Um documento setorial da Lippis Consulting

A Cisco prepara a ACI para disponibilização geral: o que esperar

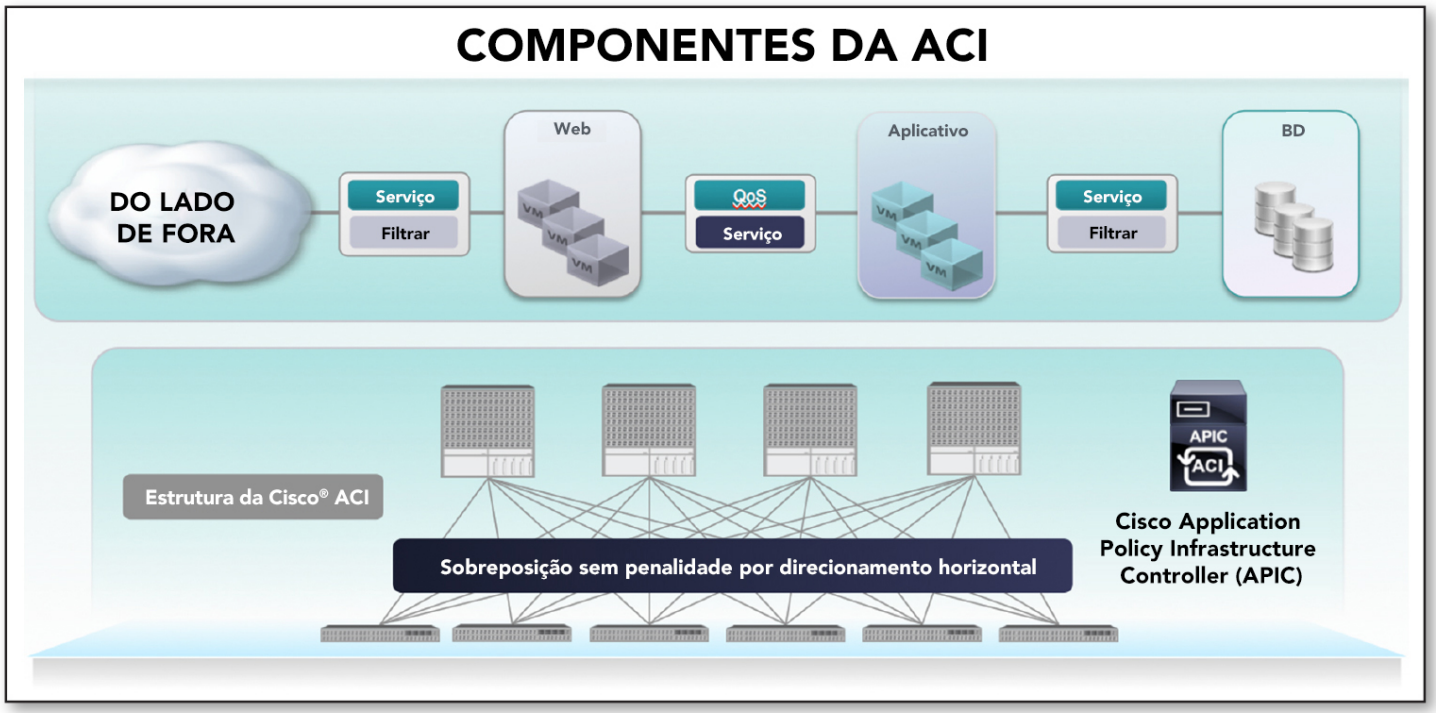
Por Nicholas John Lippis III
Presidente, Lippis Consulting

Agosto de 2014

Um dos maiores eventos de rede em agosto é a disponibilidade geral da ACI (Application Centric Infrastructure) da Cisco. Desde novembro de 2013 a Cisco disponibiliza os switches Nexus 9000 series no chamado "modo independente", ou seja, um switch Ethernet de data center ultrarrápido. Os pedidos do Nexus 9000 triplicaram de 180 no terceiro trimestre para 580 ao fim do quarto trimestre fiscal da Cisco. A Cisco prometeu como parte do lançamento do Nexus 9000 a possibilidade de implementação desses switches no "modo de estrutura da ACI". O modo de estrutura da ACI promete reduzir o custo operacional, aumentar a agilidade e vincular os aplicativos à infraestrutura de rede como nunca antes. A ACI é a manifestação do modo de estrutura e agora está sendo disponibilizada para o público em geral. Nesta nota de pesquisa do Lippis Report, analisamos a ACI do ponto de vista prático para os arquitetos de data center atuais.

Os três componentes básicos da ACI são: 1) um modelo de política que é um princípio de organização que estabelece como agrupar dispositivos em estruturas, como contêineres, e descrever como elas se conectam, 2) o APIC ou Application Policy Infrastructure Controller que fornece um único ponto de gerenciamento e repositório para todas as políticas descritas e 3) a estrutura da ACI, que é uma abstração de todos os dispositivos de rede físicos e virtuais que compõem a estrutura da ACI. Este é um lembrete sobre os três componentes da ACI.

camada de aplicativo middle-ware e uma camada de banco de dados de back-end; esse aplicativo também pode exigir conectividade com o mundo exterior. A política para descrever as necessidades de conectividade pode ser definida diretamente usando-se as Políticas baseadas em grupos na ACI, mas o modelo também pode ser muito genérico. A política pode ser utilizada para definir políticas orientadas por segurança, nas quais um grupo externo (local remoto e tráfego da Internet) se conecta ao grupo de DMZ, que se conecta ao grupo interno, por exemplo. Como alternativa, uma GBP pode modelar a forma como a maioria das redes é descrita atualmente em termos de VLANs e/ou sub-redes, as quais seriam mapeadas em vários grupos. Por fim, a Cisco deseja expor a diferentes partes interessadas esse conceito de Política baseada em grupos, para que não seja necessário ter um **Cisco Certified Internetwork Expert** (CCIE) ou um gênio da rede para criar a conectividade. Um administrador apenas expressaria que este "grupo de itens" se conecta a outro "grupo de itens". A Cisco denomina esses "grupos de itens" arbitrários usando a terminologia de Grupo de endpoint (EPG), e eles representam uma coleção de endpoints físicos e virtuais. Ou seja, um EPG pode significar serviços físicos, servidores instalados diretamente no hardware (bare-metal), máquinas virtuais em vários hipervisores diferentes etc. A questão é que a Cisco pode agrupar "itens" de forma razoavelmente flexível, independentemente de onde estejam na estrutura inteira da ACI.

