Segurança Aplicada a Redes Corporativas

Prof. Me. Wallace Rodrigues de Santana

www.neutronica.com.br

Atribuição-NãoComercial-CompartilhaIgual 3.0 Brasil (CC BY-NC-SA 3.0)

Você tem a liberdade de:

Compartilhar — copiar, distribuir e transmitir a obra.

Remixar — criar obras derivadas.

Sob as seguintes condições:

Atribuição — Você deve creditar a obra da forma especificada pelo autor ou licenciante (mas não de maneira que sugira que estes concedem qualquer aval a você ou ao seu uso da obra).

Uso não comercial — Você não pode usar esta obra para fins comerciais.

Compartilhamento pela mesma licença — Se você alterar, transformar ou criar em cima desta obra, você poderá distribuir a obra resultante apenas sob a mesma licença, ou sob uma licença similar à presente.

Ficando claro que:

Renúncia — Qualquer das condições acima pode ser **renunciada** se você obtiver permissão do titular dos direitos autorais.

Domínio Público — Onde a obra ou qualquer de seus elementos estiver em **domínio público** sob o direito aplicável, esta condição não é, de maneira alguma, afetada pela licença.

Outros Direitos — Os seguintes direitos não são, de maneira alguma, afetados pela licença:

- Limitações e exceções aos direitos autorais ou quaisquer **usos livres** aplicáveis;
- Os **direitos morais** do autor;
- Direitos que outras pessoas podem ter sobre a obra ou sobre a utilização da obra, tais como **direitos de imagem** ou privacidade.

Aviso — Para qualquer reutilização ou distribuição, você deve deixar claro a terceiros os termos da licença a que se encontra submetida esta obra. A melhor maneira de fazer isso é com um link para esta página.

Módulo 7

ISO/OSI Network Management Framework

Introdução

O modelo OSI (Open Systems Interconnection) de gerenciamento de redes é um conjunto de normas e padrões editados pela ISO (International Organization for Standardization) em 1989 com o objetivo de prover uma metodologia para gerenciar redes, serviços e equipamentos de telecomunicações.

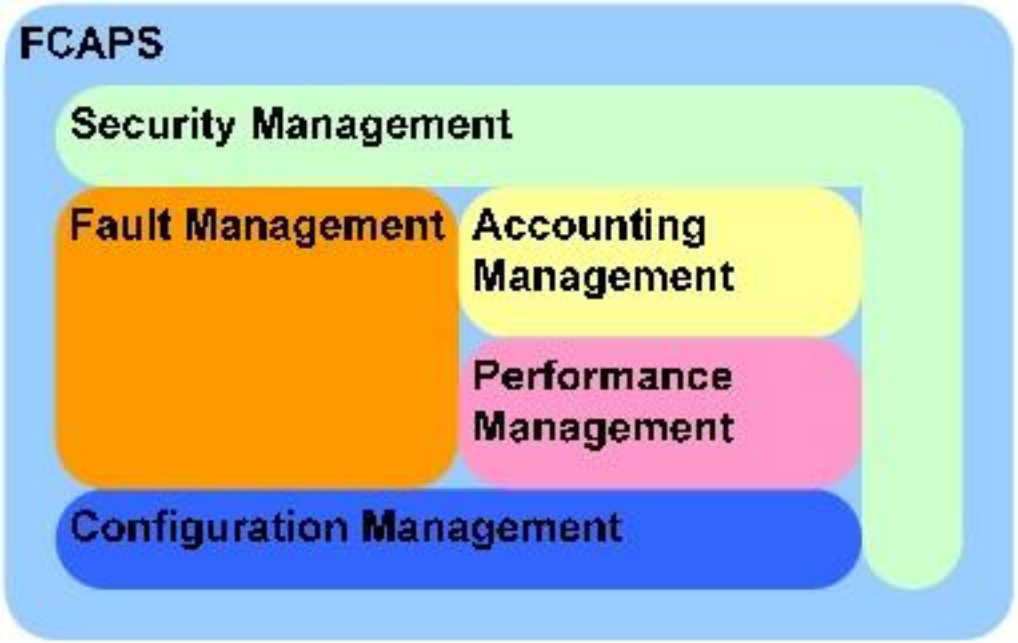
FCAPS

Neste modelo de gerenciamento de redes a ISO identificou um conjunto de cinco áreas críticas, que ficou conhecido pela sigla FCAPS, um acrônimo para *fault* (falha), *configuration* (configuração), *accounting* (contabilidade), *performance* (desempenho) e *security* (segurança).

Em organizações que não possuem tarifação, a área de *accounting* pode ser substituída por *administration* (administração).

