VIRTUALIZAÇÃO DE SISTEMAS DE SUPERVISÃO NA SAMARCO MINERAÇÃO[1]

Pablo Drumond[2]
Flávio Thimótio[3]
Ricardo Bergmann[4]
Márcio Aurélio dos Santos[5]

Resumo

Com a evolução dos sistemas de supervisão, a configuração de hardware deixou de conter apenas um par de servidores de aplicação. Este cenário, caracterizado pela maior complexidade na definição da arquitetura, induziu os profissionais de automação a superestimar os ativos, onerando e gerando a subutilização dos recursos. Diante desse panorama, a virtualização, aliada à consolidação do conceito de computação em nuvem, passou a estar em evidência na TA. Na prática, são poucos os departamentos de automação que já fazem uso desse novo modelo. À vista disso, o presente trabalho propõe a formulação de boas práticas para virtualização de sistemas de supervisão, utilizando como plano de fundo a aplicação da solução VMware vSphere 5 na Samarco Mineração. Para alcançar esse objetivo, o estudo recomenda a distinção entre ambientes de produção e teste, sugere métricas para recursos virtualizados e discute pontos do Plano de Recuperação de Desastres. A tolerância à falha e o consequente aumento da disponibilidade são a base para defesa da virtualização. Embora o gerenciamento centralizado, com medição e balanceamento de recursos entre os hosts, não sejam considerados resultados, são eles os verdadeiros responsáveis por tornar a arquitetura escalável e permitir a redução do custo de aquisição nas expansões.

Palavras-chave: Virtualização; Sistemas de supervisão; Plano de recuperação de desastres.

VIRTUALIZATION OF SCADA SYSTEMS AT SAMARCO

Abstract

With the evolution of SCADA systems, hardware configuration is no longer defined by only a couple of application servers. This scenario, characterized by greater complexity in the architecture definition, has induced automation professionals to overestimate the assets, burdening and generating underutilization of resources. With this overview, virtualization, is now being seen in the automation technology. In fact, few automation departments use this new model. Thus, this paper proposes to formulate best practices for virtualization of SCADA systems, using as background the use of *VMware vSphere 5* solution in Samarco. To achieve this goal, this study recommends distinction between production and test environments, suggests metrics for virtualized resources and discusses points of the Disaster Recovery Plan.

The fault tolerance and the availability improvement are the main aspects in defense of virtualization. Although centralized management, with measurement and resources balancing among hosts, are not considered results, they are the true responsible for making the architecture scalable and allowing cost reduction in expansions.

Key words: Virtualization; SCADA; Disaster recovery plan.

[1] *Contribuição técnica ao 17° Seminário de Automação e TI Industrial, 24 a 27 de setembro de 2013, Vitória, ES, Brasil.*

[2] *Engenheiro de Controle e Automação. Analista de Controle. IHM Engenharia. Belo Horizonte, MG, Brasil.*

[3] *Engenheiro de Controle e Automação. Mestre. Chefe do Departamento de Automação. Samarco Mineração. Mariana, MG, Brasil.*

[4] *Engenheiro de Controle e Automação e Engenheiro de Computação. Analista de Controle. IHM Engenharia. Belo Horizonte, MG, Brasil.*

[5] *Analista de Sistema. Analista de Automação. Samarco Mineração. Mariana, MG, Brasil.*

1 INTRODUÇÃO

Lowe[1] define virtualização como a abstração de recursos computacionais. Enquanto Shah,[2] considerando o termo muito abrangente, o restringe como uma tecnologia que permite a execução simultânea de múltiplos sistemas operacionais através da alocação de recursos de um mesmo hardware físico.
Segundo Portnoy,[3] a primeira virtualização foi realizada em mainframes IBM System/370 na década de 60, porém somente na década posterior, Popek e Goldberg[4] definiram os requisitos necessários para uma arquitetura computacional suportar virtualização. Além disso, promoveram o conceito de *Virtual Machine Monitor*, ou *Hypervisor*, como é conhecida hoje a camada que permite o compartilhamento de recursos entre máquinas virtuais, apresentado na Figura 1.