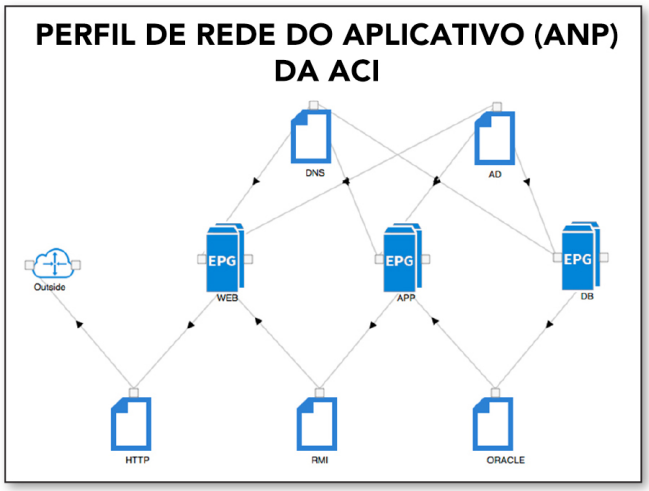


Modelo de política: o modelo de política da ACI cria uma nova forma de descrever a conectividade através do que a Cisco chama de conceito de "GBP" (Group-Based Policy, Política baseada em grupos). O modelo de política da Cisco apresenta uma maneira genérica de descrever como as coisas se conectam. Por exemplo, considere um aplicativo típico de três camadas implantado em um data center que pode consistir em uma camada de front-end da Web, uma

Outro conceito chave no modelo de política da ACI é a capacidade de definir o relacionamento entre EPGs. Esta relação é chamada de "contrato" e descreve o que pode fluir e quais métodos de conectividade são permitidos entre EPGs diferentes. Um contrato pode consistir em um protocolo específico (ou conjunto de protocolos) que seriam permitidos entre grupos, ou também pode ser utilizado para integrar um gráfico de serviço da camada 4-7 a fim de aplicar

serviços de rede, como um firewall, um balanceador de carga etc. para a conectividade entre grupos.

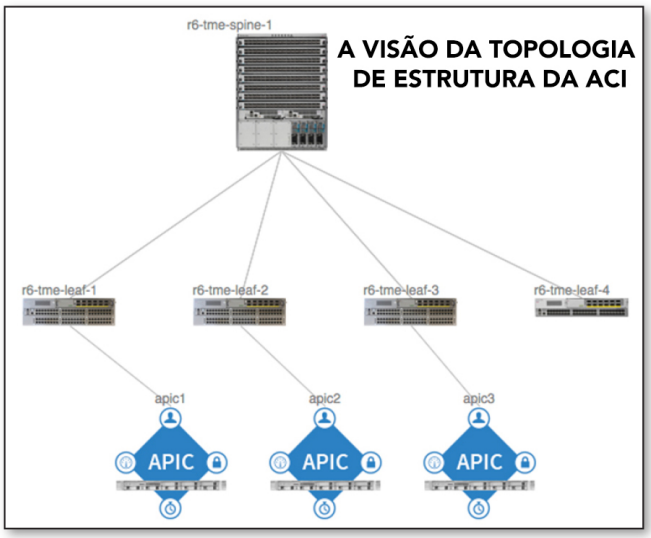
De uma perspectiva das Operações de segurança, o modelo de política da ACI implementa para a segurança essencialmente um modelo de lista branca, que é diferente da implementação atual das ACLs. No formato atual da rede, as Operações de rede consideram que qualquer coisa pode se comunicar, mas somente aqueles que não conseguem podem ser bloqueados com ACLs; isso cria um modelo de lista negra para segurança. Essencialmente, a estrutura inteira da ACI pode ser considerada como idêntica operacionalmente a um grande firewall baseado em contexto, que aplica políticas globalmente no data center inteiro.



A Cisco contém essas definições de EPGs, contratos e redes externas em algo chamado Perfil de rede de aplicativo (ANP). Estes ANPs são totalmente abstraídos/separados de qualquer infraestrutura física/virtual subjacente e, portanto, podem ser copiados para uma estrutura de ACI diferente e serem instanciados novamente. Isto facilita a definição da conectividade de aplicativo globalmente em vários pods ou sites sem o administrador de aplicativo que precisa entender os detalhes sobre como determinada estrutura é arquitetada.

APIC: as políticas da ACI são descritas no APIC ou Controlador de infraestrutura de Política do Aplicativo. O APIC é um conjunto de servidores em rack UCS C-series x86 1 RU e fornece um único ponto de gerenciamento e repositório para todas as políticas descritas, bem como qualquer outra política para provisionar, administrar, monitorar e solucionar problemas de estrutura; de acordo com a Cisco, tudo é uma política! Observe que a APIC não é utilizada para encaminhamentos ou pesquisas. Na verdade, depois que as políticas são descritas no APIC, é possível removê-las por completo e tudo continuará a funcionar, mas esse ponto serve para destacar que o APIC não é necessário durante as operações de encaminhamento.

