Реализация процесса Problem Management на основе использования методов математического анализа

Процесс Problem Management относится к основным процессам, упоминаемым ITIL в разделе Operations, при этом самый важный шаг в этом процессе - выявление проблемы, практически не раскрыт. В параграфе «Problem detection» используются термины «предположение» и «анализ», но на чем основаны предположения и какого рода анализ следует осуществить – не поясняется. Далее мы изложим наш подход к прояснению данной задачи на реальном примере.

Прежде всего следует определить основные термины, при этом постараемся чтобы они были максимально близки к определениям, данным в ITIL:

Инцидент – аварийное, незапланированное, нарушение предоставления или снижение качества услуги(сервиса). Может возникать случайно, в силу объективных причин, или в результате наличия проблемы в инфраструктуре.

Проблема – дефект или иная причина возникновения одного или нескольких инцидентов.

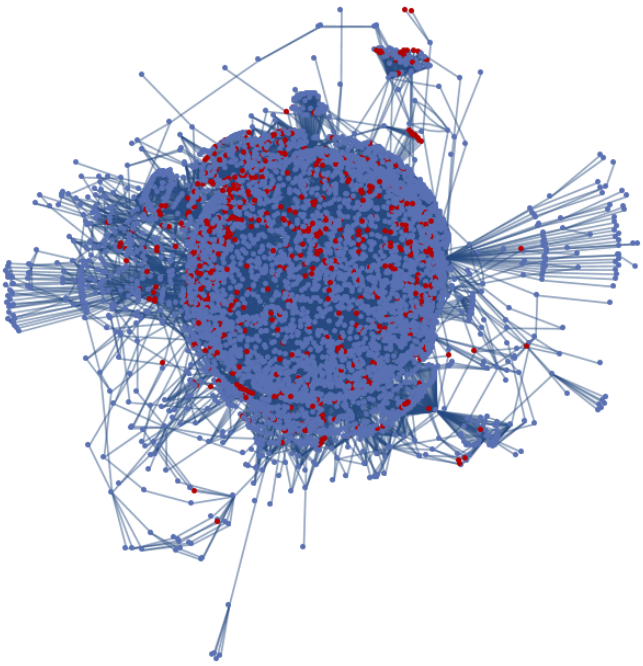
Исходя из этих определений получается, что, пользуясь аналогией с медициной, проблему можно рассматривать в качестве «болезни», которая проявляется через «симптомы» - инциденты. Следовательно, информация по инцидентам составляет основу процесса поиска проблем.

Исходные условия

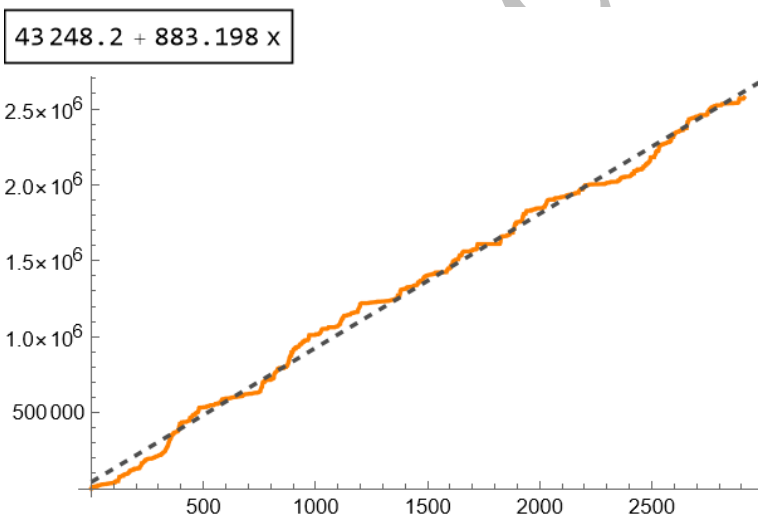
В приводимом примере исследовалась база инцидентов глубиной в один месяц. На 700-ах узлах сети (всего в сети порядка 6000 узлов) имело место 3000 инцидентов. Дополнительно в анализе использовалась информация о структуре сети, полученная в результате сканирования (Discovery) сети компании. Для учета взаимосвязи узлов при анализе необходима информация о топологии сети. К сожалению для мониторинга и сканирования в обследуемой компании используется весьма старое решение и имеющаяся информация не вполне актуальна, но иного источника данных о взаимосвязях между узлами предоставлено не было.

