



As Vantagens do
Gerenciamento de Rede
Baseado em
Agentes Remotos

White-Paper



Gerenciamento de Missão Crítica

Introdução

Este *White-Paper* discute as vantagens do gerenciamento de rede baseado em Agentes Remotos sobre o gerenciamento de rede tradicional.

Definições

Os termos seguintes serão introduzidos e utilizados ao longo deste *White-Paper*.

NOC: Network Operations Center (Centro de Operações de Rede). Um centro de manutenção pertencente e operado por uma empresa que provê manutenção e gerenciamento de serviços para outras empresas.

Cliente: Um operador que possui e opera uma rede de comunicações e para quem o NOC provê manutenção e serviços de gerenciamento.

SNMP: Simple Network Management Protocol (Protocolo de Gerenciamento de Rede Simples). Um mecanismo, consistindo em agente, gerente e protocolo de comunicações, usado para gerenciar uma grande variedade de sistemas de dados e telecom.

Segment Manager: Um gerente de SNMP que administra um segmento específico de uma rede TCP/IP e reporta a um gerente de nível mais elevado.

Gerenciamento de Rede Tradicional

Agentes

Em gerenciamento de rede tradicional, os elementos a serem administrados tipicamente possuem módulos de software que executam diretamente no elemento. Estes módulos de software, chamados agentes, são fornecidos freqüentemente pelo fabricante do elemento. Protocolo de Gerenciamento de Rede Simples (SNMP) é o mecanismo

mais comum utilizado para gerenciamento de rede tradicional. Fornecer um agente SNMP incorporado nos sistemas tornou-se um dos valores a serem considerados nos negócios de comunicação de dados. A maioria dos fabricantes de roteadores, switches, concentradores, servidores e outros sistemas de dados vêm fornecendo estes agentes por muitos anos. O mercado de telecomunicações ficou para trás mas a convergência de voz e tecnologias de dados está trazendo os fabricantes de produtos de voz rapidamente para o mundo de dados. Enquanto os agentes SNMP estão ficando mais comuns, uma enorme base instalada com sistemas legados (*legacy systems*) não-SNMP apresentarão um desafio por muitos anos ao gerenciamento de rede tradicional.

SNMP, por definição, é um denominador comum para todos os elementos baseados em IP. Foi projetado para todos os elementos parecerem iguais pela perspectiva da monitoração e do gerenciamento. Isto, é claro, introduz muitos compromissos uma vez que um roteador e um servidor terão claramente coisas em comum (por exemplo, uma pilha TCP/IP) mas claramente muitas coisas serão diferentes. O SNMP endereça este problema permitindo aos fabricantes desenvolverem extensões específicas para determinados produtos. Como veremos depois, isto complica a tarefa de gerenciamento de rede e pode dificultar na busca da raiz de um problema.

Gerenciadores

Em gerenciamento de rede tradicional, os agentes acima descritos reportam, e são controlados por um gerente. O dado SNMP é o padrão mais onipresente disponível hoje, onde a maioria dos gerenciadores de rede são baseados em SNMP. HP OpenView é um dos gerenciadores mais populares mas existem muitos outros variando em preço de centenas a centenas de milhares de dólares. As funcionalidades variam assim como os preços. Fora da caixa, estes sistemas são capacitados a lidar com objetos padrão que precisam ser

gerenciados ou monitorados. Muitos possuem bons gráficos para mostrar estatísticas sobre parâmetros comuns. Poucos têm habilidade para lidar com tarefas de produtos específicos que resulta na diferença entre um roteador e um servidor ... ou ... o fato que um roteador Cisco é diferente de um roteador Adtran. O cliente pode se apresentar com muitos objetos que são produtos específicos, mas sem nenhum modo fácil de entender os significados destes parâmetros.