A Cisco não recomenda remover por inteiro o conjunto inteiro do APIC, pois os administradores não poderiam mudar as políticas até pelo menos um APIC ser reconectado. O conjunto do APIC é totalmente redundante e equilibra as cargas simultaneamente, com três dispositivos de APIC prontos e recomendados formando um conjunto. O sistema de ACI inteiro exibe tudo como um objeto e



apresenta esses objetos no que a Cisco chama de "árvore de informações de gerenciamento distribuída" ou dMIT para que os objetos individuais herdem propriedades (privilégios de segurança, atributos etc.) dos objetos pai. Por sua vez, esses objetos são expostos de forma ascendente para o resto do mundo através do APIC por meio de vários métodos, incluindo REST (XML/JSON) APIs, Interface gráfica do usuário (GUI) ou um envelope de linha de comando semelhante ao ambiente Linux BASH. Como alternativa, a Cisco também oferece Kits de desenvolvimento de software (SDKs) adicionais para aqueles que precisam desenvolver aplicativos a fim de interagir diretamente com o modelo de política de ACI. Na Disponibilidade geral (GA), a Cisco envia e comporta um SDK Python, mas informa que uma variante Ruby e até mesmo C# surgirão em breve.

Estrutura da ACI: a estrutura da ACI é essencialmente uma coleção de dispositivos físicos e virtuais que compõem a estrutura da rede, processando todas as funções do plano de dados, como pesquisas, encaminhamento, aplicação de política etc. Esses dispositivos podem fornecer serviços de encaminhamento, como switches e roteadores, e/ou serviços de rede das camadas 4 a 7, como firewalls, balanceadores de carga etc.

No centro da estrutura da ACI estão os principais switches de data center Nexus 9000 series da Cisco, configurados em uma topologia Spine-Leaf, fornecendo conectividade de direcionamento horizontal, desempenho, resiliência e flexibilidade. Durante a GA, a Cisco oferece duas variantes de switches Leaf:

- Nexus 9396PX – 48 portas de 1/10 G SFP+ com 12 portas adicionais de uplinks QSFP de 40 G
- Nexus 93128TX – 96 portas de 1/10 G Base-T com 8 portas adicionais de uplinks QSFP de 40 G

A Cisco também oferece estas duas variantes dos switches Spine:

- Nexus 9336PQ – 36 portas de links QSFP de 40 G para os switches Leaf
- Nexus 9508 – até 288 portas de links QSFP de 40 G para os switches Leaf

A Cisco se dedicou a apoiar mais formatos de switches Spine e Leaf, incluindo switches 1 RU Leaf, além de switches Spine de pequeno porte (Nexus 9504 de 4 slots) e maior porte (Nexus 9516 de 16 slots) no futuro.

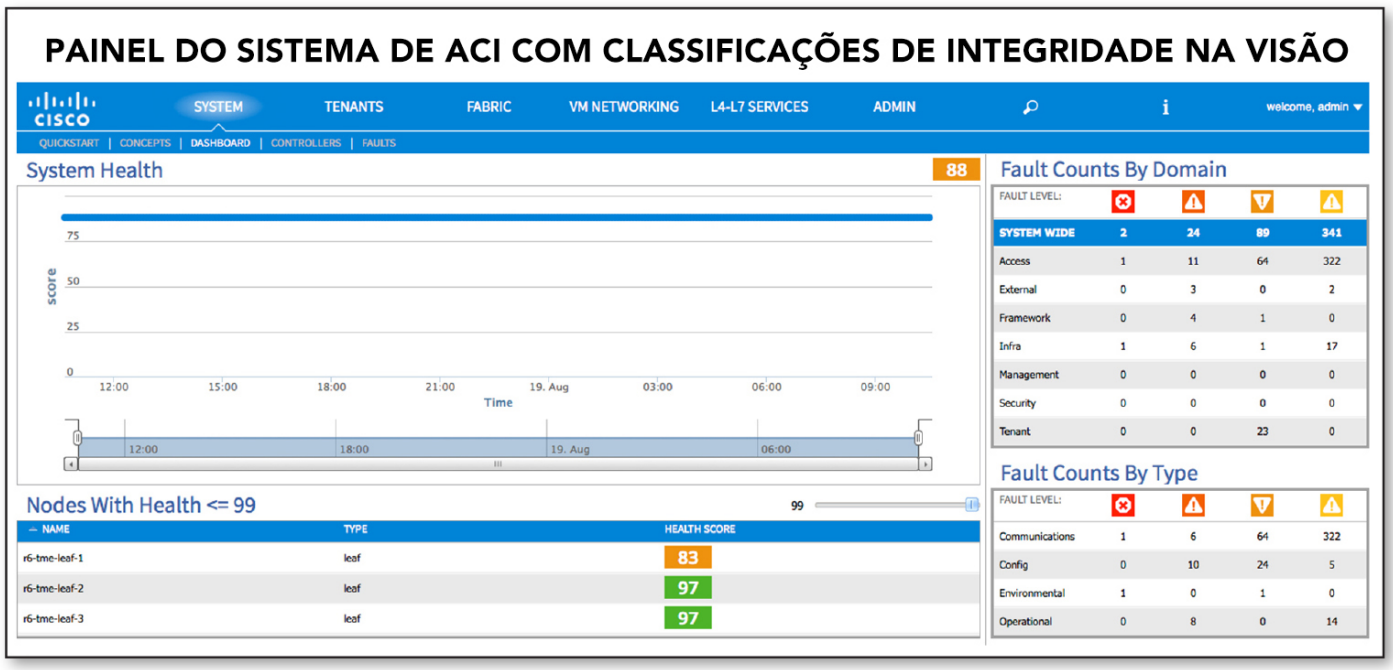
Do ponto de vista do design de rede, todos os dispositivos se conectam a switches leaf. Os únicos dispositivos que se conectam aos switches Spine são outros switches leaf. Sob a superfície, a Cisco utiliza o roteamento IPv4 na estrutura como o protocolo "subjacente" e aproveita um encapsulamento de "sobreposição" de hardware da Virtual eXtensible LAN (VXLAN) para fornecer bridging de L2/L3 e roteamento na estrutura inteira da ACI.

