Мониторинг в дата-центре: как повысить эффективность и избежать проблем

Евгений ЮМАГУЛОВ
эксперт по проектированию и построению ЦОД компании «ICL Системные технологии»

Разбираем типовые ошибки в ходе реализации систем мониторинга, с которыми чаще всего приходится сталкиваться в проектах, связанных с построением или модернизацией дата-центров.

Споры на тему, что главнее в ЦОД, — занятие увлекательное, но бесполезное. Все оборудование дата-центра должно работать в комплексе, обеспечивая эффективное функционирование ИТ-сервисов. Но одну систему незаслуженно обходят вниманием: речь идет о средствах мониторинга. Бывает, что такой подсистемы нет вообще, а для оперативного контроля ситуации используются встроенные в оборудование средства, например, отдельный интерфейс у ИБП или кондиционера. Для полноценного ЦОДа это не особенно хорошая ситуация, поэтому такой вариант мы рассматривать не будем. Система мониторинга ЦОДа должна не только информировать персонал о текущем положении дел, но и сводить к минимуму простои дата-центра, связанные с авариями, а также помогать предотвращать некоторую их часть. В реальности система

мониторинга зачастую не выполняет этих задач, несмотря на то что сама по себе работает без сбоев. Почему так происходит?

Дело в том, что для многих проектов ЦОД характерна ситуация, когда систему мониторинга настраивал тот же интегратор, который создавал дата-центр. Причем настраивал, исходя из своего опыта и понимания того, как все должно быть, то есть без тщательно проработанного индивидуального ТЗ. Служба эксплуатации после приемки объекта ничего не перенастраивала. Как справедливый итог — в распоряжении имеется в целом хорошая система, обладающая массой недостатков. Разберем основные из них: три вопроса технического характера и четыре организационных момента.

Не проработаны аварийные алгоритмы

Еще одна проблема заключается в том, что зачастую не продуманы значения тревожных сообщений и логика порогов срабатывания. Тем не менее это важнейший вопрос, которому стоит уделить самое пристальное внимание с учетом не только критичности каждого параметра, но и индивидуальных особенностей конкретного сенсора. Например, датчик влажности воздуха, находящийся около входной двери, будет показывать более широкий диапазон значений, чем тот, который установлен в дальнем углу машинного зала за тремя дверьми. Если на всех датчиках установить одинаковые пороги, то весной и осенью от первого датчика каждую неделю будут приходить десятки оповещений о высокой влажности, а второй никогда не просигнализирует о превышении параметра.

Другой пример — датчики напряжения на городском вводе и на выходе ИБП. Здесь тоже диапазоны допустимых значений могут сильно различаться. Еще одна ошибка, которая до сих пор часто встречается, — использование одноуровневого оповещения, когда фактически имеются только два варианта: «Все нормально» и «Все пропало». Но в дата-центре такой подход вряд ли принесет большую пользу. Правильнее предупреждать службу эксплуатации не о выходе за пределы допустимых значений параметра, а о приближении к промежуточному порогу (лучше даже, если таковых будет несколько). Некоторые программные продукты позволяют проводить анализ тенденций изменения параметров. Это самый лучший вариант: можно строить долгосрочные прогнозы (на неделю, месяц, квартал) и заблаговременно планировать мероприятия по устранению потенциальных проблем.

> Система мониторинга ЦОДа должна не только информировать персонал о текущем положении дел, но и сводить к минимуму простои дата-центра

Избыток информации

Для всех служб в интерфейсе отображается много ненужной информации, при этом важные сведения теряются в общем потоке. Скажем, электрики смотрят на показатели сотен датчиков температуры воздуха и при этом не замечают перегрева шин вводно-распределительного устройства. Специалисты, отвечающие за ИТ-системы, видят, что с ДГУ все хорошо, но упускают превышение допустимого тока для блока розеток в шкафу при добавлении очередного сервера. Сотрудник, контролирующий работу дизельных генераторов, в свою очередь, прекрасно информирован о количестве проходов людей в машинный зал, но не уследил за уровнем топлива в баке. И все смотрят видео с камер наблюдения... просто от скуки. Что мешает для каждой службы создать отдельные интерфейсы? Ведь это умеют многие «большие» системы — как специализированные, так и универсальные, поддерживающие ролевую модель управления. Кроме правильного информирования, это даст и еще один плюс: уменьшится риск несанкционированного (случайного) изменения настроек в смежных подсистемах.

Нет оперативного оповещения или оно нецелевое

Стандартная настройка тревожных оповещений строится по следующей схеме: «всем по почте, оперативному персоналу — по СМС, а руководству — только сообщения об авариях». При этом, как и в случае с интерфейсом отображения информации, о разделении данных задумываются далеко не всегда. В итоге большой поток сообщений превращается в надоедливый спам, сигнализирующий только о том, что система мониторинга все еще работает. И трудно сказать, что хуже — слишком большое количество оповещений или полное их отсутствие. Так, некоторые производители систем мониторинга не предлагают комплектных GSM-модемов, и, если интегратор в ходе реализации мониторинга ЦОДа не подберет подходящую модель, оперативность информирования значительно пострадает.

