Método para priorização de alertas de monitoração em ambientes de Data Center

Marx Rossi
FEEC – Faculdade de Engenharia Elétrica e Computação
UNICAMP – Universidade Estadual de Campinas
Campinas, Brasil
marx-rossi@hotmail.com

Gilberto Biondo
FEEC – Faculdade de Engenharia Elétrica e Computação
UNICAMP – Universidade Estadual de Campinas
Campinas, Brasil
gilbion@gmail.com

Resumo—Este documento apresenta métodos para análise e priorização de alertas de monitoração, focado em tecnologias hoje presente em data centers. Como exemplo, é utilizada uma base da dados de falhas em *storages*, no qual são discutidos os dados relevantes para a análise de criticidade dos alertas apresentados. Os dados são verificados com o uso de métodos estatísticos e de análise visual, apresentando-se os resultados através da base de dados estudada a fim de mostrar a eficácia dos métodos.

Keywords—monitoração, Data Centers, análise visual.

I. INTRODUÇÃO (*HEADING 1*)

O crescente consumo de dados em escala global vem sendo acompanhado pela construção de Data Centers (DCs) cada vez maiores e com maior número de equipamentos, assim como pela preocupação na garantia de disponibilidade dos recursos computacionais aos usuários finais. Neste contexto, as áreas de monitoração e suporte à infraestrutura são de suma importância para a garantia da disponibilidade, visto que atuam em tempo real nas falhas ocorridas, mitigando os riscos de impacto.

O crescimento dos DCs é acompanhado, também, pelo crescimento no número de falhas nos diversos componentes de infraestrutura presentes nos mesmos. Dentro deste contexto há um problema circunstancial, que é a priorização das tratativas às falhas ocorridas. Um fator crucial para esta priorização (além da experiência do operador), é a forma como esta falha se apresenta, assim como os dados que são acompanhados pela mesma.

Neste trabalho serão estudadas as diversas variáveis envolvidas nas falhas que indicam a probabilidade de impacto, através de uma base de dados de falhas disponível, e um estudo de métodos de análise visual para apresentação dos mesmos em conjunto à uma análise exploratória destes dados. Por fim, será proposto um método para visualização dos dados a fim de demonstrar a efetividade dos estudos feitos.

II. DADOS DISPONÍVEIS

A. Monitoração em DCs de forma geral.

De forma generalista, as falhas em DCs são sempre apresentadas como uma "linha de uma tabela", atualizada em tempo real, contendo diversos dados, como: *hostname*, endereço IP, criticidade, falha ocorrida, número de ocorrências desta falha, data e hora da ocorrência, tipo de falha, criticidade, etc. Usualmente, tais informações são preenchidas ao fundo com uma cor relacionada à criticidade do alerta (vermelho para crítico, laranja para alertas com criticidade média e amarelo para alertas com criticidade baixa), sendo esta a única forma de gerar uma visualização pré atentiva que ajude na seleção de prioridade.

Além disso, devido aos dados serem sempre relacionados somente ao equipamento e falha em si, diversos dados relevantes para mensurar a criticidade da falha não estão facilmente disponíveis, sendo necessário, muitas vezes, buscar tais informações em outras ferramentas, criando também uma alta dependência da experiência de quem está à tratar a falha. Tais fatores dificultam a tomada de decisão e tornam moroso o processo de descoberta do que a falha representa em si.

B. Dados utilizados para estudo.

Para possibilitar o estudo descrito neste artigo, foram coletados dados de falhas de diversos equipamentos de armazenamento, contendo informações relevantes para o desenvolvimento deste artigo. Conforme dito no tópico anterior, as falhas apresentam-se como linhas de uma planilha, os dados que utilizamos para cada falha estão à seguir, assim como um exemplo de um alerta ao fim:

- **Severidade:** Especificação do evento de acordo com sua severidade. Os valores possíveis são I*nformation Inactive, Warning Inactive, e Error Inactive.*
- **Nome do servidor**: Nome do servidor de armazenamento em que a informação foi coletada;
- **Dia e hora:** Dia e hora em que o evento foi armazenado na log do servidor de armazenamento.
- **Local:** A parte do equipamento a qual o dado se refere. As opções disponíveis são: *Cache, System, TSSC,* e *Physical Cartridge.*
- **Descrição**: Descrição genérica do evento criado na log do sistema.

Error Inactive 1/13/2019 8:19:01 AM 1/13/2019 08:19 Storage D Call home disabled Call home not created

III. FATORES DE CRITICIDADE

Como explicado nos itens I e II, a análise da criticidade de um evento de falha na infraestrutura possui uma complexidade maior do que o alerta é capaz de amostrar. Sendo assim, os fatores à seguir influenciam a criticidade real de uma falha.