Решение

На первом этапе результаты сканирования сети, выполненные в категориях uid(идентификаторы в базе данных), были преобразованы в бинарные зависимости в категориях ip. В категориях ip был построен граф сети компании, включающий в себя 6000 вершин (узлов). Красными точками на приведенном ниже графе сети компании выделены узлы, где имели место инциденты за анализируемый период времени.



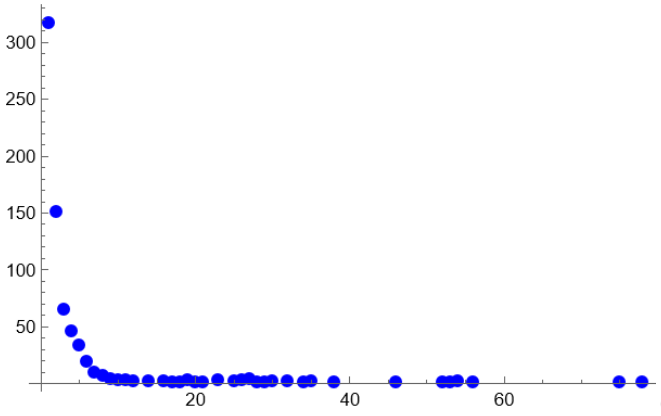
Далее был проведен первичный анализ наличия проблем. На графике ниже желтым цветом выделены моменты времени, когда имели место инциденты. Время представлено абсолютным временем, привязанным к началу месяца. Для данного ряда времени возникновения инцидентов вычислена линейная регрессия, показанная пунктирной прямой. Линейная регрессия чрезвычайно точно отражает поведение времени фиксации инцидентов. Коэффициент наклона регрессии соответствует 14минутам и 40 секундам, что можно рассматривать как среднее время между инцидентами и характеристику качества работы сети. Этот график косвенно указывает на наличие проблемы/проблем, которая **постоянно** вызывает возникновение инцидентов.



На следующем шаге была построена таблица, отражающая статистику повторяемости инцидентов на узлах (ip). Те же самые данные приведены на графике. Количество узлов, на котором был всего 1 инцидент в 2 раза больше, чем количество узлов, на которых было 2 инцидента. И близкая к этому тенденция продолжается 5-7 шагов. **{количество инцидентов, количество IP устройств на которых зарегистрировано такое количество инцидентов}**

{инцидентов, колич. IP}

{1, 317}	{11, 3}	{25, 2}	{46, 1}
{2, 151}	{12, 2}	{26, 3}	{52, 1}
{3, 65}	{14, 2}	{27, 4}	{53, 1}
{4, 46}	{16, 2}	{28, 1}	{54, 2}
{5, 33}	{17, 1}	{29, 1}	{56, 1}
{6, 19}	{18, 1}	{30, 2}	{75, 1}
{7, 10}	{19, 3}	{32, 2}	{78, 1}
{8, 7}	{20, 1}	{34, 1}	
{9, 4}	{21, 1}	{35, 2}	
{10, 3}	{23, 3}	{38, 1}	



Выявленная неравномерность возникновения инцидентов указывает на наличие областей, требующих большего внимания. Очевидно, что узлы с наибольшим числом инцидентов должны рассматриваться в качестве основных кандидатов на наличие проблем.