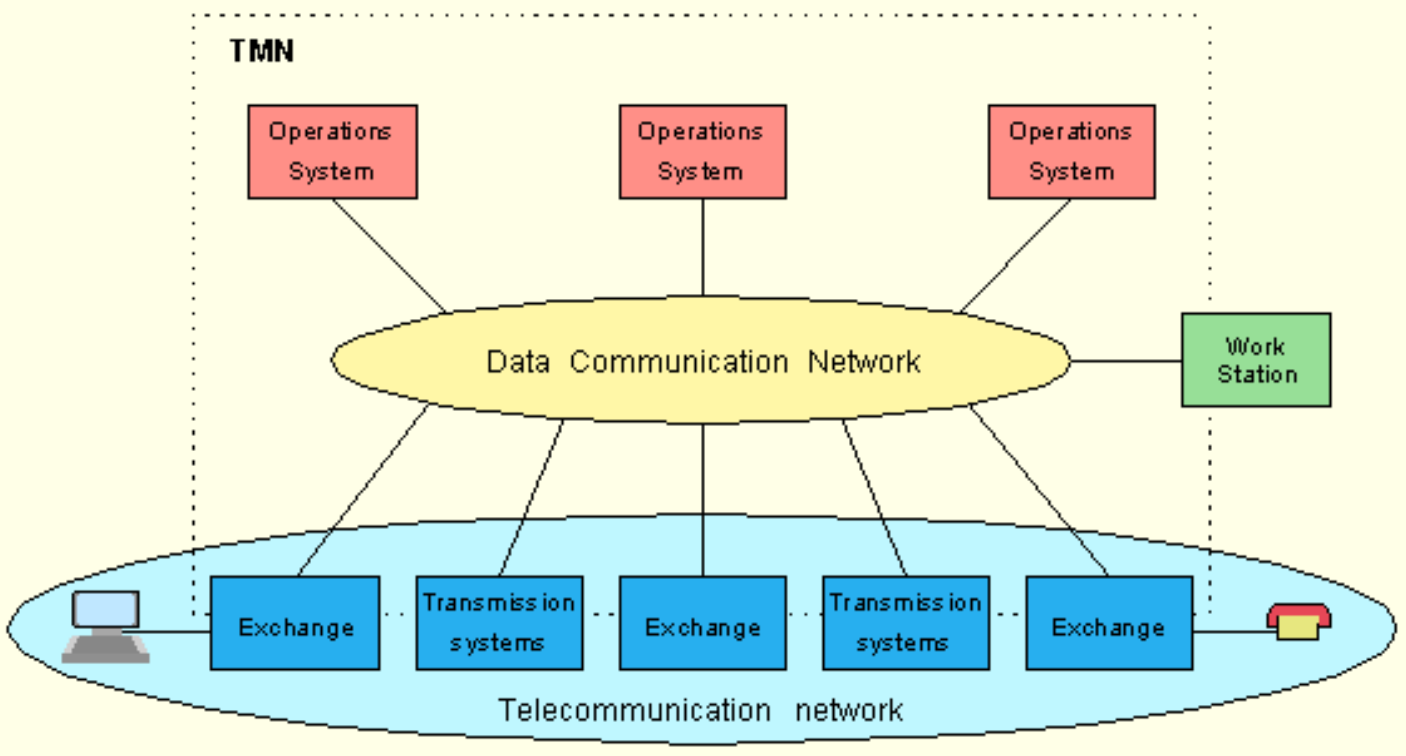
FCAPS

De acordo com a Cisco, as cinco áreas do modelo de gerenciamento de redes OSI/ISO se relacionam da seguinte forma:



TMN

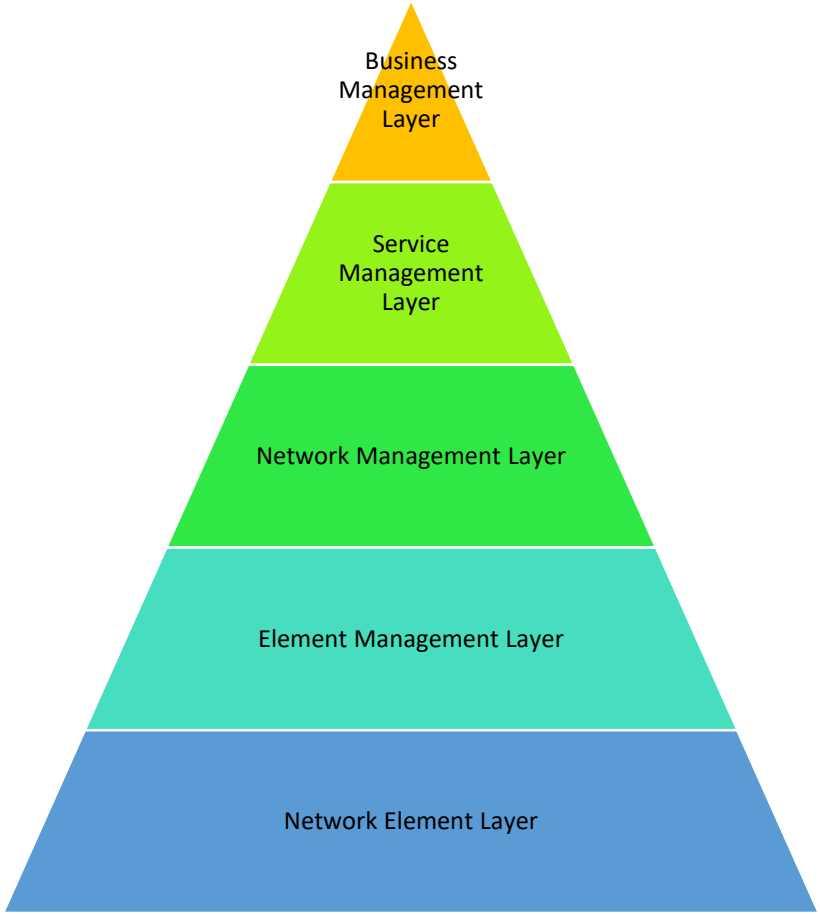
O modelo TMN é um conjunto de recomendações editados pela ITU em 1988 com o objetivo de prover uma metodologia para gerenciar redes, serviços e equipamentos de telecomunicações.



TMN – arquitetura lógica

A arquitetura lógica ou LLA (Logical Layered Architecture) tem por objetivo restringir atividades de gerência em camadas. São cinco as camadas:

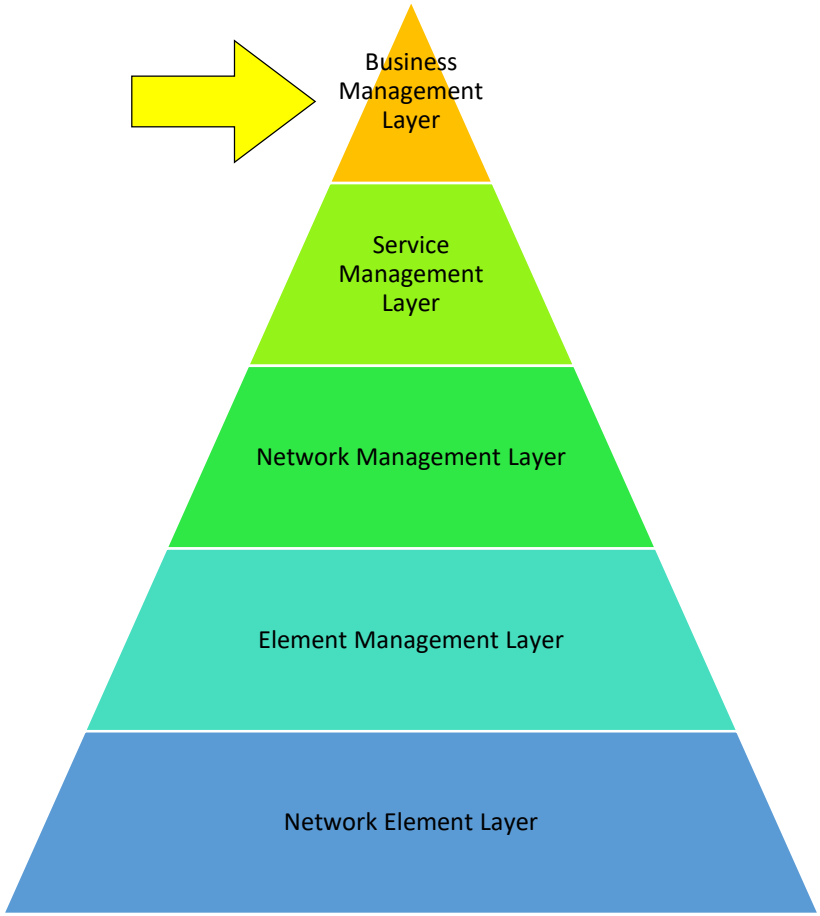
- Camada de gerência de negócios
- Camada de gerência de serviços
- Camada de gerência de rede
- Camada de gerência de elementos de rede
- Camada de elementos de rede