Os gerenciadores de rede são projetados tipicamente para o empreendimento mas não são bem adaptados para lidar com as aplicações de empresas onde a manutenção e os serviços de gerenciamento são providos por uma grande diversidade de outras empresas, cada uma com sistemas e exigências diferentes. Frequentemente estes sistemas, por possuírem designação única, não possuem qualquer conceito de "cliente". Esta é uma desvantagem clara para a empresa de serviço mas também pode ser problemático para empresas grandes e suas várias divisões que operam suas divisões como clientes internos. A falta de um banco de dados centrado no cliente torna difícil o armazenamento e coleta de dados deste cliente específico ou dados de elementos específicos do cliente, solicitados para a tomada de uma ação ou notificação deste cliente sobre os problemas.

Gerenciadores de rede tradicionais também podem falhar pela inabilidade do gerenciador em lidar com a interpretação de endereço de rede, que é requerida pela companhia de serviço para solucionar os endereços de rede sobrepostos provenientes de seus clientes. Gerenciadores que recebem *traps* chegando de várias redes podem não conseguir resolvê-los até o elemento de origem.

Infraestrutura de Comunicações

Em gerenciamento de rede tradicional, a rede de dados que leva o conteúdo do cliente é também a rodovia que provê a

conectividade para o sistema de gerenciamento. Isto é tipicamente chamado de gerenciamento *in-band* desde que a infraestrutura de gerenciamento seja a mesma infraestrutura do transporte de dados. A habilidade de um cliente para administrar os elementos da rede depende da saúde desta rede. Paradoxalmente, a determinação da saúde da rede também depende da saúde daquela mesma rede. A falha de elementos de rede sempre tem que ser antecipada. A Lei de Murphy estipula que a falha será no local que causará o maior dano. A falha de um elemento crítico de rede pode cegar o gerenciador para uma parte significativa da rede. Não é suficiente saber que ocorreu uma interrupção grave. São requeridos detalhes específicos relativos à natureza e local da falha de forma que ações corretivas possam ser tomadas.

O propósito primário da rede de dados é suportar comunicações que são necessárias para o cliente administrar seu negócio. Precauções devem ser tomadas com cautela para não congestionar este sistema, com tráfego que cause impacto ao real propósito da rede. Gerenciamento de rede tradicional, sendo *in-band* e confinado em *polling*, pode impactar com as aplicações que a rede foi projetada para suportar.

Acesso Remoto

O gerenciamento de rede tradicional é limitado tipicamente a monitorar os agentes incorporados como descrito previamente. Com esforço de desenvolvimento, ou com adição de *software plug-in*, pode ser realizada a automação para uma análise mais detalhada da falha, onde uma ação proativa de falha pode ser tomada. Os Engenheiros em serviço vão querer acessar os elementos manualmente para avaliar os problemas e tomar ações para suas devidas correções. Isto é tipicamente conhecido como Telnet, ou acessando elementos via servidores web. Se a rede ou determinado segmento cair

não será possível a utilização de métodos tradicionais de correção da falha.

Gerenciamento de Rede Baseado em Agentes Remotos

Esta seção do *White-Paper* irá focar no conceito de agente remoto para o gerenciamento de rede. Este conceito utiliza o Enterprise como o agente remoto, e uma plataforma de gerenciamento completa, como o gerente.



Agentes Remotos

A diferença fundamental entre o gerenciamento de rede tradicional e o gerenciamento de rede baseado em agentes remotos é a existência de um dispositivo dedicado que serve como um agente remoto localizado em um segmento de rede onde os elementos serão monitorados e gerenciados. Neste documento o Enterprise será descrito como modelo para todos e quaisquer agentes.

Em gerenciamento de rede tradicional um agente "representa" tipicamente um elemento, porém o Enterprise pode representar muitos elementos e uma grande diversidade de elementos diferentes. Sem se definir os elementos, este conceito apresenta uma clara vantagem para a normatização de eventos e interfaces. Nós já entendemos os gerenciadores e o Enterprise reduz a carga de trabalho do gerenciador provendo apenas um agente para ser administrado.