Также, на основе информации, полученной из инцидентов, была сделана их классификация.

agent	{{DOWN, на проблема с агентом}, 108}
connection	{{Broken, пропала связь с}, 1498}
inputPOWER	{{{Warning, на предупреждающее состояние датчика входного напряжения}, 148}, {{Critical, на критическое состояние датчика входного напряжения}, 27}}
outputPOWER	{{{Warning, на предупреждающее состояние датчика выходного напряжения}, 3}, {{Critical, на критическое состояние датчика выходного напряжения}, 6}}
powerSUPPLY	{{Critical, на критическое состояние блока питания}, 1}
batteryCAPACITY	{{{Warning, на предупреждающее состояние датчика емкости батареи}, 30}, {{Critical, на критическое состояние датчика емкости батареи}, 5}}
batteryTemperatureSENSOR	{{Warning, на предупреждающее состояние датчика температуры батареи}, 9}
temperatureSENSOR	{{{Warning, на предупреждающее состояние датчика температуры}, 18}, {{Critical, на критическое состояние датчика температуры}, 3}}
disk	{{{Warning, на предупреждающее состояние диска}, 3}, {{Critical, на критическое состояние диска}, 1}}
file	{{{Warning, на предупреждающее состояние файловой системы}, 19}, {{Critical, на критическое состояние файловой системы}, 4}}
instance	{{{Warning, на предупреждающее состояние инстансов процесса}, 5}, {{Critical, на критическое состояние инстансов процесса}, 11}}
general	{{{Warning, на предупреждающее состояние}, 17}, {{Critical, на критическое состояние}, 154}}
site	{{{Critical, на критическое состояние сайта}, 9}, {{Critical, на критическое состояние сайта работоспособность системы рассылки уведомлений}, 2}, {{Critical, на критическое состояние сайта система учета }, 1}, {{Critical, на критическое состояние сайта асу производство}, 1}}
interface	{{Critical, на критическое состояние интерфейса}, 810}
processor	{{Critical, на критическое состояние процессора}, 16}
responseTIME	{{Critical, на критическое состояние времени ответа}, 2}

Данная классификация позволяет определить функциональные области потенциальных проблем:

- Электроснабжение
- Сетевое взаимодействие
- Состояние ресурсов (processor, disk, file)

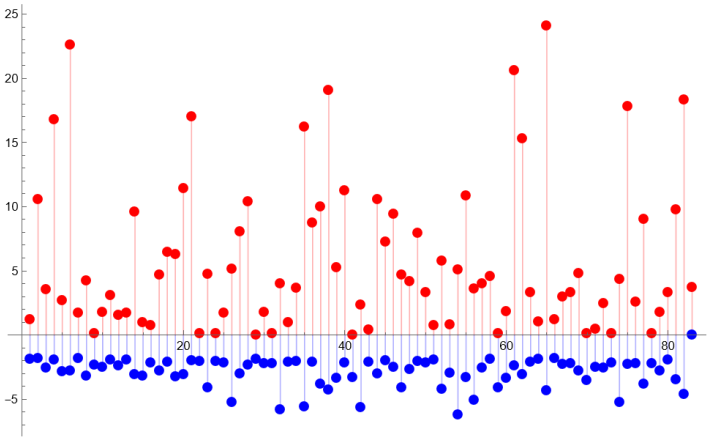
Первоначально рассматривались две гипотезы, способные прояснить время и место

возникновения начального инцидента в цепочке, но они не получили подтверждение.