TMN – arquitetura lógica

A camada de gerência de negócios ou BML (Business Management Layer) gerencia todos os aspectos ligados ao negócio, como nichos de mercado, política de preços, área de atuação, serviços a serem oferecidos, etc.

Está mais relacionada com o gerenciamento estratégico e tático do que com o gerenciamento operacional.

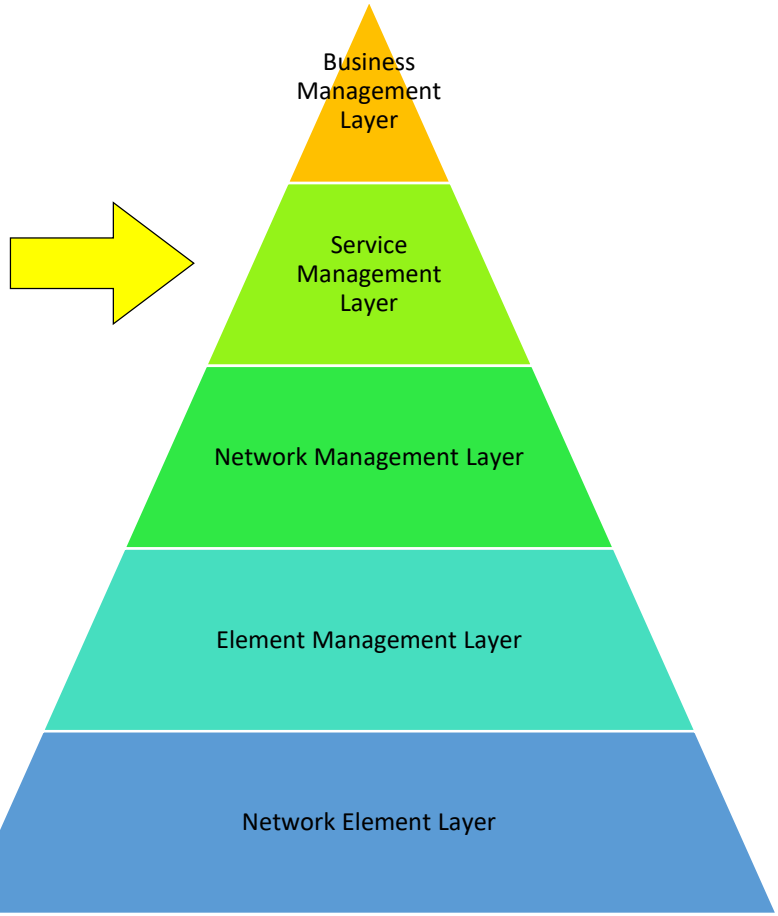


TMN – arquitetura lógica

A camada de gerência de serviços ou SML (Service Management Layer) é responsável por gerenciar os serviços oferecidos ao clientes e aos usuários internos da organização, procurando atender os requisitos de qualidade de serviço e de custo/benefício determinados pela mesma.

Exemplo de funções desta camada:

- Gerenciamento da qualidade de serviço;
- Tarifação;
- Manutenção do cadastro de usuários;
- Etc.