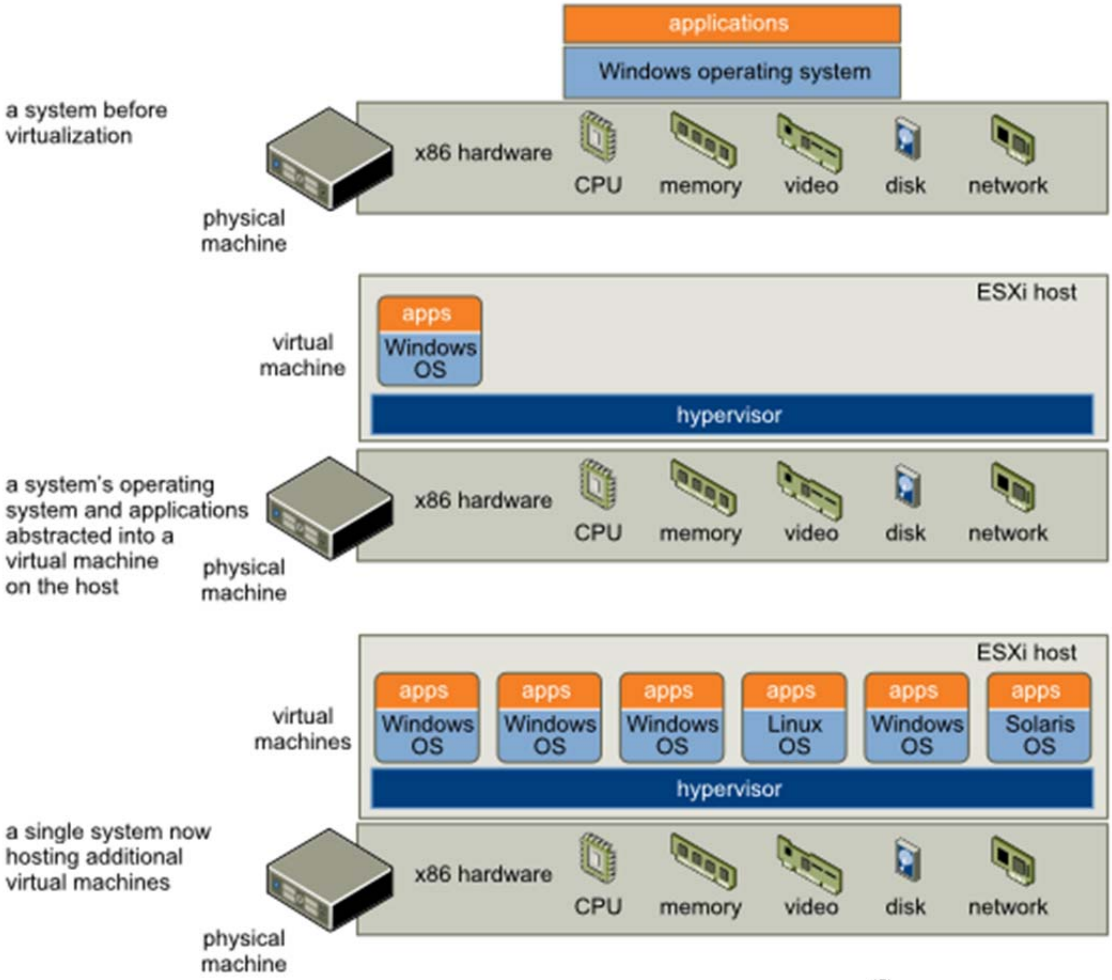

Figura 1 - Hypervisor e compartilhamento de recursos.[5]

Essencialmente, esse conceito não sofreu modificações, porém só alcançou notoriedade nos últimos anos, quando o termo *Cloud Computing*, definido por Sosinsky[6] como uma abstração do pool de recursos físicos em recursos virtualizados e no provisionamento dinâmico deles para aplicações e serviços, ganhar destaque.
Dentre as vantagens apresentadas em ambientes virtualizados podem-se destacar:

- consolidação de servidores;
- independência de hardware subjacente;

- aumento do tempo de obsolescência da solução;
- balanceamento dinâmico de carga;
- agilidade na recuperação de desastres;
- ambiente de teste para implantação.

Na automação, com a evolução dos sistemas de supervisão, a configuração de hardware deixou de conter apenas um par de servidores de aplicação, para incluir controladores de domínio, historizadores, repositórios de objetos, servidores web, além, claro, das estações de operação e engenharia. Este cenário, caracterizado pela maior complexidade no processo de definição da arquitetura, induziu os profissionais da área a superestimar a especificação dos ativos, onerando e gerando a subutilização dos mesmos. Diante desse panorama, a virtualização, aliada a consolidação do conceito de computação em nuvem nos ambientes de TI, passou a estar em evidência também na TA.