- **Topologia:** A topologia na qual o equipamento que apresentou a falha está inserido é um dos primeiros

fatores à ser analisado. Como exemplo, em ambientes de telecomunicações, ter uma falha em um equipamento que esteja em uma posição central da rede possui criticidade maior do que aquelas ocasionados em equipamentos mais periféricos.

- **Tráfego produtivo no equipamento:** Este é um dos fatores cruciais para determinar a criticidade de uma falha. Equipamentos que possuem tráfego de informações de maior relevância, e cuja indisponibilidade pode gerar impacto financeiro ou à imagem da instituição que os possui, devem possuir prioridade na tratativa.
- **Recorrência da falha:** Falhas que ocorrem com maior frequência possuem maior criticidade, visto que podem indicar equipamentos com defeitos de fabricação ou bugs de softwares.
- **Alta disponibilidade:** a redundância existente em um equipamento faz com que uma falha no mesmo possua uma criticidade diferente. Equipamentos podem não possuir redundância, possuir redundância ou estarem em clusters com 3 ou mais equipamentos, possuindo alta disponibilidade. Sendo assim, este é um fator que reduz a criticidade da falha quanto à possibilidade de impacto em serviços. Adicionalmente, também dificulta a priorização da falha, visto que pode-se apresentar uma falha em um equipamento, já existindo uma outra falha em seu equipamento redundante (ocorrida em outro instante de tempo), que, por não estar se apresentando, faz com que o analista demore a tomar a decisão de priorizar a falha.
- **Tempo para correção da falha:** à depender da falha, o tempo para resolução pode ser alto, dependendo de deslocamento de pessoas e entrega ou substituição de equipamentos em outras localidades, sendo mais um fator determinante para a priorização das tratativas. Tal dado pode ser obtido através da análise do tempo para resolução das mesmas falhas anteriores em um mesmo equipamento.
- **Criticidade da falha:** Embora haja uma separação visual em cores quanto às falhas com criticidade alta, média e baixa, o que realmente ocorre é que também dentre as mesmas temos diferentes criticidades, que não podem ser distinguidas simplesmente por 3 ou mais cores. Uma possível solução é atribuir à cada falha específica um valor.
- **Volume de dados:** A quantidade de dados (seja em tráfego ou em armazenamento) também é um fator determinante. Como exemplo, uma falha em um equipamento de telecomunicações que possua alto tráfego, irá gerar a convergência deste tráfego para outras rotas, à depender do volume, pode-se gerar lentidão, indisponibilidade momentânea ou degradação. Uma falha em um dispositivo de armazenamento que possua alta utilização do disco ocasionará maior tempo de recuperação devido ao tempo para recuperação do RAID.

Todos os fatores explanados acima são determinantes para a priorização de uma falha, sendo ideal que a visualização da falha contemple os mesmos. Como exemplo, no modelo clássico de priorização de alertas, teríamos a seguinte visualização:

> *Error Inactive | 1/13/2019 8:19:01 AM 1/13/2019 08:19 | Storage D | Call home disabled | Call home not created | 3 (recorrências nos últimos 30 dias) | Com edundância | Criticidade 7 | Volume utilizado: 65%*

Entretanto, tal quantidade de informações em conjunto gera uma demora na análise do real significado da falha visto que demanda um bom tempo na análise de todos os campos. Adicionalmente, também demonstra o quanto tal problema é mal acondicionado, embora saiba-se como os fatores influenciam na criticidade da falha, não é possível determinar facilmente o quanto cada um influencia ou como tais fatores se relacionam entre si. Sendo assim, métodos de visualização serão discutidos no próximo item a fim de propor um modelo que auxilie na identificação de vários fatores em conjunto.

IV. Análise visual

A aplicação da análise visual é amplamente utilizada para auxiliar o processo de tomada de decisão de problemas complexos e mal condicionados, pois pode gerar *insights* que não seriam possíveis sem o auxílio visual.

Dentre as diversas técnicas e estudos a respeito da analise visual, podemos destacar as "leis de Gestalt" [1], que configuram um grupo de oito leis que descrevem diferentes técnicas e efeitos que podem ser utilizados para facilitar o processo de visualização e associação de informações, sendo útil quando necessário perceber diversas partes como um todo, ou possuir uma clara distinção dentre objetos.