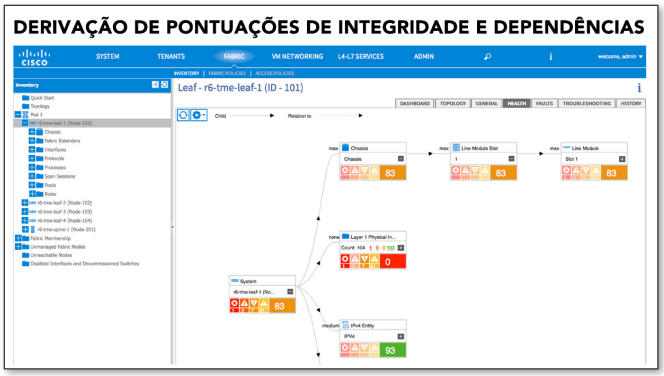
Uma observação importante é que a estrutura da ACI também é capaz de controlar qualquer switch virtual (vSwitches) em hipervisores diferentes com o qual se integra, seja a VMware através do vCenter, Microsoft através do SCVMM (System Center Virtual Machine Manager) com Windows Server 2012 R2 ou OVS através de OpenStack (comportando variantes do Ubuntu e RedHat). Além disso, a estrutura da ACI pode controlar os servidores de rede através de plugins que a Cisco chama de "Pacotes de dispositivos" e permite que o APIC facilite a orquestração, automatização e encadeamento de serviços L4-7; as políticas são ampliadas até esses serviços de rede para que os administradores não precisem gerenciar esses dispositivos separadamente. Portanto, a estrutura da ACI se estende além das plataformas Nexus 9000 da Cisco, mas também abrange os demais serviços aos quais se integra.

Operacionalização da ACI: classificações de integridade

A característica fundamental da abordagem da Cisco em relação à ACI é que com esta versão geral ela oferece um conjunto de ferramentas que ajudará os administradores de data center a operacionalizarem uma implantação da Cisco ACI. Uma dessas ferramentas é chamada de Classificações de integridade. Além de fornecer uma maneira simples de provisionar a estrutura da ACI, a Cisco desejava agregar valor às operações do segundo dia; isto é, gerenciamento e operações cotidianas. Depois que a ACI é configurada e ajustada, os administradores devem monitorar e entender como a estrutura está se comportando e respondendo às expectativas. Para isso existem as "classificações de integridade", que fornecem a administradores diferentes uma forma discreta de calcular os pontos problemáticos de integridade. Como mencionado acima, visto que todos os dispositivos na estrutura da ACI são essencialmente objetos, a ACI pode avaliar e atribuir pontuações de integridade à maioria dos objetos, pois estes estão na árvore de objetos. As classificações de integridade também podem ser "implantadas" na árvore, para que uma classificação agregada por locatário ou uma classificação de estrutura inteira possa ser relatada e coletada. É um modelo fractal que fornece uma alta classificação e permite que o administrador obtenha detalhes dos dispositivos e componentes ou funções em dispositivos, como uma porta ou até mesmo ao nível do protocolo.

Por exemplo, a estrutura inteira da ACI pode ter uma classificação de integridade de 99%, o que é ótimo, mas depois muda à medida que algo na estrutura se degrada. Podem ser erros em portas, uma porta em pane ou uma VM em um host ESX com consumo de ciclo da CPU muito alto. À medida que as falhas ocorrem, elas começam a acionar eventos, o que resulta em uma degradação das classificações de integridade dos objetos discretos e uma pista visual para os administradores. Estas classificações são acumuladas na árvore e, eventualmente, a classificação de integridade da estrutura inteira começará a diminuir enquanto as classificações de objeto subjacente são reduzidas. As pessoas que apoiam e operacionalizam redes em data centers endendem que é muito difícil rastrear a origem de um problema sem ter um bom contexto. As classificações de integridade fornecem contexto e um sistema de classificação, com a melhor classificação sendo 100.





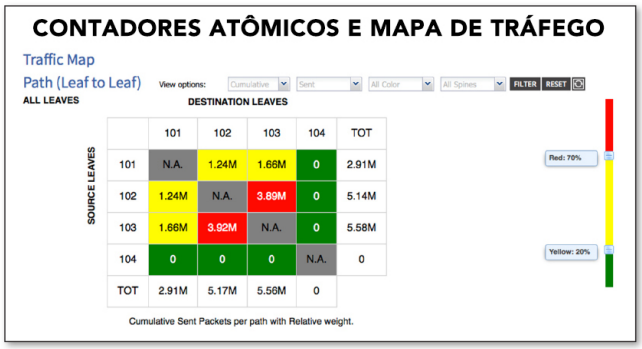
Alguns funcionários de NetOps podem acreditar que é possível criar um sistema semelhante para a classificação de integridade ao executar scripts a fim de automatizar a coleta e o processamento de estatísticas de rede regulares, mas pode ser difícil. Uma pessoa pode ocultar muita complexidade da rede atual através de scripts, mas imagine o desenvolvimento de scripts em cada aspecto operacional individual da rede. Não só é difícil exigir conjuntos de habilidade DevOps sérios, eles também não são escaláveis em um ambiente grande. O que a Cisco fez com a ACI antes da criação de hardware e software no sistema foi desenvolver o modelo de dados orientados por software para ACI a fim de comportar essas funções. Este modelo comporta não apenas o provisionamento e a exclusão quando os administradores criam e removem objetos, mas também fornece informações constantes de atributos de objetos individuais permitindo que os administradores monitorem o status do objeto. É mais escalável e deve agregar muito valor, especialmente na economia de OpEx, além de acelerar o tempo para resolução quando os problemas ocorrem.