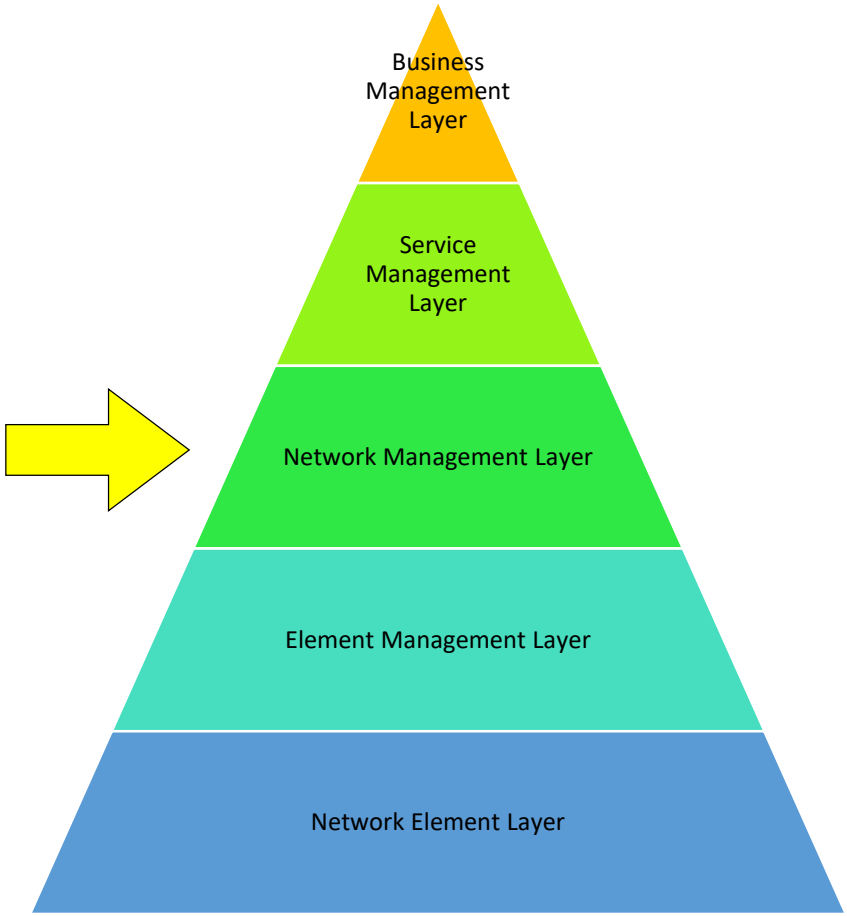


TMN – arquitetura lógica

A camada de gerência de rede ou NML (Network Management Layer) é responsável por gerenciar as funções relacionadas a interação entre os diversos equipamentos que formam os sistemas responsáveis pela entrega de serviços de telecomunicações aos clientes e consumidores. Em outras palavras, é responsável por gerenciar um conjunto de equipamentos que formam uma rede.

Exemplos de funções desta camada:

- Criação de enlaces de comunicação;
- Modificação de tabelas de roteamento;
- Monitoração de utilização de enlaces;
- Detecção de falhas;
- Otimização de desempenho da rede;
- Etc.

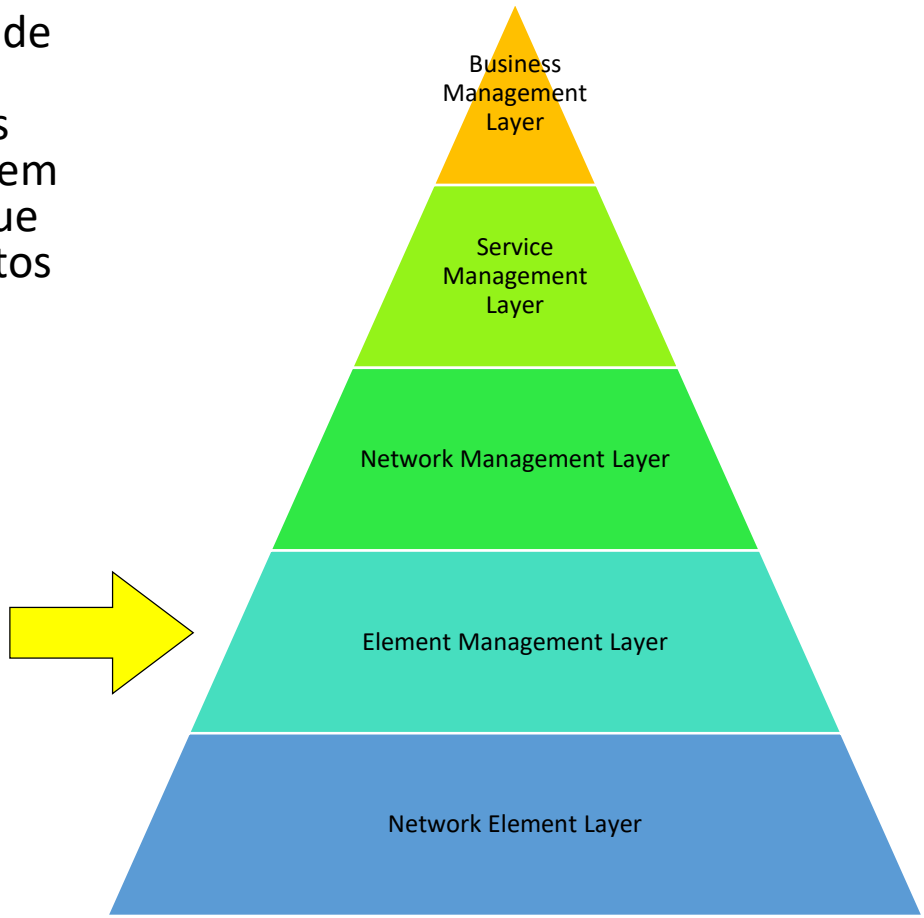


TMN – arquitetura lógica

A camada de gerência de elementos de rede ou EML (Element Management Layer) é responsável por gerenciar os elementos e dispositivos que compõem uma rede ou sistema específicos e que se encontram na camada de elementos de rede.

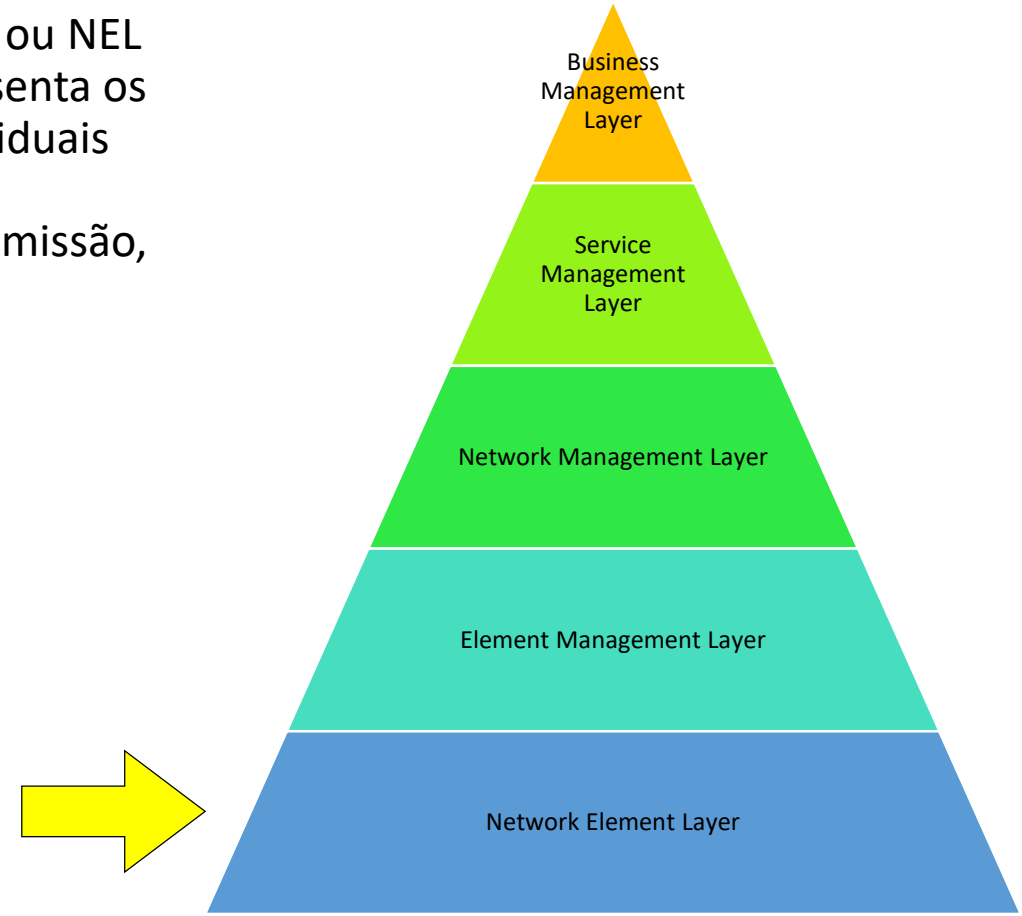
Exemplos de funções desta camada:

- Detecção de erros;
- Medição de recursos com CPU e memória;
- Medição de temperatura do equipamento;
- Medição do consumo de energia;
- Coleta de dados estatísticos;
- Etc.



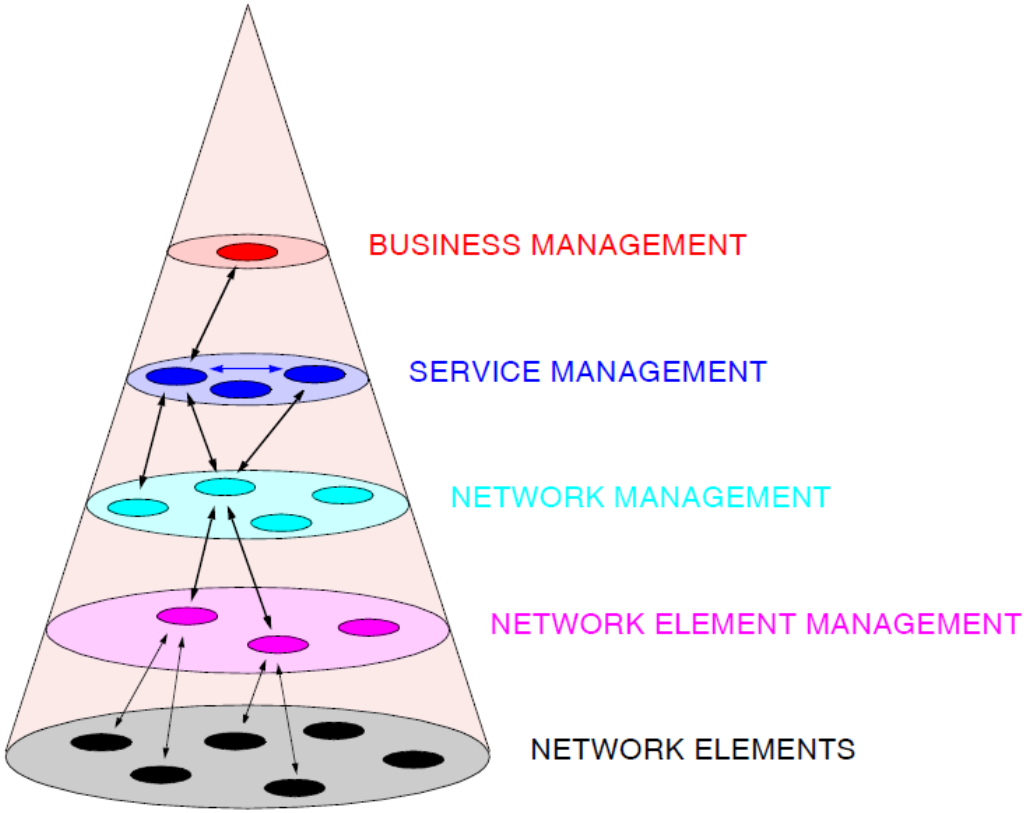
TMN – arquitetura lógica

A camada de elemento de rede ou NEL (Network Element Layer) representa os elementos ou dispositivos individuais da rede, como roteadores, comutadores, sistemas de transmissão, distribuição, etc.



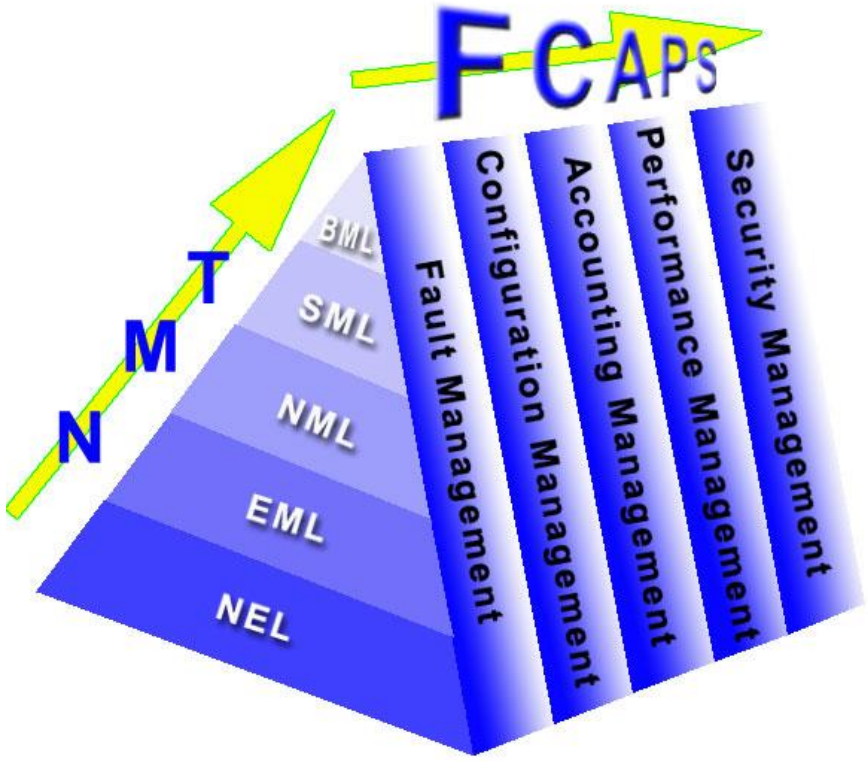
TMN – arquitetura lógica

A figura abaixo mostra a relação entre as diversas camadas da arquitetura lógica.