Отсутствие круглосуточного дежурства

Второй блок эксплуатационных проблем носит не технический, а организационный характер. Мало получить хороший инструмент — надо еще уметь им пользоваться. Не зря в системе сертификации Uptime Institute есть отдельный статус Operational Sustainability, требующий подтверждения на регулярной основе. Одна из наиболее часто встречающихся проблем связана с организацией труда людей, которые эксплуатируют систему мониторинга ЦОДа.

Например, на объекте нет круглосуточной дежурной смены. Вместо этого есть специалисты, которые приходят и уходят в стандартное рабочее время, а в случае неисправности среди ночи бегут в дата-центр, теряя время на дорогу и на препирательства с охраной («Нечего тут по ночам ходить!»). Могут и не бежать: любой сотрудник, не имеющий в должностных обязанностях пункта «Быть всегда на связи», имеет полное право на ночь выключить

телефон и, соответственно, не получит соответствующего оповещения. А ведь стоимость организации круглосуточного дежурства — даже с учетом дополнительных расходов на зарплаты в течение года — может оказаться значительно ниже, чем потери от простоя всего дата-центра из-за мелкой неисправности, которую дежурный инженер мог бы устранить за пару минут.

Отсутствие аварийных регламентов

Эта проблема связана с тем, что на многих объектах часто отсутствуют четкие инструкции, как именно действовать в случае наступления того или иного происшествия. Куда бежать (и надо ли) при запуске дизеля? Кому звонить при срабатывании системы пожаротушения? Как оперативно отключить неисправное оборудование, ввести в работу холодный резерв и как долго можно работать на этом резерве? Типичная реакция человека, прибежавшего устранять аварию, проходит в несколько этапов: паника, ступор и непонимание, анализ ситуации, принятие решения и устранение проблемы. Поэтому у оперативного персонала должно быть четкое понимание того, что случилось и как действовать прямо сейчас. В идеальном случае эта проблема решается комплексно: пошаговые краткие инструкции, размещенные в месте установки оборудования (в рамочке на стенке, как план эвакуации), детальные алгоритмы и указания, которые изучены заблаговременно, и, конечно, регулярные тренировки.

> У оперативного персонала должно быть четкое понимание того, что случилось и как действовать прямо сейчас

Нет склада ЗИП и заключенного сервисного контракта

Даже при полном резервировании всех систем дата-центра открытым остается вопрос о том, как долго будет длиться ремонт неисправного оборудования. Хорошо, если производитель известный и с долгой историей — такие компании обычно поддерживают локальные склады запчастей. Но доставка даже с российского склада может занять недели, поэтому принцип «поближе положишь — побыстрее возьмешь» в данном случае очень актуален. Можно переложить часть ответственности на подрядную организацию, заключив сервисный контракт на обслуживание и поставку запасных частей с оговоренным в SLA гарантированным сроком реакции. При должном уровне резервирования подсистем такой подход позволяет выстроить многоуровневую схему защиты от сбоев: отказ одной единицы оборудования не приводит к простою ЦОДа, мелкие неисправности устраняются сразу же силами эксплуатирующего персонала, а через некоторое время на объекте появляется бригада профильных специалистов, которые окончательно решают любую серьезную проблему.

Не организован процесс фиксации инцидентов и контроля их устранения

Зачастую нет и метода анализа причин и последствий сбоев. В большинстве случаев инциденты, не приведшие к фатальному отказу, не фиксируются, а их отработка не контролируется. Особенно если есть резерв оборудования или оперативный ремонт удалось провести своими силами с использованием запчастей, имевшихся на складе. В итоге бывает так, что инцидент случился, персонал ЦОДа прошел все этапы — от паники до устранения аварии, а через год о случае все благополучно забыли. И даже имевшейся когда-то готовности к следующему отказу уже нет, ведь резервного оборудования и запчастей не осталось, а новые детали на склад никто не заказал. В такой ситуации повторный отказ гарантированно приведет к длительному простою ЦОДа.

Правильные вопросы о мониторинге в ЦОД

Чтобы неприятностей было как можно меньше, а пользы от системы мониторинга как можно больше, при ее создании нужно задать себе четыре основных вопроса:

1. Зачем нужна система мониторинга на объекте?
2. Какие задачи она будет решать?
3. Какая информация действительно необходима и как срочно?
4. Что делать с полученной информацией?

Ответы на эти вопросы на самом деле оказываются непростыми, но они станут хорошим началом для продуктивной работы над действительно эффективной системой мониторинга ЦОДа.