Visibilidade e solução de problemas: contadores atômicos

Outro recurso operacional importante é o que a Cisco chama de "contadores atômicos"; uma ferramenta de solução de problema e análises. Os contadores atômicos são expostos de algumas formas, mas essencialmente a Cisco incluiu contadores atômicos como uma função específica no hardware para evitar uma penalidade de desempenho quando habilitado. A Cisco também confirmou que os contadores atômicos serão estendidos para o switch de software da Cisco, o Application Virtual Switch (AVS), e possivelmente existem em outros switches de software aberto. O que os contadores atômicos fazem? Sua função é muito simples, mas crucial. Os contadores atômicos contam cada pacote que entra e sai da estrutura e também fornecem contextualização da contagem de pacotes.

Tradicionalmente, é difícil ganhar visibilidade sobre o movimento do fluxo de tráfego nas redes. A estrutura da ACI procura alterar isso com os contadores atômicos que acompanham ou rastreiam fluxos à medida que entram e saem da estrutura ao redor e dentro dos grupos de políticas acima. Os pacotes que entram na estrutura da ACI são marcados no primeiro ponto de entrada da estrutura, e os marcadores são removidos na saída. Esses pacotes marcados são a fonte do rastreamento e da contagem de fluxo dos contadores atômicos. Com os contadores atômicos, os administradores descobrirão rapidamente se a estrutura descartou pacotes para determinado par de leaf de entrada/saída (o que a Cisco chama de "caminho"), ou até mesmo entre um determinado par de porta para uplink de entrada/saída (o que a Cisco chama de "trilha"). Essas informações fornecem uma maneira de os administradores acompanharem as informações de pacote/fluxo de ponta a ponta na estrutura e limitarem os fluxos entre fontes e destinos.

A Cisco criou um gráfico para exibir a coleta de dados dos contadores atômicos no formato de mapa de calor ou tráfego a fim de mostrar o percentual de utilização geral dos fluxos entre caminhos e trilhas diferentes. Os diferentes usos têm códigos de cores para fornecer áreas com níveis de utilização altos/médios/baixos. Estas informações são úteis para entender se há redução de pacotes na estrutura e como ferramenta de planejamento a fim de entender onde colocar a carga de trabalho adicional na estrutura.



Um dos principais desafios de diagnóstico dos problemas de rede ocorre quando a NetOps precisa correlacionar informações de vário dispositivos e sistemas de gerenciamento diferentes. Normalmente, os funcionários de NetOps precisam interagir com dispositivos diferentes executando uma série de comandos de CLI, como "show ip arp", "show mac-address"..., e, em seguida, tentam rastrear todas essas informações, em geral com uma folha de papel para entender o caminho da rede. A capacidade de detalhamento dos contadores atômicos permite que a equipe de operações ignore esse processo tedioso e cansativo indo direto até a origem do problema. Os contadores atômicos podem ser utilizados nesses cenários para auxiliar na solução de problemas de sistema de ponta a ponta, permitindo que os administradores filtrem locatários específicos, EPGs, endpoints etc. nos quais estejam interessados e contêm somente os pacotes que correspondem aos critérios especificados.

Vinculação de aplicativos aos serviços de rede

O maior interesse dos administradores de infraestrutura é saber como vincular os ANPs aos serviços de rede nos quais os de L4-7 podem ser instanciados como um dispositivo físico, os tamanhos virtualizados ou uma combinação de ambos. A ACI fornece várias maneiras de solucionar esse problema de design enquanto minimiza o número de pontos de gerenciamento a apenas um. Para vincular um serviço de rede L4-7 a um ANP, o administrador não precisa interagir com interfaces de dispositivo ou sistemas de gerenciamento diferentes. Como os serviços de L4-7 são modelados como parte da estrutura de ACI, a Cisco basicamente arquitetou esses serviços no mesmo modelo de política de grupo

mencionado anteriormente. Um benefício adicional do modelo de estrutura da ACI que vincula os serviços de L4-7 aos ANPs é que os serviços de L4-7 podem ser independentes da localidade; ou seja, esses serviços podem ser vinculados em qualquer parte da estrutura de forma que quando o administrador vincular a função do serviço ao ANP, a estrutura descobre automaticamente onde se encontram e provisiona qualquer encapsulamento correspondente para esses nós de serviços a fim de automatizar o encaminhamento do caminho de dados.

A Cisco modela essas funções de serviço da L4-7 como um Gráfico de serviço e pode conter uma ou mais funções de serviço (Firewall, Balanceador de carga etc.). Estes gráficos de serviço podem ser agrupados na definição da ANP para refletir o comportamento desejado do ANP.

CRIAÇÃO DE UM GRÁFICO DE SERVIÇO DE L4-7

Por exemplo, ao associar Gráficos de serviço da L4-7 ao ANP, o administrador ou auditor de segurança pode entender que, em um nível mais alto, todas as correspondências de tráfego no HTTP/S destinado ao Web EPG na estrutura da ACI primeiro devem passar através de um Gráfico de serviço do firewall específico. Ou antes de um fluxo entrar no EPG do banco de dados de back-end, deve passar através de um Gráfico de serviço do balanceador de carga. A abordagem da Cisco ACI com relação ao vinculamento de ANP aos serviços de rede reduz um dos maiores empecilhos na cadeia de disponibilização do serviço de TI, que demora minutos para acelerar uma VM, mas por outro lado demora semanas ou meses para configurar a rede e os serviços de rede da L4-7. Atualmente, a Cisco ACI fornece integração com os firewalls Cisco ASA e ASAv, além dos Balanceadores de carga Citrix e F5. Os pacotes de dispositivo de cada um desses nós de serviço estão disponíveis nos sites dos respectivos fornecedores.