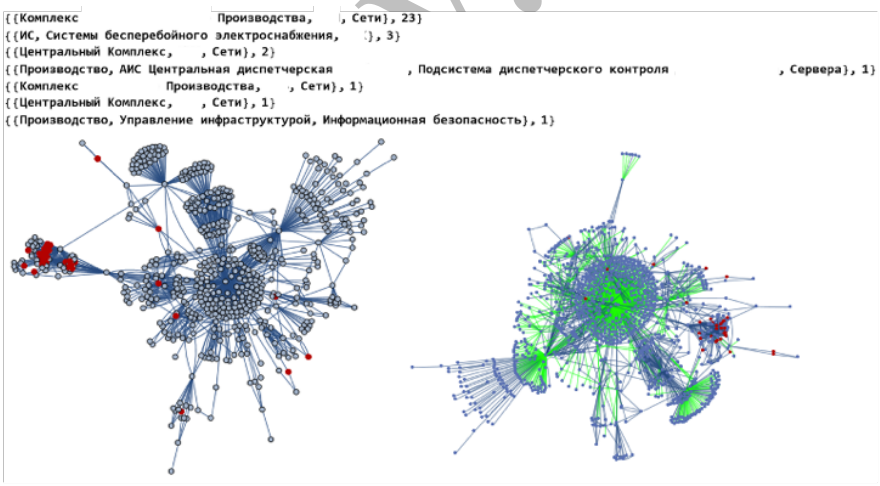
Первая гипотеза.

Эта гипотеза состоит в том, что новая цепочка инцидентов возникает после длительного периода работы без инцидентов. На графике каждая вертикальная линия характеризует период времени (в часах) работы без инцидентов (синяя точка) и период времени, когда инциденты случались чаще, чем установлен предел «безинцидентной» работы (красная точка). Для данного графика предел безинцидентной работы составляет 110 минут.

Анализ показал, что последним инцидентом в предыдущим красном периоде был такой же инцидент как первый в следующем красном периоде. Работа без инцидентов в основном происходит на стыке смен (если считать трехсменный график работ) и, скорее всего, связана с отключением оборудования.



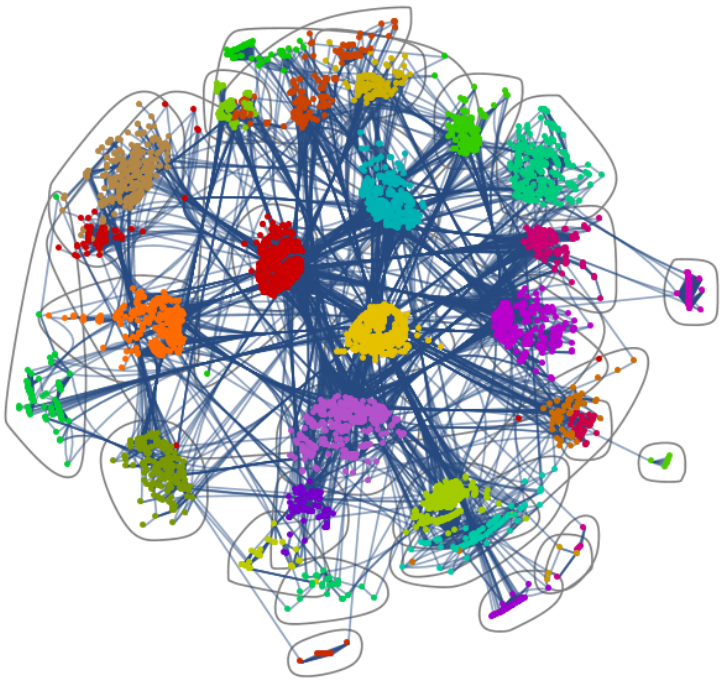
Вторая гипотеза. Логическая структура сети в основном соответствует физическому электрическому соединению узлов. На рисунке показана локальность узлов, в которой в одном месте соединены узлы, относящиеся к разным логическим частям производственных процессов.



Неприменимость данного подхода скорее всего связана с неактуальностью данных по топологии сети, взятых из используемой системы мониторинга. Кроме того, специфика данных в используемой системы мониторинга состоит в том, что там присутствуют как физические, так и логические связи между узлами.

В результате, к выявлению причинно-следственных закономерностей был применен

чисто графовый подход. На рисунке ранее приведенный граф сети компании изображен с учетом имеющихся коммуникационных связей.