Como previamente discutido, SNMP tornou-se o denominador comum por administrar elementos de comunicação de dados e integra a mais recente produção de elementos de telecomunicações. O Enterprise, por incorporar capacidades

SNMP de gerenciamento, pode se comunicar com os agentes SNMP localizados em até 20 elementos na rede do cliente. No mundo SNMP isto é freqüentemente visto como um gerenciador de função intermediária ... ou em termos GMC (Gerenciamento de Missão Crítica) ... um Gerenciador de Segmento. O papel do Gerenciador de Segmento é:

- a) Fazer com que o sistema de gerenciamento de rede trabalhe sem-carga;
- b) distribuir inteligência para aumentar a robustez;
- c) reduzir o tráfego de WAN;
- d) prover proatividade no controle local de elementos de rede, independente do sistema de gerenciamento de rede ou da infraestrutura de comunicações.

Ao operar como um Gerenciador de Segmento, o Enterprise pode não apenas detectar *traps* SNMP de elementos e interrogar os agentes pelo estado do elemento; ele pode também correlacionar eventos de múltiplos agentes no segmento gerenciado. Esta capacidade pode reduzir muito o número de eventos que devem ser reportados no fluxo de dados e ainda simplificar na determinação da raiz da causa de um problema, que pode impactar vários elementos. Escrevendo Scripts no agente remoto permitirá o acesso a objetos únicos para vários elementos e à tradução da informação deste elemento específico em algo significativo e útil. Em gerenciamento de rede tradicional esta tarefa fica a cargo do gerenciador. Enquanto muitos são capazes de fazê-lo, poucos fazem *out-of-band* ... onde o desenvolvimento ou software adicional é requerido.

Gerenciadores de rede tradicionais devem entrar em comunicações constantes com os elementos administrados (*via polling*) através de toda a rede de dados ou ser transferido para receber *traps* ... que freqüentemente pode saturar a rede e muitas vezes prover informação insuficiente. Adicionalmente, os *traps* são mecanismos não confiáveis para reportar

a informação de falha crítica através de redes congestionadas. Distribuindo inteligência e executando funções localizadas de gerenciamento, o tráfego de rede pode ser reduzido drasticamente.

Enquanto o Enterprise é capaz de usar qualquer rede TCP/IP (LAN, WAN, VPN, Internet, etc.) para reportar eventos, não é dependente do conceito *in-band* como um gerenciamento de rede tradicional. O agente dedicado sempre tem uma *back-door* para se comunicar com o gerenciador no caso de sua *front-door* estar fechada. Isto é realizado por um modem interno e a mais segura rede do mundo ... a rede de telefonia pública. Isto será melhor discutido abaixo.

Se a LAN/WAN é utilizada para informar eventos ao Sistema, o Pedido de Informação SNMP v3 é utilizado. Isto confere uma integridade fim-a-fim no controle considerando o uso de *traps* no conceito de "*send-and-hope*".

Discutimos então os benefícios do Enterprise como um agente remoto dedicado, focado em SNMP e como melhorar o conceito tradicional de agente/gerenciador. Devemos notar que há dezenas de milhares de elementos que necessitam ser monitorados mas que não tem nenhuma capacidade SNMP. O Enterprise é capaz de monitorar estes elementos legados (*legacy elements*) através de interfaces seriais e uma grande variedade de sensores internos e externos conectados. Reportando-se a um sistema de gerenciamento de rede baseado em SNMP, o Enterprise opera como um *SNMP proxy-agent* provendo visibilidade a uma extensa gama de elementos que previamente estavam invisíveis ao gerenciador. Quando reportado ao Sistema estes elementos são tratados de modo equivalente a qualquer outro e a correlação de eventos entre elementos SNMP e elementos legados (*legacy elements*) é facilmente realizada.