Os principais players de automação industrial iniciaram a homologação dos softwares de supervisão para ambientes virtualizados em 2009. No entanto, não existe na literatura especializada uma informação confiável da primeira planta a adotar essa tecnologia para sistemas de automação. Na prática, são poucos os departamentos de automação que já fazem uso desse novo modelo, seja pelo desconhecimento ou conservadorismo dos profissionais da área, e/ou pelo rotineiro atraso na compatibilização das aplicações pelos fornecedores de software.

À vista disso, e com o atingimento da maturidade das soluções, o presente trabalho propõe a formulação de boas práticas para virtualização de sistemas de supervisão, utilizando como plano de fundo a aplicação da solução *VMware vSphere 5* em quatro áreas de processo da Samarco Mineração, unidade Germano.

2 MATERIAIS E MÉTODOS

2.1 Boas Práticas

Dentre as melhores práticas mencionadas por Miller,[7] pode-se destacar e adaptar para a realidade da automação as seguintes:

- Avaliar as necessidades dos sistemas a serem virtualizados para o correto dimensionamento do pool de recursos. Portanto, o presente trabalho sugere a construção de um plano de virtualização, contendo as necessidades das aplicações envolvidas no sistema de automação em termos de uso de CPU, ou cores, memória primária (RAM), memória secundária (espaço em disco) e interfaces de rede;
- Controlar a proliferação de máquinas virtuais: com os hipervisores atuais, a clonagem de máquinas virtuais se tornou uma tarefa simples, podendo acarretar:
  - Falhas de segurança: *patches* e atualizações de segurança podem não ter sido aplicadas aos sistemas operacionais antes do ingresso na rede;
  - Conflitos de rede, pela duplicidade de endereços, normalmente fixados nos ambientes de automação; instabilidade no serviço de diretório, pela duplicidade nos identificadores do sistema operacional das máquinas;
  - Ilegalidade: deve ser observada a necessidade de aquisição de novas licenças para os sistemas operacionais.

Além das práticas herdadas da TI, propõem-se ainda:

- Não vincular a estabilidade do sistema de supervisão às funcionalidades do hipervisor. Apesar das ferramentas de gerenciamento para ambientes

virtualizados contarem com recurso de migração de máquinas entre hosts físicos, sem *downtime*[1], alguns softwares de automação homologados, não são compatíveis com essa funcionalidade. A mesma observação pode ser aplicada à utilização de *snapshots*, onde existem relatos de desequilíbrios em algumas soluções. Esse conselho pode parecer ser óbvio para um profissional de TA, mas não para um profissional de TI, atual responsável pela proposição de arquiteturas com virtualização;

- Construir um ambiente de teste, espelho do ambiente de produção, fundamental para projetos de migração como também para aplicação de *Service Packs* e *Patches* não somente relativos ao sistema operacional, como também aqueles fornecidos para os softwares de automação, visando a melhoria do panorama atual, assim pontuado:
  - Poucos fabricantes testam os *KBs*[2] para Microsoft Windows, certificam a compatibilidade com os produtos, e liberam a instalação para os clientes;
  - Poucas empresas possuem um ambiente teste dos *Service Packs* e *Patches* liberados pelo fornecedor de softwares de automação, afinal, construí-los em bancada é dispendioso;
  - Quando existe necessidade de instalação de uma atualização crítica é requerido um agendamento de parada e a construção de um plano de contingência com eficácia não avaliada, pela inexistência de um ambiente de teste.

É importante observar que toda essa plataforma de teste deve ser levada em consideração na etapa de dimensionamento do pool de recursos, com intuito de não prejudicar aquela de produção.

2.2 Métricas

Para construção de métricas de apoio à definição de pool de recursos para sistema de automação foram adaptadas tabelas sugeridas por Rockwell(8) e Wonderware.(9) Após equalização das responsabilidades das máquinas em cada solução, obtiveram-se necessidades típicas apresentadas na **Erro! Fonte de referência não encontrada.**.