Каждая группа одного цвета имеет между собой более короткие (в ребрах) связи, чем все остальные. Синие ребра показывают имеющиеся связи между «цветными» группами. Список «цветных» групп, из которых состоит граф сети компании (номер по порядку, количество вершин) приведен в таблице.

{1, 268,}	{2, 225,}	{3, 195,}	{4, 162,}
{5, 147,}	{6, 139,}	{7, 121,}	{8, 98,}
{9, 92,}	{10, 85,}	{11, 83,}	{12, 66,}
{13, 64,}	{14, 58,}	{15, 56,}	{16, 41,}
{17, 40,}	{18, 28,}	{19, 28,}	{20, 23,}
{21, 19,}	{22, 18,}	{23, 17,}	{24, 10,}
{25, 7,}	{26, 6,}		

При дальнейшем анализе для локализации проблем формируются причинно-следственные закономерности, которые могут быть связаны с объектами трех типов: сильно связанные локальности, частично связанные локальности и точечные локальности.

- Сильно связанная локальность представляет собой подграф, в котором во всех вершинах имели место инциденты, а сам подграф расположен на расстоянии не менее 4-х ребер от вершины, в которой так же имел место инцидент.

- Частично связанная локальность представляет собой подграф, в котором между вершинами, в которых имели место инциденты может располагаться только одна вершина (узел), в котором инцидента не было, а сам подграф расположен на расстоянии не менее 4-х ребер от вершины, в которой так же имел место инцидент.
- Точечные локальности представляют собой единственную вершину, в которой имели место инциденты и отстоящую от других вершин, в которых имел место инцидент на расстоянии не меньше 4-х ребер.

В исследованных данных было выявлено около 100 локальностей. Из них порядка 65% сильно связанных, порядка 35% частично связанных и только 3 точечных. **Каждую локальность можно рассматривать как группу, связанную общей проблемой.**

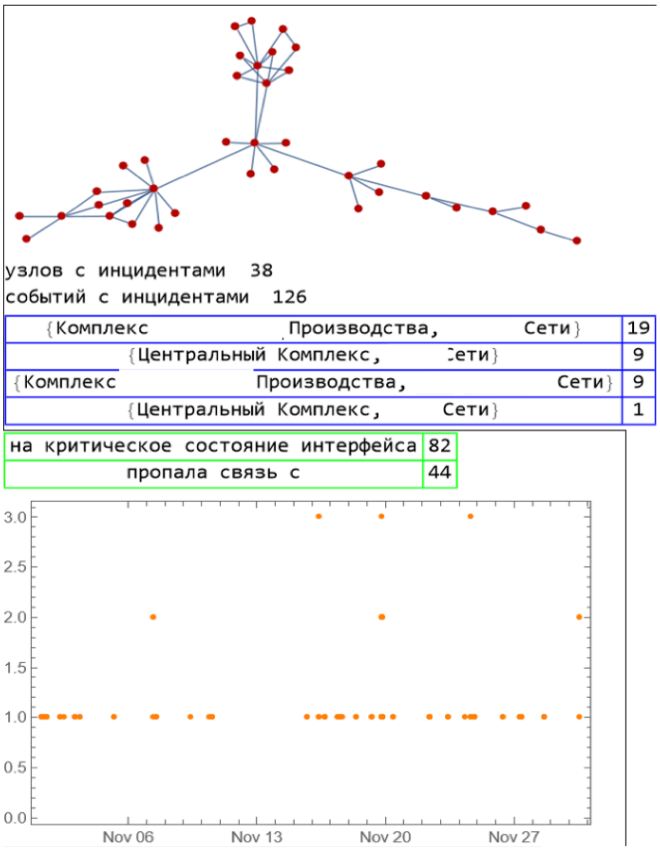
В результаты проведенного анализа были получены отчеты, состоящие из следующих элементов:

- Граф с красными вершинами - сильно связанная локальность (подграф инцидентов).
- Таблица(с голубой рамкой) с логическими наименованиями групп, к которым относятся узлы.
- В серой таблице - наименования узлов из uuid.
- В зеленой рамке сообщения системы о произошедших инцидентах в данной сильно связанной локальности.
- График с оранжевыми точками - время произошедших инцидентов.
- Причинно-следственный граф (месячный). Зеленая вершина соответствует первому инциденту в цепочке, фиолетовая - последнему инциденту месяца.
- Итоговая таблица. Содержит данные из сообщений об инцидентах для описываемого сильно связанной локальности. В таблице первый столбец – критичность инцидента, второй столбец – сообщение в инциденте, третий столбец – IP адрес возникновения инцидента, четвертый столбец – количество инцидентов.

Дальнейший поиск проблем может осуществляться на уровне анализа локальных файлов аудита для связанных в группу устройств. При наличии единой системы обработки сообщений (Event Management) процесс локализации проблем может быть частично автоматизирован.

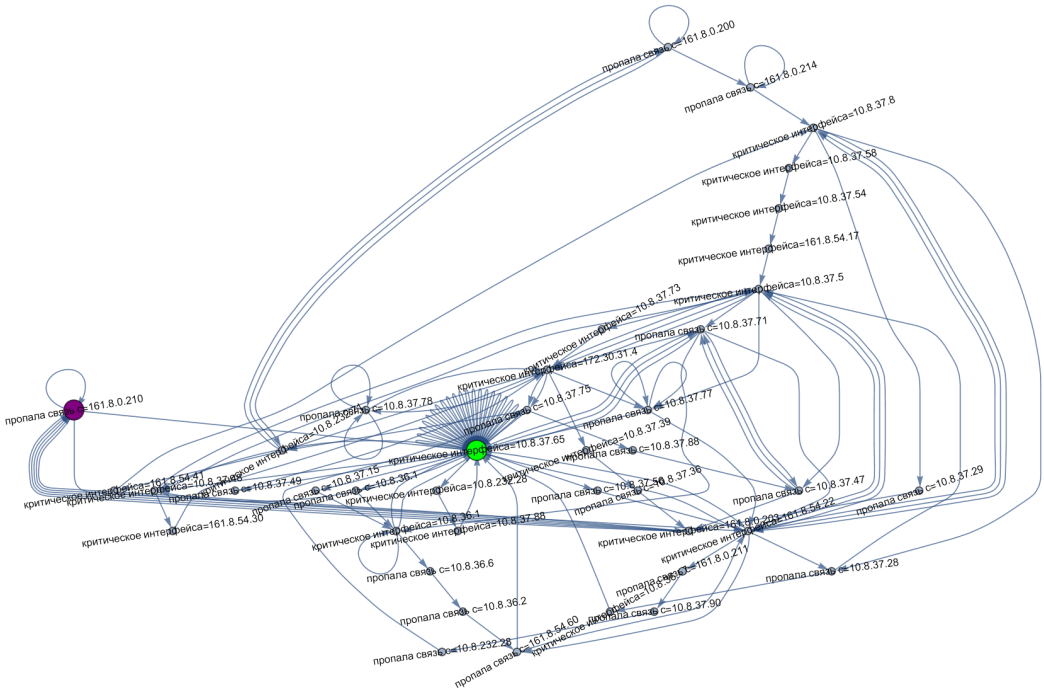
Примеры отчетов

Пример 1.



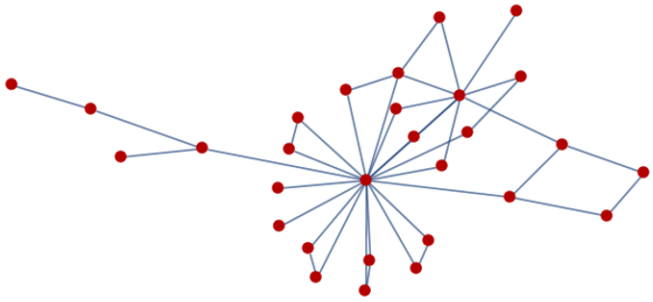
Зеленая таблица указывает на то, что на этих узлах возникали только два типа ошибок. Из графика следует что инциденты возникают достаточно равномерно, что косвенно указывает на наличие проблемы, вызывающей их постоянное возникновение.

