами, связанными с поддержанием работоспособности торговых терминалов. Это стало серьезной проблемой из-за того, что после каждого отключения системы приходилось производить калибровку весов, используемых для взвешивания отгружаемых товаров. Из-за этого время простоев значительно увеличивалось. Проведя расследование, ИТ-менеджер выяснил, что сотрудники торговых точек «нелегально» подключали к ИБП, обеспечивающим работу торговых терминалов, обогреватели, вентиляторы и другие подобные устройства. Поскольку система была рассчитана только на поддержку нагрузки, создаваемой торговыми терминалами, подключение дополнительных устройств приводило к перегрузке и отключению системы.
- Отключение стойки серверов произошло из-за того, что ИТ-администратор случайно перегрузил цепь питания, уже работавшую на максимуме.

Любой, кому приходилось иметь дело с управлением удаленными серверными залами, наверняка может добавить к этому списку еще несколько историй о человеческих ошибках. К счастью, имеется множество средств мониторинга, которые способны облегчить жизнь операторов, беспокоящихся по поводу непредвиденных простоев удаленных систем.

Заключение

Серверных залов и небольших удаленных коммутационных узлов становится все больше, и они часто страдают от непредвиденных простоев, связанных с человеческими ошибками. Управление этими небольшими центрами обработки данных требует много времени и отличается сложностью. Многие подобные объекты представляют собой не имеющие обслуживающего персонала ИТ-залы с минимальным контролем.

Комплексный подход, предполагающий использование систем мониторинга и автоматизации, видеонаблюдения, интеллектуальных стоечных розеток и датчиков, позволяет значительно уменьшить число человеческих ошибок в подобных небольших системах. Эти системы дают возможность привлекать к работе с данными квалифицированных администраторов, которые могут удаленно управлять объектом и выявлять проблемы, прежде чем они приведут к простою.

Об авторе

Деннис Булли — старший научный сотрудник Научно-исследовательского центра по центрам обработки данных APC by Schneider Electric. Он получил степень бакалавра по журналистике и французскому языку в Университете Род-Айленда, а также годовой сертификат Сорбонны (Париж, Франция). Он опубликовал ряд статей в международных журналах, посвященных ИТ-оборудованию и физической инфраструктуре ЦОДов, и стал автором нескольких информационных статей для проекта The Green Grid.

Ресурсы

Значки служат ссылками на дополнительные материалы

Библиотека информационных статей
whitepapers.apc.com

TradeOff Tools™
tools.apc.com

Обратная связь

Отклики и комментарии к настоящей статье направляйте по адресу:

Data Center Science Center
DCSC@Schneider-Electric.com

С вопросами по конкретным проектам заказчикам следует обращаться к закрепленным за ними представителям Schneider Electric