Tabela 1 – Necessidades típicas

Máquina	*vCPU*[3]	*vCPU/Core*	Memória	Disco
Servidor de Aplicação	04	02	8GB	100GB
Servidor de Historização	02	02	8GB	200GB
Servidor de Domínio	01	02	2GB	80GB
Estação de Operação	01	04	2GB	80GB
Estação de Engenharia	01	02	4GB	80GB

Em uma arquitetura contendo 06 servidores de aplicação, 01 servidor de historização, 2 servidores de domínio, 19 estações de operação e 04 estações de engenharia seria necessário um pool de recursos definido na

Tabela 2.

[1] vMotion na solução VMware vSphere e Live Migration na solução Microsoft Hyper-V

[2] Terminologia adotada pela Microsoft para atualizações dos seus produtos, descritas em sua base de conhecimento.

[3] Processadores virtuais atribuídos às máquinas virtuais.

Tabela 2 – Pool de Recursos

	Core	**Memória**	**Disco**
Recursos físicos calculados	20,75	114GB	2,8TB
Recursos físicos com reserva de 30%	~27	~150GB	~3,6TB

Após a estimativa das necessidades em termos de recursos físicos, é necessário definir o número de hosts responsáveis pela execução do hipervisor. O mínimo recomendado para configurações de alta disponibilidade é 03, e o dimensionamento deve ser realizado de modo que o *cluster* seja capaz de prover recursos, sem diminuição de desempenho, em caso de falha em um host. Levando-se em consideração 08 *cores*[4] por host, seriam requeridos 5 deles, com 150GB de memória RAM e um *storage*[5] com 3,6TB. A Figura 2 compara a arquitetura tradicional e virtualiza para o cenário citado.

Ainda no que tange a construção de métricas para um sistema de automação, boas práticas devem ser ressaltadas:

- É recomendada a reserva de recursos para os servidores de aplicação, através de ferramentas de gerenciamento centralizadas - mais exatamente processamento - de modo que em surtos de demanda o bom desempenho seja preservado.
- É necessário reservar 2GB de memória RAM para que o hipervisor realize operações de escrita/leitura e comunicação.
- É imprescindível um bom planejamento de disco de forma a evitar a superestimação do recurso e prevenção do crescimento sob demanda, essa última causa fragmentação e perda considerável de desempenho.

[4] Apesar de o recurso *Hyperthread* ser recomendado pelos fabricantes é razoável para etapa de dimensionamento não considera-lo.

[5] Hardware dedicado para armazenamento de dados. As definições de métricas para escrita e leitura através da rede nas soluções de storage do mercado estão além do escopo desse trabalho.