Причинно-следственные связи



Critical	на критическое состояние интерфейса	10.8.37.65	32
Critical	на критическое состояние интерфейса	161.8.54.22	8
Critical	на критическое состояние интерфейса	172.30.31.4	7
Critical	на критическое состояние интерфейса	10.8.37.5	7
Broken	пропала связь с	161.8.0.210	5
Broken	пропала связь с	10.8.37.71	5
Critical	на критическое состояние интерфейса	161.8.0.203	4
Critical	на критическое состояние интерфейса	10.8.37.8	4
Critical	на критическое состояние интерфейса	10.8.36.1	4
Broken	пропала связь с	10.8.37.77	4
Critical	на критическое состояние интерфейса	10.8.37.48	3
Critical	на критическое состояние интерфейса	10.8.232.71	3
Broken	пропала связь с	161.8.0.200	3
Broken	пропала связь с	10.8.37.78	3
Broken	пропала связь с	10.8.37.75	3
Broken	пропала связь с	10.8.37.47	3
Broken	пропала связь с	161.8.54.60	2
Broken	пропала связь с	161.8.0.214	2
Broken	пропала связь с	10.8.37.28	2
Critical	на критическое состояние интерфейса	161.8.54.41	1
Critical	на критическое состояние интерфейса	161.8.54.30	1
Critical	на критическое состояние интерфейса	161.8.54.17	1
Critical	на критическое состояние интерфейса	10.8.37.88	1
Critical	на критическое состояние интерфейса	10.8.37.73	1
Critical	на критическое состояние интерфейса	10.8.37.58	1
Critical	на критическое состояние интерфейса	10.8.37.54	1
Critical	на критическое состояние интерфейса	10.8.37.39	1
Critical	на критическое состояние интерфейса	10.8.36.17	1
Critical	на критическое состояние интерфейса	10.8.232.28	1
Broken	пропала связь с	161.8.0.211	1
Broken	пропала связь с	10.8.37.90	1
Broken	пропала связь с	10.8.37.88	1
Broken	пропала связь с	10.8.37.56	1
Broken	пропала связь с	10.8.37.49	1
Broken	пропала связь с	10.8.37.36	1
Broken	пропала связь с	10.8.37.29	1
Broken	пропала связь с	10.8.37.15	1
Broken	пропала связь с	10.8.36.6	1
Broken	пропала связь с	10.8.36.2	1
Broken	пропала связь с	10.8.36.1	1
Broken	пропала связь с	10.8.232.28	1

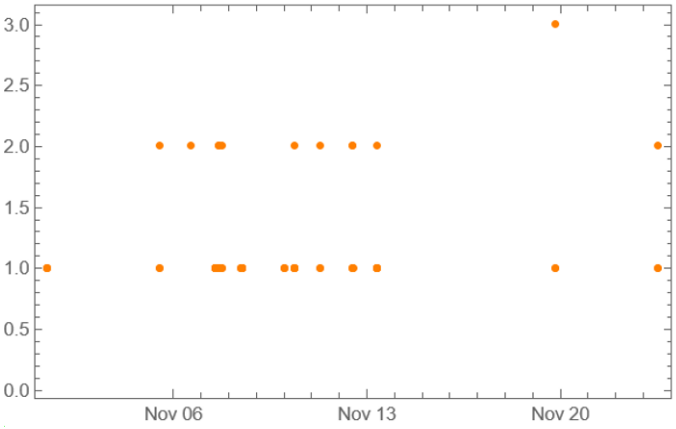
Пример 2.