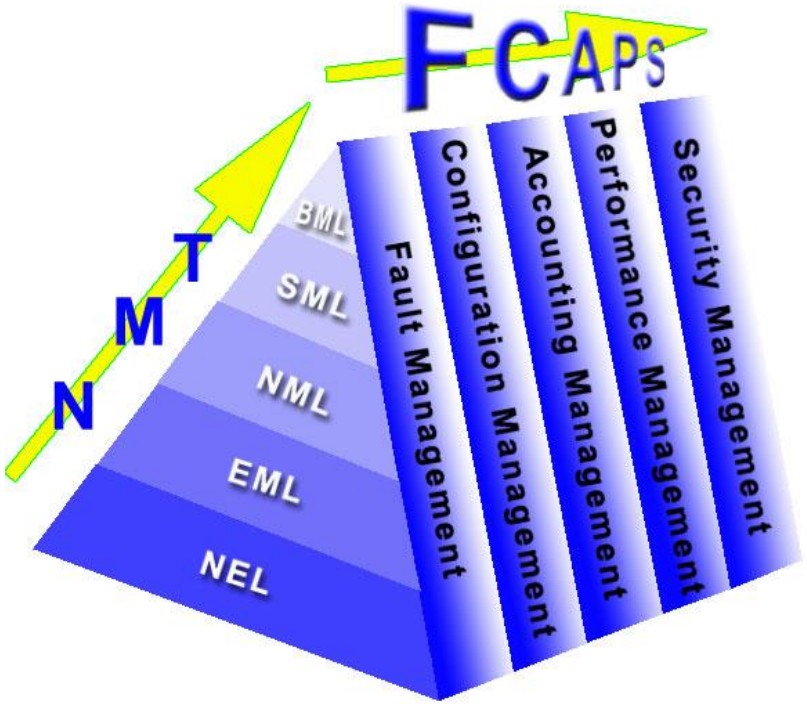
FCAPS versus TMN

O modelo FCAPS da ISO e o modelo TMN da ITU-T podem ser relacionados de acordo com a figura abaixo:



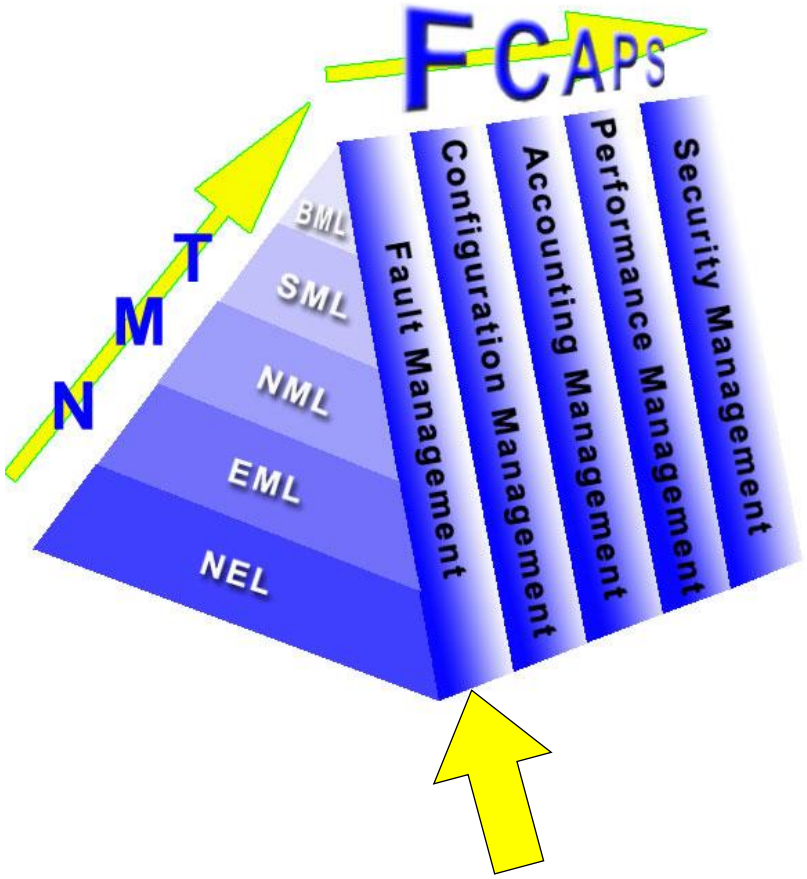
FCAPS

- Gerenciamento de falhas
- Gerenciamento de configuração
- Gerenciamento de contabilidade
- Gerenciamento de desempenho
- Gerenciamento de segurança