Dentre estas oito leis, pode-se destacar a lei da semelhança, onde elementos relacionados utilizam o mesmo padrão de cor, facilitando a associação pré atentiva, e criando a ideia de unidade única, dessa forma, é intuitivo agrupar os círculos brancos e pretos em grupos separados. Tal lei pode ser utilizada quando na tentativa de agrupar diferentes falhas ou dados distintos em torno de uma mesma falha, em uma única associação.

Também vale ressaltar outra lei de Gestalt, a lei da continuidade, na qual padrões contínuos podem ser identificados. De acordo com a mesma, podemos prever a continuidade de formas a partir de padrões como texturas e cores, devido ao fato de preferirmos figuras fluídas e sem interrupções. Tal lei pode ser útil, visto que é importante prever recorrências de mesmas falhas ou associações entre falhas que apresentam similaridade de tempo ou equipamento.

V. Relacionando os dados aos fatores de criticidade

A fim de prover uma melhor visualização dos dados coletados, primeiramente iremos analisar como os dados que possuímos relacionam-se com os fatores de criticidade descritos no item III, agrupando-os sob diferentes pontos de vista, tornando-os também aplicáveis aos modelos de análise visual explanados no item IV.

Analisando a criticidade das falhas, os tipos das mesmas podem ser categorizados em uma escala de criticidade dos eventos (CE), tal escala pode ser facilmente obtida através da

experiência dos analistas e do significado de cada falha (inoperância total, falha parcial, etc). Como exemplo, nos dados em estudo, uma falha de login de usuário é apresentada, em determinadas circunstâncias, dentro da mesma severidade de uma falha física em disco. Dentro das severidades já descritas nos eventos analisados, fez-se necessário classificar os sub-tipos de eventos de acordo com sua descrição e criticidade, definida entre 1 e 10, sendo 1 a menos crítica, e 10 a mais crítica. Também foram retiradas da análise algumas falhas que não indicam problemas em hardware, tendo caráter somente informativo de um evento ocorrido. A explicação detalhada de cada tipo de falha está presente no Apêndice B, a categorização das falhas que realmente indicam problemas em hardware está na Tabela I a seguir.

TABELA I. DEFINIÇÃO DOS VALORES DE CRITICIDADE DOS EVENTOS

Criticidade inicial	***Falha***	***Valor de criticidade atribuído***
Information	Physical tape read error	2
	Tape drive failue	3
Warning	System checks disabled	3
	Dvd drive write error	
	DVD drive read error	
	DVD drive mount error	
	Only 1 spare disk available	4
	Call home disabled	6
	Server disk failure	7
Error inactive	Call home disabled	6
	Call home created	7
	Cache disk error	10

Conforme é possível verificar na Tabela I, há um ganho com a caracterização da falha por um valor de criticidade numérico. Enquanto apresentados somente como linhas e com uma cor preenchida ao fundo, alertas de "*call home disabled*" são apresentados com uma criticidade maior do que aqueles que indicam *server disk failure* em *warning*, e em conjunto com os alertas de "*cache disk error*", sendo este último o mais crítico.

Também foram coletadas informações a respeito das aplicações que armazenam dados nos servidores analisados. As aplicações identificadas foram posteriormente agrupadas de acordo com os servidores de armazenamento utilizados, e suas respectivas criticidades. Aplicações contando com redundância em múltiplos servidores de armazenamento foram excluídas da análise, uma vez que mesmo uma falha total em um servidor de armazenamento não acarretaria em um impacto direto e crítico no funcionamento da aplicação, e trariam uma complexidade que extrapola os objetivos deste trabalho.

As aplicações foram separadas em cinco grupos distintos, de acordo com as informações de criticidade já disponíveis e de conhecimento do ambiente analisado, disponíveis no apêndice desse artigo.

Desse modo, o primeiro agrupamento realizado durante a pesquisa, foi a atribuição de aplicações (e suas determinadas prioridades) à cada servidor *storage*. Tal visualização permite identificar os ambientes com mais aplicações críticas ao negócio da empresa, bem como sua relação à totalidade de aplicações existentes.

Após extração das informações, foi possível elaborar a Tabela II e um gráfico para análise visual (Figura 3), disponíveis a seguir.