O gerenciamento de rede tradicional freqüentemente ignora condições que causam impacto na operação da rede pois

tecnicamente não são equipamentos gerenciados. Um bom exemplo é a temperatura. Uma sala com temperatura elevada pode seguramente "derrubar" um roteador por uma falha em sua fonte de força. O Enterprise pode não só detectar e informar esta condição, como pode tomar uma ação corretiva ligando um ventilador/exaustor ou sistema de refrigeração automaticamente. Energia é outro exemplo. A maioria dos data centers possuem sistema UPS (*uninterruptible power system*) para assegurar a operação contínua de elementos críticos. Enquanto o UPS estiver mantendo o servidor em operação, o agente no servidor não tem nenhuma "idéia" de que as baterias estão a ponto de se esgotar devido a falha no acionamento do gerador. Estes são apenas alguns exemplos de coisas que podem ser executadas com um agente flexível como o Enterprise.

A ação corretiva não é limitada em apenas ligar um ventilador. O Enterprise pode ser configurado para tomar uma ação de correção de falhas em elementos baseados em SNMP e elementos legados (*legacy elements*) através de interfaces seriais. Isto é realizado por um processador de script robusto e aberto. O diálogo para realizar a ação corretiva é confinado no segmento de rede e é realizado automaticamente sem a intervenção do pessoal de manutenção. Problemas que não podem ser corrigidos podem ser reportados no fluxo de dados junto com a informação de *trouble shooting* que é descoberta no diálogo local com o sistema (*host*).

Gerenciadores

Como mencionado previamente, o Enterprise pode reportar a sistemas de gerenciamento de rede tradicionais. Em muitos casos, um cliente pode decidir adotar um sistema como o HP OpenView para seu empreendimento enquanto continua terceirizando funções de gerenciamento ou manutenção junto à uma empresa de serviço terceirizada. O Enterprise facilmente apóia ambos, reportando a múltiplos gerenciadores.

Para possibilitar uma maior funcionalidade, o Enterprise reporta ao Sistema, uma aplicação cliente/servidor rodando em ambiente MS Windows 2000 Server.



Ao contrário dos gerenciadores de rede mais tradicionais, esta Gestão é entregue com um banco de dados abrangente que suporta o conceito de clientes, as localidades pertencentes a cada cliente, e o gerenciamento de elementos destas localidades. O banco de dados é escalável e o número de clientes, localidades e sistemas só estão limitados pela capacidade e performance do servidor. O Sistema opera seu agente remoto (o Enterprise) de forma que os usuários saibam exatamente qual é o elemento que possui o problema. Este gerenciador olha dentro de cada evento para determinar o ponto de origem, eliminando assim qualquer problema que possa ser causado pelo tradução de endereços de rede (NAT).

O Sistema também oferece uma hierarquia independente que permite à empresa de serviço ou ao cliente afinar o sistema para atender exatamente suas práticas empresariais. Esta hierarquia pode ser vista junto a um cliente, uma localidade, ou na criação de estruturas únicas de banco de dados por elemento. Por exemplo, é possível agrupar os clientes em regiões geográficas e permitir aos gerenciadores regionais verem somente esses clientes. Pode-se agrupar elementos de Dados e Telecom em *nodes* únicos. *Nodes* podem ser criados para grupos de elementos, para que a informação da falha possa ser direcionada a engenheiros com habilidades específicas. Muitas combinações são

possíveis considerando que a hierarquia dos *nodes* são definidas pelo cliente.

Com a adição de módulos do fabricante, a correlação dentro- e entre-elementos é suportada, assim como: escalabilidade, emulação de terminal, geração de relatórios customizáveis (*ad-hoc report*), e remessa inteligente de alarmes. Estas funções são totalmente suportadas não requerendo *scripts* pelo cliente ou *plug-ins* de outros fornecedores.