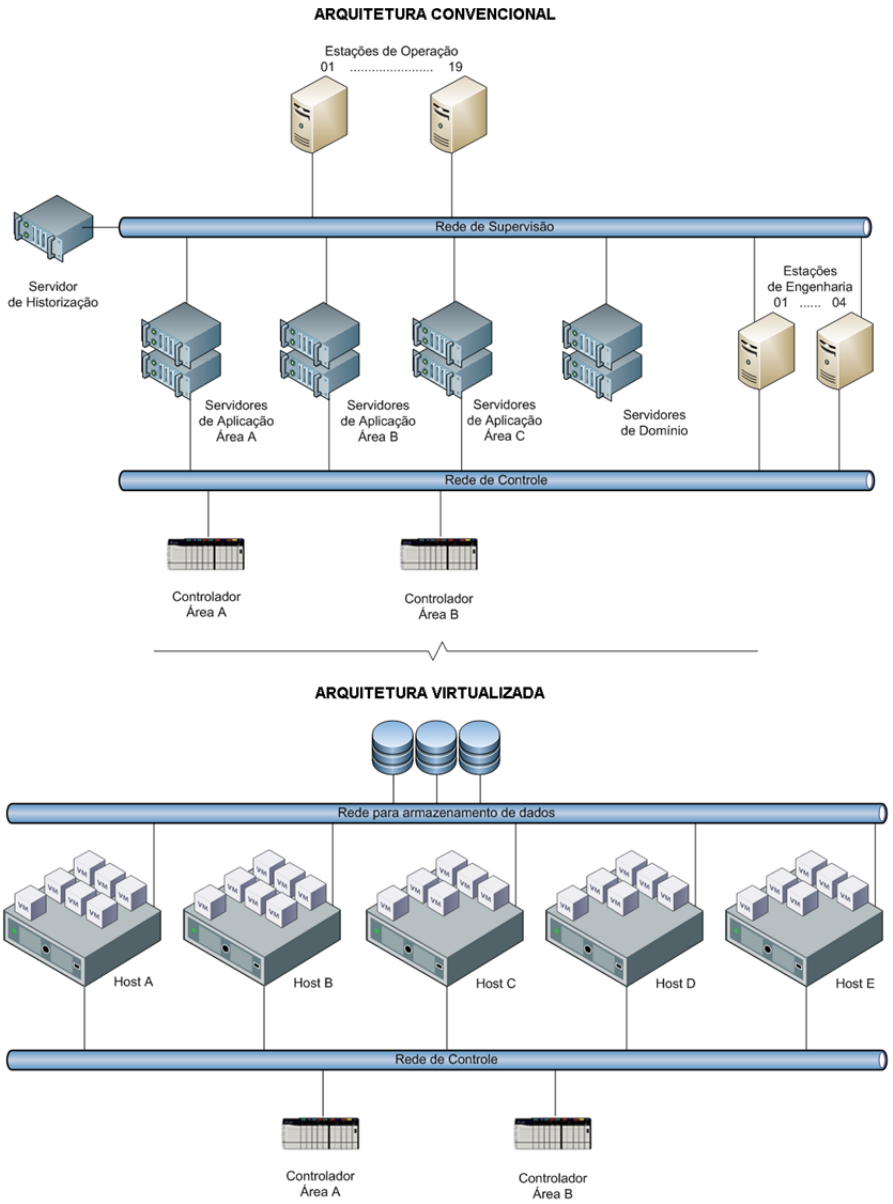

Figura 2 - Comparação de Arquiteturas

2.3 Plano de Recuperação de Desastres

De acordo com Snedaker,[11] o plano de recuperação de desastres, lida com os impactos imediatos de um evento sobre um determinado sistema, descrevendo os passos necessários para que a continuidade do negócio seja restabelecida.

Para um sistema de automação, o plano abrange a localização do evento, a avaliação dos impactos e a estratégia de recuperação, nesse último incide a maior contribuição da virtualização, através de ferramentas como *Fault Tolerance*, que tornam os hipervisores capazes de detectar *crash* nos hosts e migrar as máquinas virtuais para outro host do mesmo datacenter; *High Availability*, que permitem a realização de operações de escrita/leitura em duas máquinas virtuais duplicadas, possibilitando assim, redundância instantânea em caso de falha do host; *Site Recovery*, que permite a recuperação completa de um site em outro site backup.

Em um ambiente convencional, como apresentado no tópico **Erro! Fonte de referência não encontrada.**, a recuperação do sistema envolveria, no mínimo: a substituição de hardware, quando disponível, onerosa, já que constitui imobilização

de ativos; e a restauração de imagens/backup, o que levaria horas mesmo para profissionais experientes e treinados.
Outra vantagem da adoção dessa tecnologia baseia-se na facilidade de aplicação dos passos contidos no plano de recuperação em um ambiente de teste, corroborando para a construção proposta no item **Erro! Fonte de referência não encontrada.** e permitindo que a validação de rotinas de backup e criação de imagens sejam realizadas.

3 RESULTADOS

Após a avaliação das melhores práticas e construção de métricas para sistemas de automação, elaborou-se a arquitetura para o projeto de restruturação dos sistemas de supervisão da Usina de Concentração 01, Mina, Planta de Britagem e Planta de Reagentes da Samarco Mineração, apresentada na Figura 3. Como ferramenta de virtualização a Samarco escolheu o *VMware vSphere 5* pelos seguintes motivos:

- Nível de maturidade já atingido pelo hipervisor e liderança, com 86% de participação de mercado;(12)
- Compatibilidade e parcerias desenvolvidas com a maior parte dos fornecedores de softwares de automação.