TABELA II. DEFINIÇÃO DE CRITICIDADE CONFORME APLICAÇÕES

Servidor	***Total de apps***	***Apps P1***	***Apps P2***	***Apps P3***	***Apps P4***	***Apps P5***
Storage A	49	2	6	36	3	2
Storage B	91	6	4	37	38	6
Storage C	3	0	0	3	0	0
Storage D	92	4	2	71	13	2
Storage E	111	16	7	77	7	4
Storage F	46	10	4	23	7	2
Storage G	105	16	7	71	6	5
Storage H	60	11	4	35	9	1
Storage I	46	6	3	31	4	1

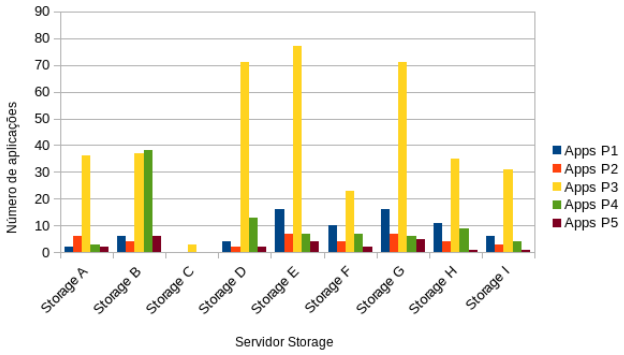

Fig. 1. Distribuição de aplicações por servidor *storage*.

Através da análise gráfica dos dados, tornou-se possível visualizar sutis diferenças entre as criticidades relativas de cada servidor, como por exemplo, o *Storage* G, sendo responsável por aproximadamente 17% do total de aplicações, mas com cerca de 23% das aplicações de prioridade 1, ao passo que o *Storage* D concentra cerca de 15% do total de aplicações, porém apenas 6% das aplicações de prioridade 1, reduzindo assim significativamente sua criticidade relativa ao ambiente total.

Através destes dados, é possível estimar qual a criticidade de cada *storage* no ambiente, definindo uma criticidade relativa (CR) para os mesmos. Sendo P1, P2, P3, P4 e P5, respectivamente, a quantidade de aplicações de prioridade 1 à 5 contidas em um único *storage*, é possível mensurar um valor através do percentual de cada aplicação em um *storage* com relação ao parque, e atribuindo um peso relativo para cada app (pr), é possível atribuir um valor numérico para a criticidade deste *storage* relativamente ao parque. A fórmula 1 que define esta criticidade está a seguir.

$$CR = \frac{(P1/\sum P1)*pr1+(P2/\sum P2)*pr2+(P3/\sum P3)*pr3+(P4/\sum P4)*pr4+(P5/\sum P5)*pr5}{(pr1 + pr2 + pr3 + pr4 + pr5)} \quad (1)$$

Através da experiência no ambiente é possível definir os valores para cada prioridade de aplicações, sendo as mesmas "pr1" à "pr5", definimos para o caso em estudo os valores, respectivamente: 12, 9, 5, 3 e 1. A soma de todas estas prioridades (30), justifica o valor da divisão na fórmula 1.

Outro fator que dificulta a tomada de decisão são alertas redundantes, pois, em alguns casos, uma mesma falha gera mais de um alerta, a fim de identificar tais alertas redundantes, foram gerados os gráficos nas Figuras 4, 5 e 6, nos quais os alertas para cada criticidade (*Information, Warning e Error*) estão dispostos no tempo (o tempo, neste caso, sendo somente para fins de análise superficial, está apresentado de forma genérica). Os gráficos gerados estão nas Figuras 2 à 4 a seguir.

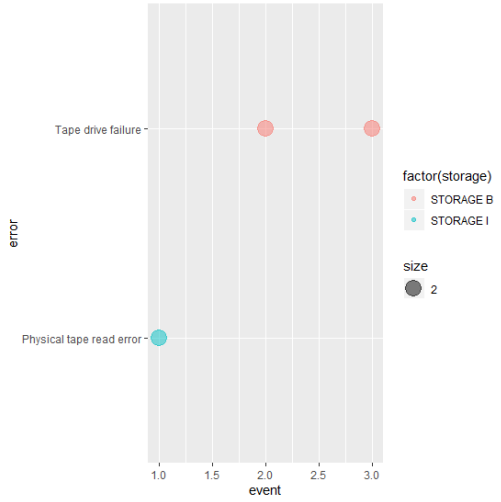

Fig. 2. Distribuição de alertas para a criticidade Information.