GMC (Gerenciamento de Missão Crítica) não é o único provedor de dispositivos de agente remotos, porém, a combinação de Sistema e Enterprise é a única em que eles são totalmente integrados.

Unidades Enterprise são agentes muito inteligentes que podem ser distribuídos ao longo da rede. Toda programação, configuração e gerenciamento desta inteligência distribuída é realizada pelo gerenciador de Gestão. Atualizações podem ser programadas e realizadas automaticamente ... para um local ou milhares.

Infraestrutura de Comunicações

Na discussão de gerenciamento de rede tradicional, a relação entre a saúde de uma rede e a habilidade para monitorar/gerenciar foi destacada. Nenhuma tentativa foi feita para subestimar ou declarar que isto não é viável. O conceito de agente remoto é completamente compatível com este conceito.

Dito isto, acreditamos que nunca deveria-se proceder o gerenciamento com um único mecanismo. Isto conduz à síndrome da raposa no galinheiro. Se redes nunca falhassem, então por que os monitorá-las? Elas falham ... e nesta ocasião utiliza-se portanto a rede de telefonia pública. A chave é ter rotas alternativas para reportar e acessar os elementos gerenciados quando houver problemas na rede. Um agente remoto como o Enterprise provê todas as funcionalidades necessárias. Enquanto o *dial-up* pode parecer ultrapassado no

mundo de Cable Modems, DSLs e Internet, esta é uma linha permanente e sempre disponível. Ela também provê um mecanismo de acesso alternativo se a rede estiver saudável. Isto pode ser muito valioso nas aplicações de empresas de serviços onde a conectividade em tempo-real para todas as localidades do cliente não é prática ou quando os Engenheiros estão longe do NOC (Centro de Operações de Rede).

Acesso Remoto

Como em gerenciamento de rede tradicional, os Engenheiros precisarão ter acesso ao elemento com problemas de *troubleshoot*. Neste caso o agente remoto é acessado via TCP/IP, Telnet e web browsers podem ser usados como dito anteriormente, para um acesso direto ao elemento gerenciado. Engenheiros de serviço também podem usar linhas de comando nas interfaces para até oito dispositivos legados (*legacy systems*) acessando o servidor de Telnet no Enterprise e então selecionar a conexão a um destes oito sistemas legados ... através de uma emulação de terminal completa tirando proveito das funções nativas do sistema legado (*legacy systems*). Ainda, Engenheiros de serviço que não têm acesso a LAN/WAN podem utilizar facilidades seguras de *dial-in* para ter acesso aos elementos habilitados por IP e sistemas legados (*legacy systems*). Procedimentos de Auditoria são mantidos para permitir que sistemas gerenciadores conheçam quem e teve acesso aos seus elementos e quando.

Conclusões

O gerenciamento de rede tradicional operou bem e por muito tempo, mas não é o único conceito. Como os mundos de dados e voz continuam a convergir, o termo "rede" será redefinido e virá certamente composto da mais diversa linha de produtos. Esta convergência não é só de produtos e tecnologia mas

também de práticas empresariais. Tecnologia da Informação está se tornando o conjunto que vai abranger as aplicações de dados e voz. Profissionais de TI estão procurando por melhores caminhos para gerenciar uma matriz desordenada de sistemas, em uma lista sempre crescente de fornecedores.

O gerenciamento de rede baseado em agente remoto apresenta uma alternativa interessante. A solução de Gerenciamento de Sistemas Inteligentes CSM é bem moldada para o empreendimento como também para grandes empresas de serviços. Os agentes remotos distribuem inteligência, provêem caminhos alternativos de gerenciamento assegurando o acesso durante as "paradas", acomodando facilmente sistemas legados (*legacy systems*), como também os elementos mais atualizados baseados em IP. A solução é integrada com elementos independentes. Este conceito simplifica o gerenciamento e ajuda a equipe de TI a se dedicar à atividade principal ... provendo uma infraestrutura segura para suportar as metas de negócios do empreendimento.