A Cisco se dedicou a trabalhar com mais de uma dezena de fornecedores para serviços de L4-7 para disponibilizar pacotes de dispositivo adicionais. Para obter a lista mais atualizada de parceiros de ecossistema da ACI, consulte a página da ACI da Cisco em http://www.cisco.com/go/aci

Cadeia de serviços e replicação

Há duas abordagens básicas para integrar serviços da L4-7: aproveitar os serviços de rede física e dividi-los logicamente em vários contextos para cada locatário, ou dedicar serviços virtuais individuais por locatário.

A ACI é capaz de comportar ambas as abordagens, pois a maioria das empresas de TI e dos provedores de nuvem necessitam de ambos. Por exemplo, na maioria das corporações, antes de entrar na definição de aplicativo corporativo, o tráfego deve passar por um firewall de perímetro. Esta função de firewall é bem controlada e altamente segura, quase como uma folga de ar em naves espaciais ou submarinos. No entanto, a qualificação recente não requer uma real folga de ar física, mas a maioria dos SecOps procura um dispositivo físico que atua como um ponto de controle de política. Neste cenário, a ACI é capaz de integrar as plataformas de firewall da Cisco e de outros fornecedores, da mesma forma como deveria ser capaz de vincular à estrutura da ACI. As empresas com controles de segurança mais rigorosos preferem esse modelo de arquitetura, pois não confiam tanto em firewalls virtualizados para proteção contra ameaças na DMZ. As empresas ficam mais confortáveis aproveitando o Cisco ASA, o firewall Check Point, o Juniper SRX ou os firewalls Palo Alto Networks atuais. O APIC permite que essas empresas de TI aproveitem o investimento atual em firewall físico ao conectá-los diretamente à estrutura da ACI, incorporando a funcionalidade e as políticas de provisionamento através do APIC.

Há cada vez mais interesse em bloquear ou segmentar as comunicações entre camadas de aplicativos diferentes; aqui, o modelo de política da ACI contribui a partir de uma perspectiva de escala e desempenho. Como as políticas são definidas através do ANP, estas são renderizadas através de uma infraestrutura e aplicadas no primeiro ponto de entrada na estrutura da ACI, o que fornece funcionalidade de firewall distribuída em todos os ANPs.

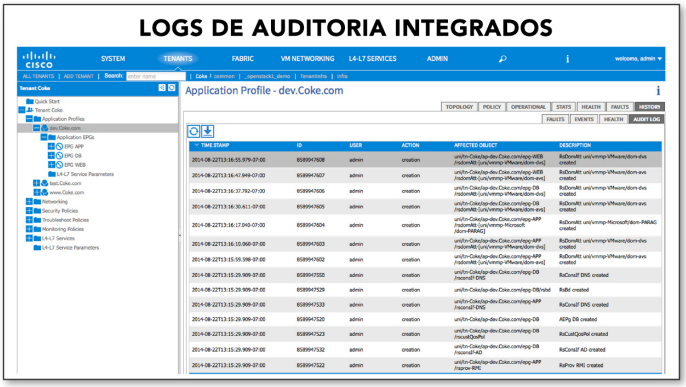
Os serviços virtuais individuais dedicados por locatário têm respaldo na ACI de formato semelhante aos dispositivos físicos. Os provedores de nuvem querem configurar e separar uma instância de um firewall virtual, um balanceador de carga etc. para cada locatário hospedado, para que seja controlado e gerenciado individualmente por cada locatário. Muitas empresas de TI aplicam o conceito de locatário a unidades de negócios individuais, por exemplo. Entretanto, com os serviços de rede virtual, há mais uma etapa necessária para implantar o firewall virtual ou o equilibrador de carga, que é fornecer o controle de versão apropriado e instalar as licenças corretas. Normalmente é chamado de gerenciamento do ciclo de vida dos serviços virtuais. A Cisco se une à Embrane para incorporar essa função à oferta da ACI.

Um grande avanço para os auditores dos sistemas de TI

Um grande benefício para a definição explícita de EPGs e "contratos" é que fornece aos administradores e auditores da TI a capacidade de fazer a auditoria de forma fácil da política instanciada em comparação à intenção original do proprietário do aplicativo. Não é segredo que a documentação sobre a política dos sistemas é escassa na maioria da empresas de TI e, quando existe, a manutenção da precisão e a atualização desses documentos gera uma grande sobrecarga em cima do administrador da TI. Além disso, os aplicativos originais ou o proprietário da plataforma podem ter mudado para funções diferentes ou saíram da empresa, deixando uma lacuna de conhecimento relevante. Aqueles que precisam derivar novamente a intenção do proprietário do aplicativo ou da plataforma envolvendo a recuperação e a revisão de

switch/roteador/firewall/balanceador de carga percebem que é um processo caro, desafiador e demorado.

Esta é uma grande área, na qual a ACI é importante. Como as políticas da ACI são expressas de forma simplificada, os auditores da TI podem entender rapidamente a intenção do proprietário do aplicativo analisando o ANP. O auditor não precisa rastrear/correlacionar os arquivos de configuração de rede e serviços detalhados para entender as políticas de aplicativo abrangentes. Além disso, a Cisco implementou um log de auditoria altamente detalhado para objetos modificados, indicando o carimbo de data e hora, o usuário, o objeto e a descrição do que foi modificado a fim de oferecer uma capacidade completa de rastreamento.