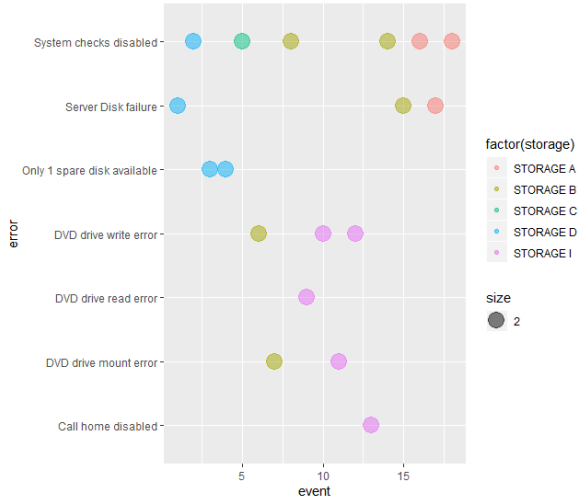

Fig. 3. Distribuição de alertas para a criticidade Warning.

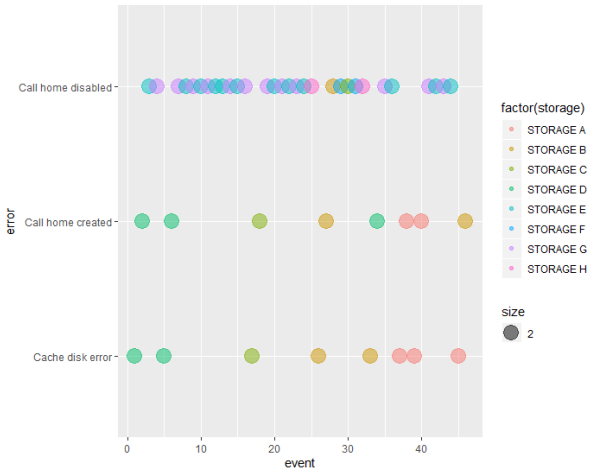

Fig. 4. Distribuição de alertas por criticidade *error inactive*.

Conforme é possível verificar na Figura 4 nos eventos *error inactive*, para cada evento de *cache disk error* gerado, também é gerado automaticamente um evento do tipo *call home created*, que é responsável pelo acionamento do técnico de campo para correção do problema identificado, sendo responsabilidade do time de operação apenas o acompanhamento da execução do serviço em um intervalo de tempo aceitável. Sendo assim, estando tais eventos relacionados, pode-se fazer a simplificação para a análise visual.

Outro fator importante para análise de criticidade de um alerta é a sua recorrência, conforme explicado no item III, alertas recorrentes podem indicar problemas graves de bugs em software que afetam o hardware ou mesmo, equipamentos com defeitos de fábrica.

A fim de avaliar tal fator, pode-se efetuar a análise de recorrência de falha para um mesmo equipamento em um dado intervalo de tempo. De forma simples, a frequência de ocorrência de uma falha pode ser dada pelo somatório de eventos (e) ocorridos no período de tempo que a mesma ocorreu dividido pelo período de tempo (t) analisado.

$$FF = \frac{\sum e}{t} \quad (2)$$

Outro fator relacionado à criticidade, e correlacionado à frequência da falha, é o tempo médio para recuperação da mesma, visto que uma falha recorrente possuirá um bom banco de dados para análise deste tempo. Tal dado não estava disponível para este estudo.

VI. Método Proposto

A fim de verificar a eficácia do que foi exposto até agora, podemos utilizar tais dados em gráficos, com o intuito de analisar as correlações entre os dados e analisar se é possível gerar uma visualização pré atentiva que melhore a tomada de decisão.

Para tanto, foi utilizado o software RStudio, a fim de gerar diferentes visualizações. Como os alertas ocorrem durante o tempo, podemos utilizar os valores definidos para a criticidade relativa (CR) do *storage*, frequência de falha (FF) e criticidade do evento (CE), em gráfico cujo eixo x seja o horário de falha do alerta. Para fins de estudo, serão utilizados somente alguns alertas do universo total de eventos.

Como exemplo, na Figura 5 temos um gráfico no qual temos a data de ocorrência do alerta no eixo x, a criticidade relativa (CR) no eixo y, cada *storage* definido por uma mesma cor, e a criticidade do evento como o tamanho do círculo na falha.

Tal visualização foi gerada baseada nos princípios exemplificados de Gestalt no item IV, cores semelhantes agrupadas e próximas valem-se do princípio da continuidade, a fim de auxiliar a identificar padrões de falhas, por outro lado círculos semelhantes entre si (cor ou tamanho) fazem uso da lei da semelhança para gerarem correlação.