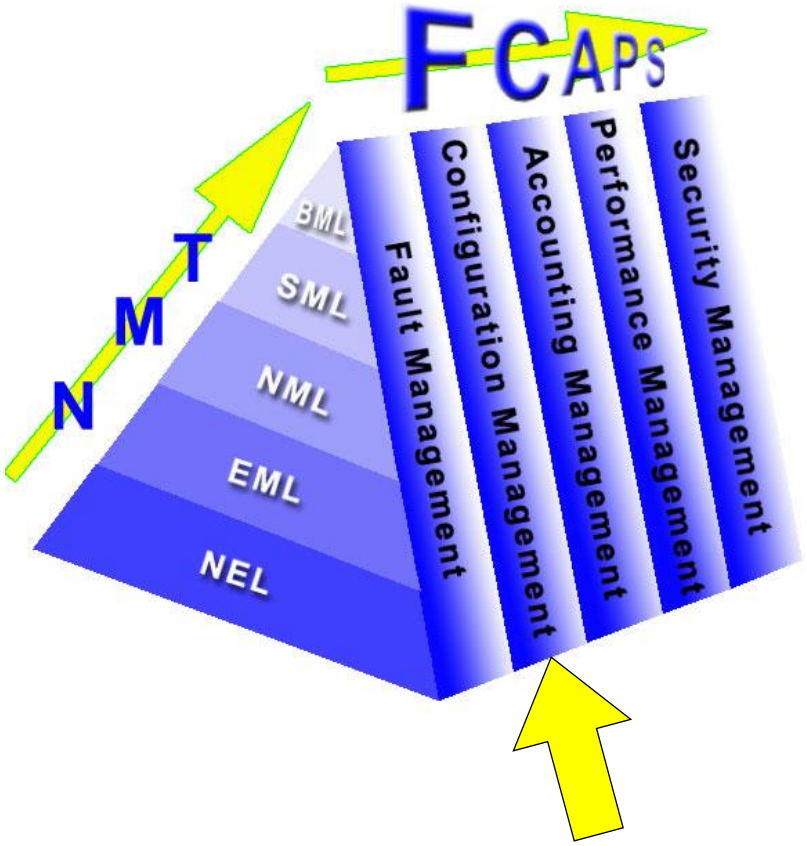
Gerenciamento de falhas

O gerenciamento de falhas é responsável por detectar, isolar e corrigir as falhas que podem ocorrer nos equipamentos ou serviços da rede. É responsável também pela interoperabilidade dos sistemas de telecomunicações.



Gerenciamento de configuração

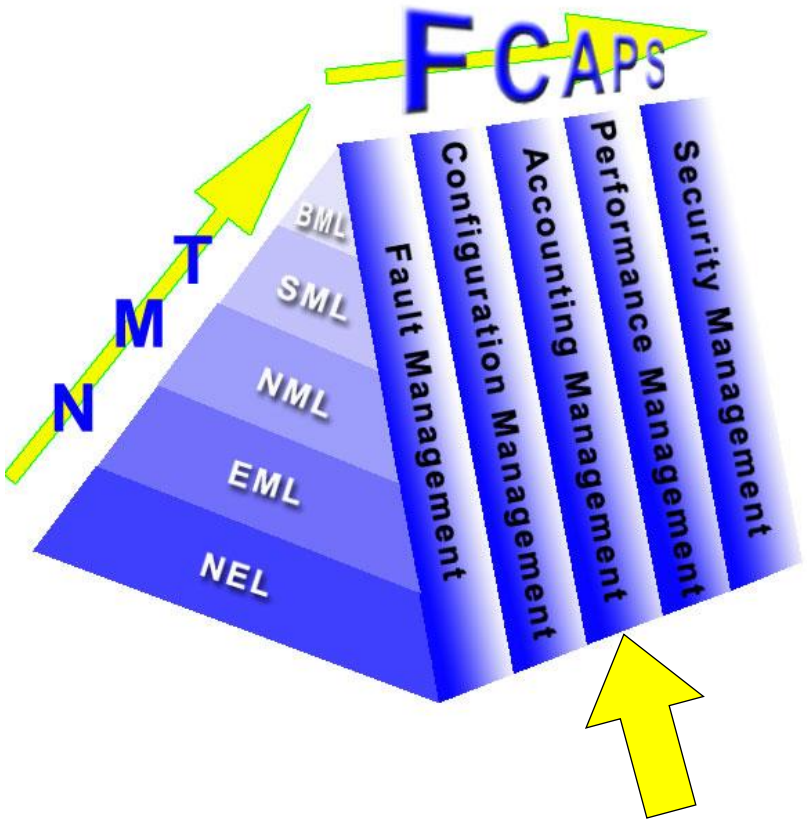
O gerenciamento de configuração é responsável por controlar, identificar e coletar informações de configuração dos equipamentos de telecomunicações.



Gerenciamento de contabilidade

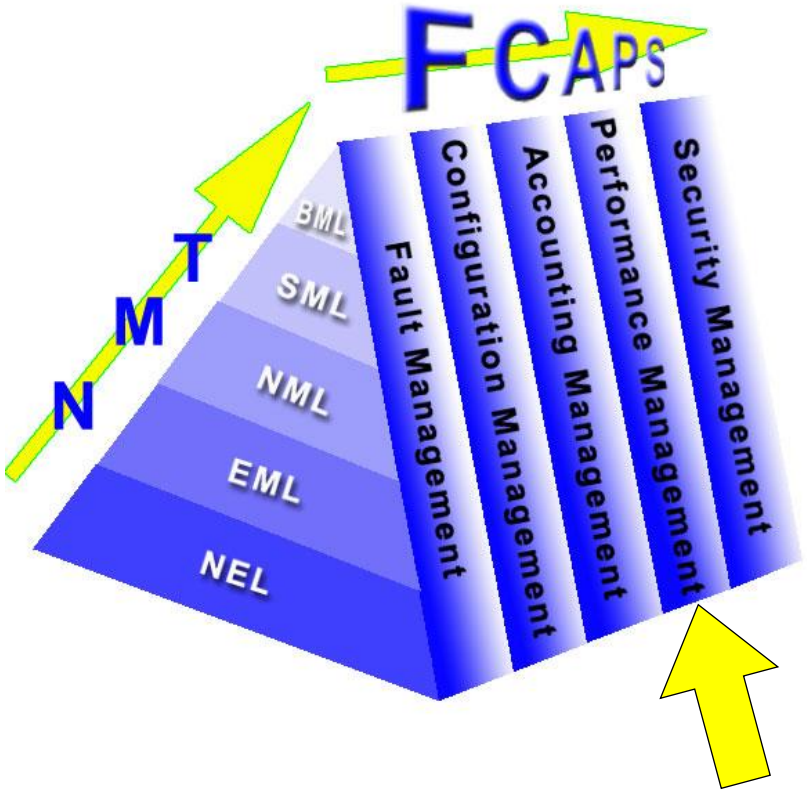
O gerenciamento de contabilidade é responsável por medir o uso dos serviços de rede de modo a determinar o custos para os provedores de serviços e demais clientes e consumidores.

Quando a organização não possui sistemas de tarifação, o gerenciamento de contabilidade pode ser substituído pelo gerenciamento de administração.