В качестве примера можно рассмотреть следующую гипотетическую ситуацию. Некая организация имеет обширный парк оборудования, и есть следующие проблемы с его эксплуатацией:

- оборудование периодически отключается или выходит из строя в случае превышения заданных температурных параметров в помещениях;
- нет актуальной информации о парке оборудования: количество и модели, версии прошивок, техническое состояние, наличие отказов и т. д.;
- отсутствуют данные о действиях, произведенных с этим оборудованием.

Здесь уже кроется ответ на первый вопрос: есть сформулированная потребность. Система мониторинга в первую очередь должна решать перечисленные выше проблемы, но раз уж она создается, то можно придать ей и дополнительный функционал, который будет полезен для работы.

Какие задачи будут решаться

Основные задачи, выполняемые гипотетической системой мониторинга, которую мы рассматриваем в примере, можно разделить на два условных блока — основные и дополнительные.

К первой группе относятся такие вопросы, как:

- контроль температуры в помещениях, где установлено оборудование;
- контроль текущего состояния оборудования;
- контроль доступности интерфейсов управления оборудованием по сети;
- предупреждение отказов оборудования;
- оперативное оповещение персонала об отказах;
- учет количества, моделей, версий прошивок, выработки ресурса оборудования;
- учет физического доступа к оборудованию;
- учет действий, производимых с оборудованием;
- автоматизация создания отчетов по парку оборудования.

В числе дополнительных задач можно упомянуть:

- контроль влажности в помещениях, где установлено оборудование;
- централизованное обновление прошивок;
- централизованная групповая настройка параметров оборудования;
- визуализация общего текущего состояния парка оборудования.

Какая информация действительно необходима и как срочно?

Казалось бы, все просто: температура, влажность, системная и диагностическая информация с оборудования, факты открытия дверей шкафов. Но есть немало нюансов. Например, требуется уточнение, в каком именно месте следует организовать контроль температуры, ведь на разных участках в одном и том же помещении она может существенно отличаться.

Обычно учитывается температура в месте подачи холодного воздуха к активному оборудованию. То есть если в помещении несколько ИТ-шкафов, то датчики должны быть на передних дверцах каждого из них, а не один общий датчик на все помещение. Более того, в высоконагруженных ЦОДах даже на разной высоте в одной и той же стойке температура может существенно различаться, и в этом случае на дверцу шкафа ставят уже три датчика. Информация о температуре воздуха на выходе (в горячем коридоре) для данной системы, скорее всего, неактуальна.

Что касается влажности, то ее лучше всего контролировать в тех же точках, что и температуру, тем более что при одной и той же абсолютной влажности относительная влажность будет зависеть от температуры воздуха. Но если оборудование нечувствительно к влажности, то ради экономии можно поставить один общий датчик на все помещение.

Также необходимо уточнить для себя вопрос необходимости системной и диагностической информации от оборудования. Действительно ли вся она нужна? Ведь зачастую ее гораздо больше, чем реально необходимо для мониторинга состояния. Если есть техническая возможность, то лучше оставить лишь критически важную информацию, чтобы не утонуть потом в потоке незначительных сообщений.

> Информацию надо получить еще до отказа оборудования, а не зафиксировать сбой постфактум с задержкой в час-другой.

Если говорить о срочности получения сведений, то здесь, как правило, чем быстрее, тем лучше. Оповещение персонала должно осуществляться не только через графический интерфейс системы мониторинга, но и по электронной почте и СМС. А сам мониторинг должен осуществляться в режиме реального времени. Ведь информацию надо получить еще до отказа оборудования, а не зафиксировать сбой постфактум с задержкой в час-другой. Важно помнить и о том, что не все системы мониторинга способны выдавать информацию в режиме реального времени.

Выше мы говорили о предупреждении отказов оборудования. Необходимо понимать, что сама по себе система с этим не справится — необходимо человеческое вмешательство. И здесь мы подходим к заключительному вопросу.

Что делать с полученной информацией?

Основные данные, полученные от системы мониторинга ЦОДа, должны в первую очередь использоваться для таких действий, как:

- инвентаризация парка оборудования и составление отчетов по нему;
- планирование фонда запасных частей;
- оперативное реагирование на инциденты;
- контроль состояния работ по инцидентам;
- планирование регламентных и сервисных работ;
- оформление заявок на улучшение климатических параметров в проблемных помещениях.

На этом месте поставим точку. Точнее, многоточие, поскольку тема еще очень далека от того, чтобы быть раскрытой полностью. Но даже учет рассмотренных выше вопросов и следование этим несложным рекомендациям позволят сделать систему мониторинга ЦОДа более эффективной. ■

Если вы хотите оставить комментарии к статье, воспользуйтесь данным QR-кодом.