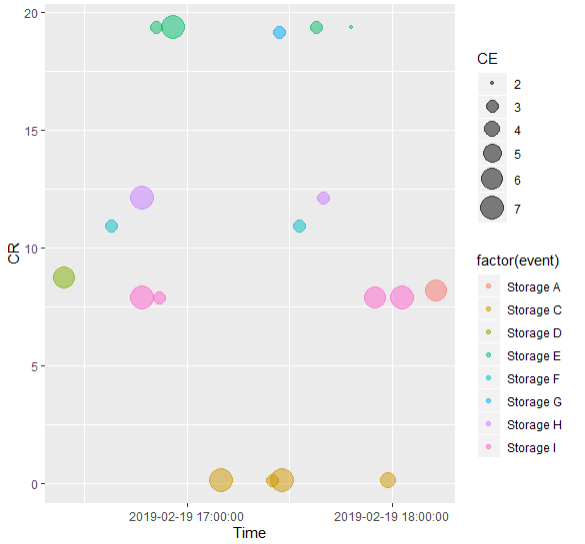

Fig. 5. Gráfico amostrando a criticidade relativa das falhas pelo tempo, com as cores para identificar os *storages*, e o tamanho dos pontos indicando a criticidade do evento.

Embora tenhamos um gráfico capaz de auxiliar na decisão de priorização do alerta, visto que, quanto maior o círculo, maior a criticidade da falha, e quanto mais acima no gráfico, maior a criticidade do *storage* que falhou, ainda assim, temos diversos fatores que não são amostrados no gráfico, como a frequência de recorrência das falhas e o tempo médio de recuperação.

A fim de amostrar os dados aqui estudados que determinam a criticidade da falha, podemos propor um fator que englobe os mesmos, sendo assim, de forma simples, podemos multiplicar estes fatores, e, com o uso de uma interface interativa, estudar o quanto esta solução é efetiva.

Conforme definido no item V, temos a criticidade relativa do *storage* (fórmula 1), a criticidade do evento (CE, definido na Tabela I), e a frequência de falha (fórmula 2). Também iremos inserir um valor para a Tempo Estimado de correção (TEC), neste trabalho tal valor é arbitrário, pois não há como aquisitá-lo a partir dos dados disponíveis, mas pode ser facilmente obtido através da média de resolução dos respectivos problemas. A fórmula 3 à seguir amostra o modelo proposto, retornando um valor que chamaremos de Taxa de Risco (TR):

$$TR = FF \times CR \times CE \times TEC \quad (3)$$

Um exemplo de como seria uma visualização utilizando o TR está na Figura 6 a seguir.

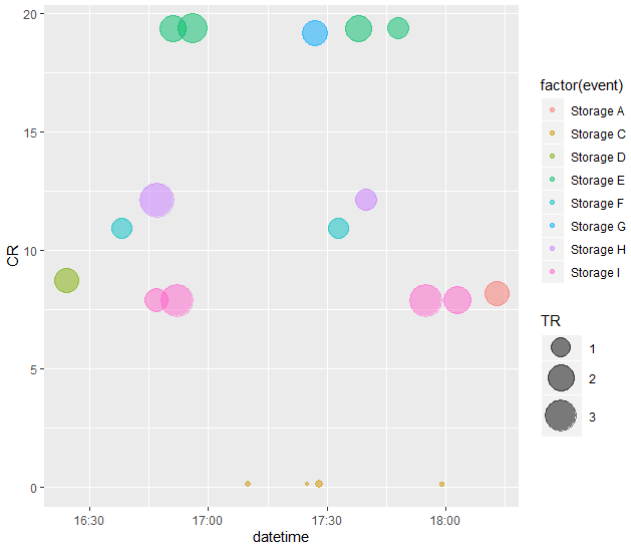

Fig. 6. Gráfico amostrando a criticidade relativa das falhas pelo tempo, com as cores para identificar os *storages*, e o tamanho dos pontos utilizando o indicador proposto de taxa de risco.

É possível verificar diferenças entre os dois gráficos, pois, devido ao uso de vários fatores em conjunto, é possível destacar a recorrência no *Storage* E (círculos verdes na parte superior do gráfico), assim como as falhas no *Storage* C tornaram-se menos relevantes (círculos amarelos na parte inferior do gráfico).

Outro ponto de melhoria, aplicado na interface interativa (Figura 7), é a visualização dos dados relacionados aos diversos fatores no pontos, a Figura 10 à seguir amostra esta funcionalidade, e o quanto a mesma pode agilizar a tomada de decisão, pois fornece rapidamente ao usuário diversos valores numéricos (de forma qualitativa) que antes necessitavam de vários minutos para análise com os dados sendo apresentados como linhas de uma tabela.