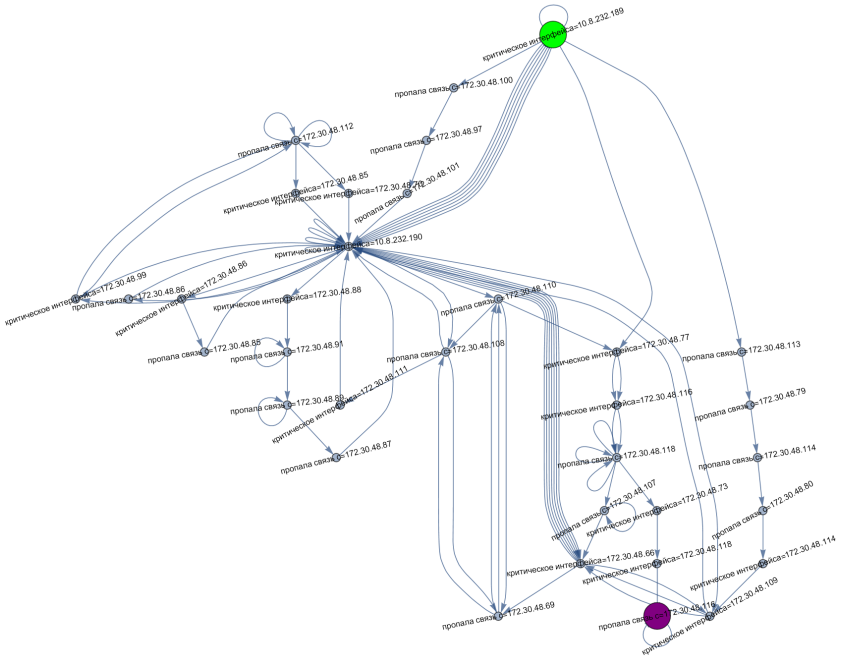


узлов с инцидентами 29

событий с инцидентами 84

{Комплекс Прокатного Производства, , Сети}	29
на критическое состояние интерфейса	48
пропала связь с	36





Critical	на критическое состояние интерфейса	10.8.232.190	19
Critical	на критическое состояние интерфейса	172.30.48.66	6
Critical	на критическое состояние интерфейса	10.8.232.189	6
Broken	пропала связь с	172.30.48.118	5
Broken	пропала связь с	172.30.48.112	4
Critical	на критическое состояние интерфейса	172.30.48.109	3
Broken	пропала связь с	172.30.48.69	3
Broken	пропала связь с	172.30.48.110	3
Broken	пропала связь с	172.30.48.108	3
Critical	на критическое состояние интерфейса	172.30.48.99	2
Critical	на критическое состояние интерфейса	172.30.48.77	2
Critical	на критическое состояние интерфейса	172.30.48.116	2
Broken	пропала связь с	172.30.48.91	2
Broken	пропала связь с	172.30.48.89	2
Broken	пропала связь с	172.30.48.116	2
Broken	пропала связь с	172.30.48.107	2
Critical	на критическое состояние интерфейса	172.30.48.88	1
Critical	на критическое состояние интерфейса	172.30.48.86	1
Critical	на критическое состояние интерфейса	172.30.48.85	1
Critical	на критическое состояние интерфейса	172.30.48.73	1
Critical	на критическое состояние интерфейса	172.30.48.70	1
Critical	на критическое состояние интерфейса	172.30.48.118	1
Critical	на критическое состояние интерфейса	172.30.48.114	1
Critical	на критическое состояние интерфейса	172.30.48.111	1
Broken	пропала связь с	172.30.48.97	1
Broken	пропала связь с	172.30.48.87	1
Broken	пропала связь с	172.30.48.86	1
Broken	пропала связь с	172.30.48.85	1
Broken	пропала связь с	172.30.48.80	1
Broken	пропала связь с	172.30.48.79	1
Broken	пропала связь с	172.30.48.114	1
Broken	пропала связь с	172.30.48.113	1
Broken	пропала связь с	172.30.48.101	1
Broken	пропала связь с	172.30.48.100	1