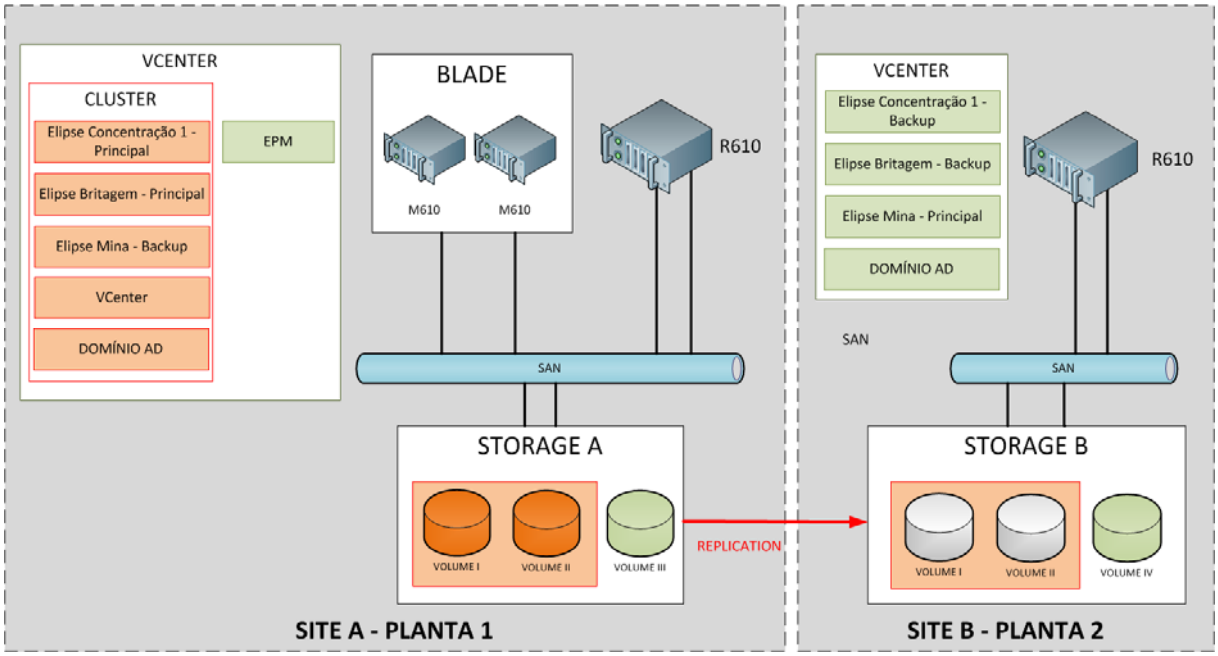

Figura 3 - Arquitetura Samarco

Como solução de hardware a Samarco, optou por uma *Blade* (Dell M1000e, com 03 lâminas Dell M610), forma construtiva que desloca a alimentação, refrigeração e interfaces de rede de dentro dos servidores para um chassi externo, e compartilha esses recursos entre vários servidores inseridos em slots. De acordo com Goldworm e Skamarok,(13),essa solução é indicada para:

- redução de espaço e aumento de eficiência;
- redução do custo total da propriedade (TCO) e custo operacional (OpEx);
- facilidade na implantação, substituição e gerenciamento.

No que se refere ao plano de recuperação de desastres, uma estratégia de replicação de dados entre os *storages* da Planta 01 e 02 foi configurada, estabelecendo uma redundância do tipo *cold standby*. Como as máquinas virtuais

estão armazenadas nos *storages*, a sincronia dos dados permite a partida das mesmas no site backup, nesse caso, Planta 02. No entanto, essa operação implica em pesado uso de rede, dessa forma, nem toda estrutura pôde ser sincronizada, apenas os servidores de aplicação e historização foram escolhidos para a replicação.

4 DISCUSSÃO

Segundo Lowe(1) o custo total da propriedade de um servidor de dados em três anos, considerando alimentação, refrigeração, manutenção e pessoas envolvidas na atividade de manutenção, está entre 3 e 10 vezes o custo do servidor propriamente dito. Deste modo, caso a Samarco optasse por um modelo convencional, em um cenário otimista onde cada servidor custa $10K, em três anos, 13 servidores, levando em consideração redundância no Site A e servidores de contingência no Site B, custariam $390K, enquanto em um cenário pessimista e virtualizado com 05 hosts custariam $150K de hardware processador, $70K para solução de armazenamento e $40K para licenciamento, totalizando $260K, uma redução superior a 33% no TCO.

Ademais, torna-se categórico o emprego da virtualização quando é avaliada a diferença do tempo necessário para a recuperação de desastre, entre os cenários descritos, em uma planta de concentração de minério de ferro.

Para que esse investimento seja capitalizado também nos projetos futuros é fundamental o uso de uma ferramenta de gerenciamento central de recursos, pela TA. É através dela que o profissional conseguirá entender a demanda e as reservas e ponderar sobre futuras aquisições.