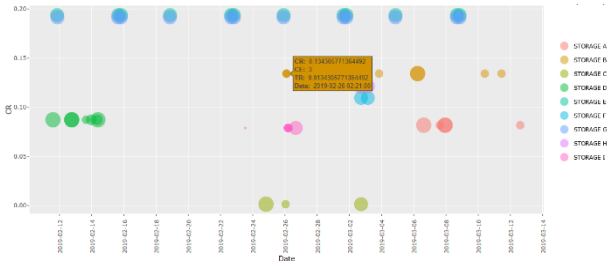

Fig. 7. Gráfico amostrando um universo de falhas em uma interface interativa.

VII. Conclusão

Através do uso de interfaces interativas, com dados sumarizados e com o uso de métodos de análise visual é possível, com o método proposto, auxiliar na tomada de decisão e agilizar a priorização de falhas mais críticas quando comparado ao método mais comum de apresentação das falhas em linhas de uma tabela.

A capacidade do método de agrupar em uma única visualização diversos dados, já aplicadas análises no ambiente como um todo (criticidade relativa às aplicações, frequência de falha, criticidade dos eventos e tempo estimado de correção) e trazer tais dados de forma qualitativa em um gráfico, mas também disponibilizando um detalhamento dos

valores contidos de forma rápida através de uma interface interativa representa um ganho no suporte à tomada de decisão, pois sumariza a criticidade do evento. Assim, ao verificar que o alerta possui uma frequência de falha alta, ou uma criticidade relativa alta, prove ao analista insumos para que o mesmo verifique de forma mais acertiva a falha.

Contudo, é necessário notar que o modelo proposto possui limitações técnicas ainda por serem estudadas, como a necessidade de um modelo que inclua as informações de equipamentos com aplicações redundantes assim como o volume de dados e tráfego nos mesmos, o que traria problemas no modelo matemático proposto para a Taxa de Risco, que, embora tenha se mostrado efetivo para o cenário em estudo, carece de testes em outros ambientes para mais validações e um provável refinamento.

Além disso, para contar com uma melhor efetividade, o usuário deve dispor de uma série de dados relevantes do ambiente analisado, incluindo a quantidade de aplicações suportadas, em quais servidores elas se encontram, e sua criticidade para o sistema em geral. Tais dados podem não estar facilmente disponíveis em todos os ambientes.

Apêndice A

Descrição das prioridades de cada aplicação, de 1 a 5, da maior prioridade para a menor:

- **Prioridade 1:** Aplicações vitais para o cliente. A falha de tais aplicações, mesmo que por apenas alguns minutos, podem afetar severamente o negócio da companhia, resultar em penalidades legais e má exposição nas mídias.
- **Prioridade 2:** Aplicações críticas para o cliente. Falhas nessas aplicações devem ser tratadas como alta criticidade, porém possuem um menor impacto quando comparado com aplicações prioridade 1.
- **Prioridade 3**: Aplicações de média criticidade. Embora causem impacto para o cliente, não afetam serviços vitais para o negócio, e podem suportar um período maior de indisponibilidade.
- **Prioridade 4:** Aplicações de apoio. São consideradas aplicações de apoio aquelas que proveem funções e ferramentas auxiliares para a execução de tarefas administrativas.
- **Prioridade 5:** Aplicações não críticas. São aplicações que geram pouco ou nenhum impacto para o negócio do cliente, tais como aplicações de teste e desenvolvimento. Aplicações prioridade 5 geralmente não possuem acordos de nível de serviço, ou não impactam o cliente no caso de falhas.

Apêndice B

Especificação dos tipos de eventos, suas descrições, e criticidade associada.