Túneis e interoperabilidade multi-hipervisor

Basicamente, a ACI fornece conectividade, mas a forma de conectar os dispositivos muda à medida que os aplicativos abrangem ambientes físicos e virtuais. Embora ocorra um aumento constante da migração de cargas de trabalho físicas para virtuais, ainda há o requisito inevitável de comunicação das cargas virtuais com cargas de trabalho hospedadas diretamente no hardware. No ano passado, ocorreu um aumento considerável do interesse em investigar as cargas de trabalho com base em contêiner para aprimorar o desempenho e reduzir a sobrecarga de processamento. A rede sempre foi um ponto de normalização subjacente para recursos da TI e modelos de computação, pois todas as cargas de trabalho aproveitam a rede a fim de oferecer conectividade. A ACI tenta se transformar na nova base de normalização dessas cargas de trabalho diferentes, tanto para conectividade como política.

O espaço que requer mais normalização atualmente é a rede virtualizada, com diferentes ofertas de hipervisor fornecendo métodos diferentes para gerenciar redes virtuais com suporte a vários encapsulamentos do plano de dados (VLAN, VXLAN, NVGRE etc.). Há cada vez mais ambientes que procuram implantar ambientes multi-hipervisor e, com essa tendência, as empresas precisam buscar uma forma abrangente de gerenciar esses ambientes diferentes, bem como os respectivos encapsulamentos subjacentes.

A Cisco ACI fornece integração direta com a versão do vCenter e OpenStack Icehouse da VMware, executando Ubuntu KVM com a versão GA do software. A Cisco se dedicará ao apoio do SCVMM da Microsoft, do Microsoft AzurePack e do Red Hat KVM com OpenStack futuramente. Ao integrar multi-hipervisores à ACI, o APIC se transforma no ponto central de gerenciamento para políticas de rede físicas e virtuais. Além disso, a estrutura da ACI se transforma em um ponto de normalização de encapsulamento distribuído para vários tipos de encapsulamento (VLAN, VXLAN, NVGRE), fornecendo aos administradores a capacidade de encerrar, interpretar e remapear encapsulamentos diferentes entre si. Esses encapsulamentos também são orquestrados pelo APIC, portanto, o administrador de rede ou da VM não precisam coordenar as vinculações de marcador. Quando os pacotes entram na estrutura da ACI, essas marcas de encapsulamento exclusivas são removidas e inseridas novamente ao retornarem ou são convertidas para o esquema de encapsulamento do hipervisor de destino fornecendo conectividade multi-hipervisor.

A integração com esses Virtual Machine Managers (VMMs) permite que o administrador trate as cargas de trabalho físicas e virtuais da mesma forma ao aproveitar o modelo de política da ACI. Quando os administradores criam camadas de aplicativo, zonas de segurança ou qualquer item que se vincula a um EPG, esses grupos são enviados para os dispositivos físicos e virtuais subjacentes. No vCenter da VMWare, o APIC envia os EPGs como grupos de porta da VMWare. No SCVMM da Microsoft, o APIC envia EPGs como redes de VM e com OpenStack, o APIC envia os EPGs como redes simples.

Por exemplo, considere um hipervisor VMWare ESX que usa VXLAN; ele marca todos os pacotes através da VXLAN, mas deve ser comunicar com dois outros hipervisores ESX que utilizam encapsulamento da VLAN. A estrutura da ACI executa a conversão da VLAN, ou bridging e roteamento de VXLAN para VLAN, portanto, esses pacotes podem transcender as sub-redes. Ou seja, a ACI fornece funções completas de terminação, normalização e roteamento de VLAN e VXLAN no desempenho do hardware.

Abordagem de host ou rede para normalização de esquemas de túnel virtual

A ACI fornece uma abordagem de arquitetura diferente das redes somente com hipervisor. Na abordagem somente com hipervisor, as funções da rede são implementadas no hipervisor. Isto começa com a marcação e os mecanismos de aplicação de política no hipervisor, fornecendo conhecimento de ponta a ponta da rede virtual no nível do hipervisor. Neste modelo, cada host com túnel, isto é, os endpoints do túnel, devem estar na mesma pilha vertical, como VMWare, Microsoft ou o esquema de túnel virtual utilizado. Os esquemas de túnel virtual devem ser coordenados em cada host de hipervisor no domínio de conectividade. Isto significa essencialmente que as cargas de trabalho devem ser virtualizadas e emparelhadas com os mesmos hipervisores. Há pouca ou nenhuma interoperabilidade entre os sistemas de gerenciamento de hipervisor que permitem uma mistura e correspondência de encapsulamentos e políticas. Além disso, para se conectar a servidores instalados diretamente no hardware (não virtualizados), por exemplo, um switch físico na rede deve entender os mesmos esquemas de túnel virtual e requer integração detalhada com os sistemas de gerenciamento do hipervisor para possibilitar a coordenação/orquestração dos encapsulamentos e das políticas.

Um desafio adicional para implantações de produção é que os administradores de data center agora precisam testar e validar não apenas a estrutura física subjacente (o "subjacente"), mas também aproveitar outro conjunto de ferramentas para validar as redes virtuais (o "sobreposto"), duplicando a quantidade de tempo para qualificação a fim de colocar a infraestrutura de rede geral em uma implantação pronta para produção.

Em vez de promover a coordenação no nível do host, a ACI utiliza a rede para coordenar os esquemas de túnel virtual, o que fornece a normalização em cada nó de leaf. Como os nós de rede compõem o ponto de normalização na ACI, ela fornece a conectividade e as políticas completas para todos os dispositivos, sejam estes físicos, virtuais ou contêineres que se conectam à rede. Para operacionalizar a estrutura da ACI em uma implantação pronta para produção, o administrador de data center deve testar e validar somente a estrutura da ACI, pois combina o subjacente e o sobreposto no mesmo plano, o que economiza tempo de qualificação da solução de ponta a ponta.