Afora os benefícios citados nesse trabalho, novos desafios surgem em decorrência dessa adoção: o domínio da tecnologia pelo profissional de TA e entendimento das reais necessidades para construção de propostas coerentes; a administração dos recursos em um ambiente virtualizado constitui atividade fora da rotina do profissional, que tende ser reativo. O profissional deve tratar a alocação de recursos computacionais assim como trata a alocação de recurso físico para pontos de I/O ou de interfaces de redes inteligentes, equilibrando o dimensionamento enxuto, porém, com sobras para expansão e aumento de demandas. Aqui o cenário é mais fácil visto os recursos de alocação dinâmica e facilidade de expansão, quando comparados ao árduo processo de expansão de controladores e redes de campo; a implementação de políticas que limitam e definem a adequada utilização dos recursos para os diferentes tipos de aplicações, também não faz parte da cultura dos profissionais da área.

É válido, ainda, descrever quando a virtualização não é a solução apropriada para aumento de disponibilidade:

- Caso o uso das interfaces de rede seja intenso, de modo que o somatório das operações realizadas pelas máquinas virtuais que compartilham o recurso, superem a velocidade do hardware, normalmente 1Gbps;
- Caso o uso de disco seja acentuado, de maneira que as operações de escrita/leitura superem a capacidade do switch entre o host e o hardware dedicado para armazenamento e exista uma restrição com relação ao uso de interfaces integradas para acesso ao *storage*;
- Caso a demanda ativa por memória RAM seja superior ao total físico instalado e o custo impeça a aquisição de um número maior de hosts, de

forma que seja necessário *swap*[6] nas máquinas virtuais, comprometendo, o desempenho de toda plataforma.

5 CONCLUSÃO

A tolerância à falha e o consequente aumento da disponibilidade, sobretudo no que tange a recuperação de desastres, é a base para defesa da virtualização. Embora o gerenciamento centralizado, com medição e balanceamento de recursos entre os hosts, permitindo a adição de processamento, memória ou disco ao cluster, sem necessidade de parada no processo, não sejam considerados resultados, são eles os verdadeiros responsáveis por tornar a arquitetura escalável, permitindo uma visão holística do sistema e a consequente redução do custo de aquisição para as futuras expansões.

REFERÊNCIAS

1 LOWE, S. Mastering VMware vSphere 5. Sybex; 1st Edition (October, 2011)
2 SHAH, Z. H. Windows Server 2012 Hyper-V: Deploying Hyper-V Enterprise Server Virtualization Platform. Packt Publishing (March, 2013)
3 PORTNOY, M. Virtualization Essentials. Sybex; 1st Edition (May, 2012)
4 POPEK, G. J. e GOLDBERG, R. P. Formal Requirements for Virtualizable Third Generation Architectures. 4th ACM Symposium on Operating Systems Principles, New York, October, 1973
5 VSPHERE 5 Documentation Center: Aspects of Virtualization. Disponível em: pubs.vmware.com/vsphere-50/index.jsp. Acesso em 13/05/2013.
6 SOSINSKY, B. Cloud Computing Bible. Wiley; 1st Edition (January, 2011)
7 MILLER, W. Virtualization: Top 10 Virtualization Best Practices. TechNet Magazine (September, 2010)
8 ROCKWELL Automation Publication. Virtualization for Process Automation System (January, 2013). Disponível em: http://www.ab.com/onecontact/process/whitepaper/get/PROCES-WP007A-EN-P.pdf. Acesso em: 13/05/2013.
9 WONDERWARE. ArchestrA System Platform in a Virtualized Environment Implementation Guide (2011/2012). Disponível em: http://www.vmware.com/files/pdf/techpaper/vmw-wonderware-ArchestrA-System-Platform.pdf. Acesso em: 13/05/2013.
10 SIEMENS. WinCC/Server Virtualization (April, 2011). Disponível em: http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&objId=49368181 Acesso em: 13/05/2013.
11 SNEDAKER, S. Business Continuity and Disaster Recovery Planning for IT Professionals. Syngress; 1st Edition (July, 2007)
12 IQBAL, M. SMADI, M. MOLLOY, C. RYMARCZYK, J. IT Virtualization Best Practices. Mc Press; 1st Edition (January, 2011)
13 GOLDWORM B. e SKAMAROK A. Blade Servers and Virtualization. Wiley; 1st Edition (February, 2007)

[6] Operação realizada pelo sistema operacional responsável pela escrita/leitura de dados da memória RAM em disco.