- ***Information Inactive***
  - *Add, modify, or delete user*: Evento relacionado a alteração ou remoção de usuários em um servidor *storage*. Removido da análise pois não está associado a um problema de hardware.
  - *Events clear*: Limpeza de eventos salvos no servidor *storage*. Removido da análise pois não está associado a um problema de hardware.
  - *Insert virtual volumes*: Inserção de volumes virtuais a serem usados pela aplicação. Removido da análise pois não está associado a um problema de hardware.
  - *Login/Logout*: Atividade de Login ou Logout de um usuário em um determinado servidor *storage*. Removido da análise pois não está associado a um problema de hardware.
  - *Modify user password*: Alteração de senha realizada por um usuário para um servidor *storage* específico. Removido da análise pois não está associado a um problema de hardware.
  - *Physical tape ejected*: Remoção de fitas físicas gerenciadas por um dado servidor *storage*. Removido da análise pois não está associado a um problema de hardware.
  - *Physical tape inserted*: Inserção de fitas físicas gerenciadas por um dado servidor *storage*. Removido da análise pois não está associado a um problema de hardware.
  - *Physical tape read error*: Erro de leitura de fita física. Criticidade 2
  - *Tape drive failure*: Erro de hardware em um drive de leitura/gravação de fitas físicas. Criticidade 3
- ***Warning Inactive***
  - *System checks disabled:* Checagem de sistema desabilitado. Pode ser iniciado por um erro ou solicitação de um usuário. Criticidade 3
  - *DVD drive write error:* Erro no drive de DVD durante um processo de gravação. Criticidade 3
  - *DVD drive read error:* Erro no drive de DVD durante um processo de leitura. Criticidade 3
  - *DVD drive mount error:* Erro no drive de DVD durante um processo de solicitação de mídia de DVD. Criticidade 3
  - *Only 1 spare disk available:* Apenas um disco de reserva para uso em caso de falha de um disco de produção. Criticidade 4
  - *Call home disabled:* Sistema de solicitação de reparo desabilitado. Pode ser iniciado por um erro ou solicitação de um usuário. Criticidade 6
  - Server disk failure: Falha irreparável em um disco de produção contendo o banco de dados do servidor *storage*. Criticidade 7
- ***Error Inactive***
  - *Login/Logout:* Erro durante o processo de Login ou Logout. Geralmente relacionado a problemas de usuário/senha incorretos. Removido da análise pois não está associada a um problema de hardware.
  - *Call home disabled**:*** Sistema de solicitação de reparo desabilitado. Pode ser iniciado por um erro ou solicitação de um usuário. Criticidade 6
  - *Call home created:* Sistema de solicitação de reparo foi acionado e criou uma nova solicitação de reparo técnico. Criticidade 7
  - *Cache disk error:* Falha irreparável em um disco de produção contendo dados de aplicação. Criticidade 10

Exemplos de eventos do tipo "*Warning Inactive", "Error Inactive"* e *"Information Inactive".*

1. Warning Inactive 3/13/2019 9:11:38 PM 3/13/2019 21:11 STORAGE B Server disk failure Call Home Initiated

O primeiro caso descreve um evento do tipo "*Warning Inactive"*, no servidor *Storage* B, sob a descrição "*Server disk*

failure". Ao aplicar a fórmula de criticidade relativa para o evento, que possui CE = 8, obtemos:

$$CR = \frac{(6/71)*12+(4/37)*9+(37/384)*5+(38/87)*3+(6/24)*1}{30}$$

$$CR = \frac{4.029}{30}$$

CR = 0.1343, ou CR = 13.43%

Assim como a frequência de falha:

$FF = (\sum e/\sum t)*1440$

$FF = (2/43200) = 4{,}58 \times 10^{-5}$

Definindo um tempo estimado de correção: TEC = 1440

É possível calcular a taxa de risco (TR):

$TR = 0.1343 \times 4{,}58 \times 10^{-5} \times 1440 \times 8$

TR = 0.0709, ou TR = 7.09%

2. Error Inactive 3/13/2019 4:42:49 PM 3/13/2019 16:42 STORAGE A System Call home created Call Home Initiated

O segundo caso analisado consiste um evento do tipo "*Error Inactive"*, descrição "*Call home created"* para o servidor *Storage* A, que possui CE = 9. Nesse cenário temos:

$$CR = \frac{(2/71)*12+(6/37)*9+(36/384)*5+(3/87)*3+(2/24)*1}{30}$$

$$CR = \frac{2.453}{30}$$

CR = 0.08176, ou CR = 8.18%

$FF = (\sum e/\sum t)$

$FF = (3/43200)$

Determinando TEC = 1440, temos:

TR = 0.0736, ou TR = 7.36%

Alterando o TEC para 10080, teríamos:

TR = 0.5151, ou TR = 51.51%

3. Information Inactive 3/13/2019 12:58:02 PM 3/13/2019 12:58 STORAGE D Physical Cartridge Physical tape read error Call Home Not Required

O caso seguinte se aplica ao servidor *Storage* D, com um evento do tipo "*Information Inactive"* e descrição "*Physical tape read error"*.

$$CR = \frac{(4/71)*12+(2/37)*9+(71/384)*5+(13/87)*3+(2/24)*1}{30}$$

$$CR = \frac{2.6186}{30}$$

CR = 0.08728, ou CR = 8.73%

$FF = (\sum e/\sum t)$

$FF = (4/43200)$

TEC = 10080

TR = 0.08728*0.9333*2

TR = 0.1629, ou TR = 16.29%

REFERENCES

[1] D. Keim, J. Kohlhammer, and G. Ellis, "Mastering the information age: solving problems with visual analytics", 2010.