Portanto, a escolha que a maioria dos arquitetos deve fazer é: 1) aproveitar a rede como um ponto de normalização para conectividade e política, bem como qualificar a rede física e virtual em conjunto, 2) virtualizar tudo e solicitar que todos os hosts executem exatamente os mesmos hipervisores no data center inteiro, bem como duplicar a quantidade de tempo para verificação, e/ou 3) executar várias redes de sobreposição sem interoperabilidade entre hipervisores e/ou servidor instalados diretamente no hardware, adicionando os ciclos de qualificação apropriados.

No modelo da ACI, os aplicativos podem conter Microsoft Hyper-V, VMWare ESX e Ubuntu/RedHat KVM como servidores instalados diretamente no hardware. Neste modelo, parte de um aplicativo da Web pode ser hospedada no ESX com VXLAN, o aplicativo pode ser hospedado no Hyper-V com os bancos de dados no KVM e instalados diretamente no hardware com conectividade e de políticas fornecidas para todos através de um único ponto de gerenciamento. A ACI é uma ótima escolha para aqueles que procuram uma opção flexível de infraestrutura de data center.

Conclusão

A Cisco analisou os problemas que os executivos da TI observaram ao gerenciarem a infraestrutura de data center moderna e desenvolveu uma nova abordagem que busca reduzir o custo operacional, acelerar a disponibilização da TI, abranger recursos de TI físicos e virtuais, além de fornecer apoio multi-hipervisor e interoperabilidade. A Cisco manteve o único princípio verdadeiro da rede: comportar todos os aplicativos e cargas de trabalho, além de ser uma infraestrutura geral para várias finalidades que pode ser personalizada para conectividade através da política, automação e programabilidade. Esta nova abordagem é a Application Centric Infrastructure e, com ela, a Cisco desenvolveu algumas das ideias mais aprofundadas do setor de redes nos últimos 25 anos. Embora demore algum tempo para o setor adotar por completo a ACI, o que a maioria descobrirá é que a Cisco fornece um novo modelo de redes que apresenta inovações tecnológicas importantes, as quais são mais fáceis de controlar e gerenciar do que as redes orientadas por dispositivos atuais. O resultado deve ser a liberação de OpEx a curto prazo, além da arquitetura de infraestrutura de data center avançada que serão a base para impulsionar a economia mundial por mais 25 anos no longo prazo.

Sobre Nick Lippis

Nicholas J. Lippis III é uma autoridade mundialmente reconhecida em redes avançadas de IP, comunicação e seus benefícios aos objetivos empresarias. Ele é o editor do *Lippis Report,* um recurso para os responsáveis por decisões empresariais de redes e de TI assinado por mais de 35.000 executivos líderes empresariais de TI. Seus podcasts do Lippis Report foram baixados mais de 200 mil vezes; o iTunes informa que os ouvintes também baixam o *Money Matters*, do Wall Street Journal, o *Climbing the Ladder,* do Business Week, o *IdeaCast,* do The Harvard Business Review, e *The Economist*. Ele é também o cofundador e diretor da conferência Open Networking User Group, que patrocina um encontro bianual de mais de 200 líderes empresariais de TI de grandes empresas. O Sr. está trabalhando atualmente com clientes para projetar suas arquiteturas de rede de computação em nuvem pública e privada de data center virtualizado com tecnologias de rede aberta com o objetivo de agregar o máximo de valor empresarial e resultados.

Ele aconselhou várias empresas da Global 2000 sobre arquitetura de rede, design, implementação, seleção de fornecedores e orçamentos, com clientes que incluem Barclays Bank, Eastman Kodak Company, Federal Deposit Insurance Corporation (FDIC), Hughes Aerospace, Liberty Mutual, Schering-Plough, Camp Dresser McKee, o estado do Alasca, Microsoft, Kaiser Permanente, Sprint, Worldcom, Cisco Systems, Hewlett Packet, IBM, Avaya e muitos outros. Ele trabalha exclusivamente com CIOs e seus subordinados diretos. O Sr. possui um ponto de vista exclusivo sobre as forças de mercado e as tendências que ocorrem no setor de computação em nuvem, derivado de sua experiência tanto com o lado do fornecedor quanto do cliente.

O Sr. recebeu o prestigiado prêmio dos alunos de engenharia da Boston University College pelos avanços na profissão. Ele foi nomeado uma das 40 pessoas mais poderosas e influentes no setor de redes pela *Network World. O TechTarget,* uma publicação online do setor, o nomeou guru do design de rede, enquanto a *Network Computing Magazine* o chamou de guru-estrela da TI .

O Sr. fundou a Strategic Networks Consulting, Inc., uma empresa respeitada e influente de consultoria do setor de rede de computadores, que foi comprada pela Softbank/Ziff-Davis em 1996. Frequentemente, ele é o palestrante principal em eventos do setor e é amplamente citado pela imprensa empresarial e setorial. Ele trabalha na reitoria do quadro de conselheiros da Faculdade de Engenharia da Boston University, assim como em quadros de conselheiros de muitas empresas start-ups. Ele proferiu o discurso de formatura aos graduados de engenharia do Boston University College em 2007. O Sr. recebeu os títulos de Bacharel em Ciências em engenharia elétrica e de Mestre em Ciências em engenharia de sistemas pela Boston University. O trabalho de sua tese de mestrado incluía cursos técnicos e conselheiros selecionados da Massachusetts Institute of Technology em comunicações e computação óptica.