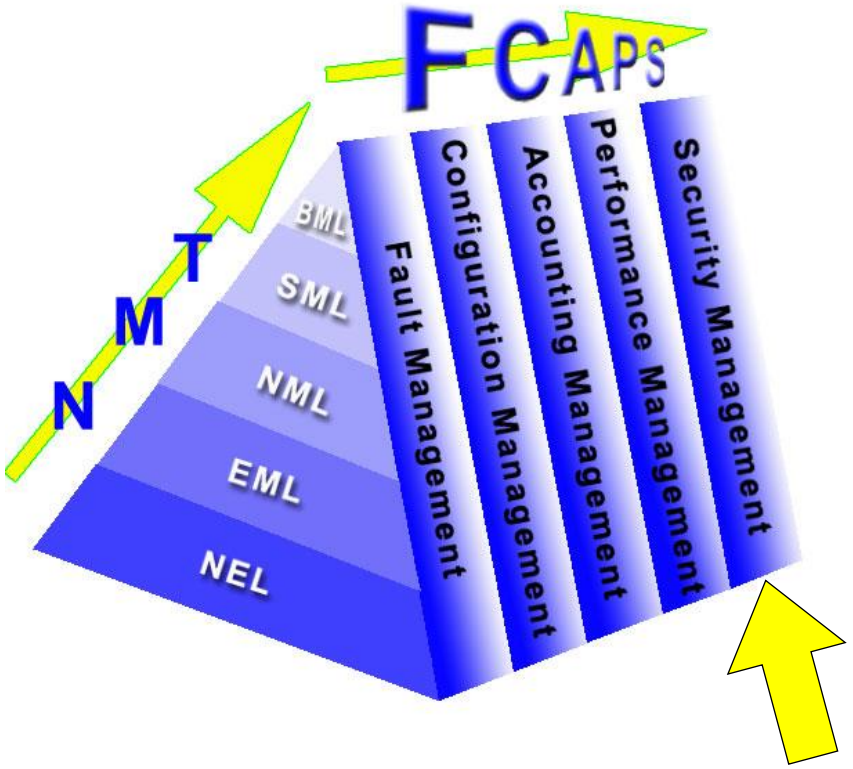
Gerenciamento de desempenho

O gerenciamento de desempenho é responsável por medir e avaliar a qualidade do serviço percebido pelo usuário ou especificada nos acordos de nível de serviços, bem como identificar possíveis gargalos e congestionamentos na rede de telecomunicações.



Gerenciamento de segurança

O gerenciamento de segurança é responsável por administrar o acesso e as permissões de usuários aos diversos sistemas, serviços e equipamentos de rede de telecomunicações.



Para saber mais...

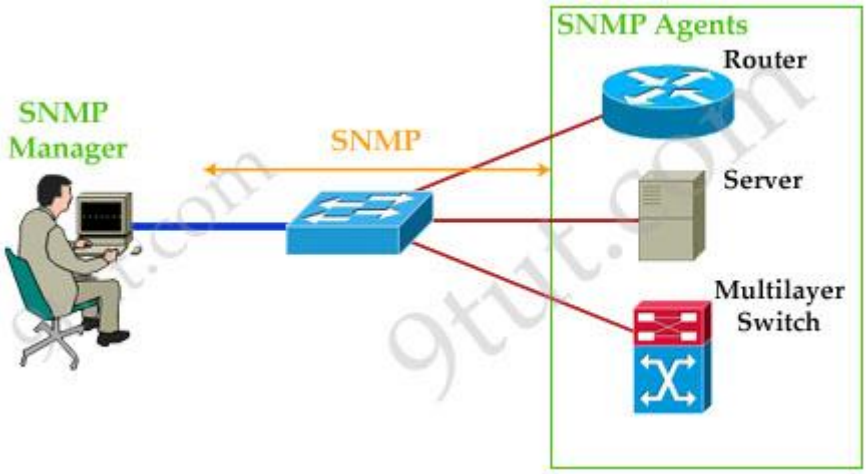
… acesse a norma ISO/IEC 7498-4: Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 4: Management framework, da International Organization for Standardization (ISO) e da International Electrotechnical Commission (IEC).

Módulo 8

Simple Network Management Protocol

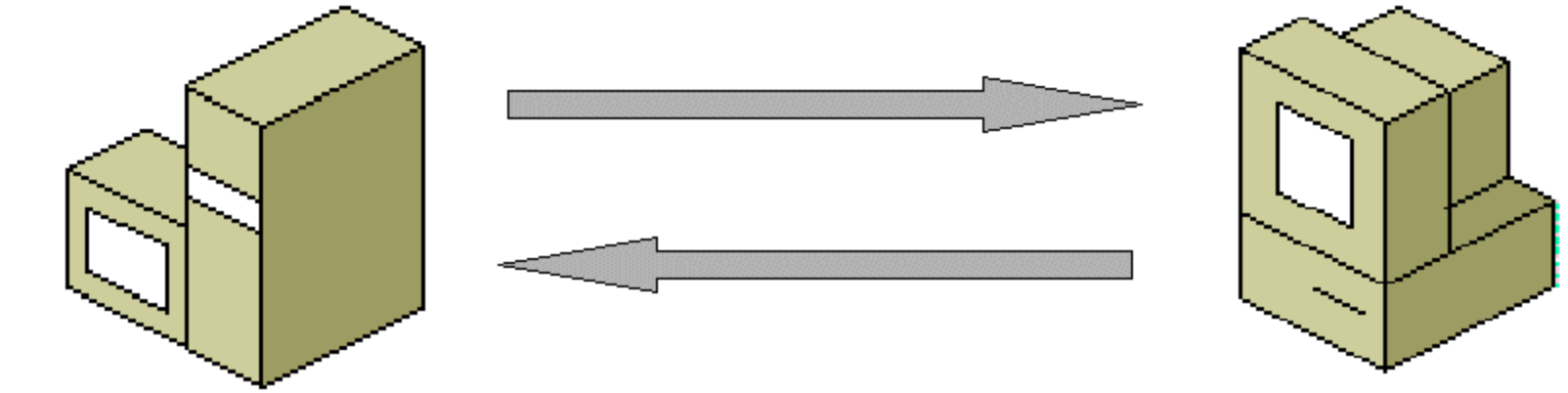
Introdução

O Simple Network Management Protocol ou Protocolo Simples de Gerência de Rede é um protocolo da pilha TCP/IP responsável pela troca de informações entre dispositivos de redes com o intuito de configurar, monitorar e detectar falhas.



SNMP

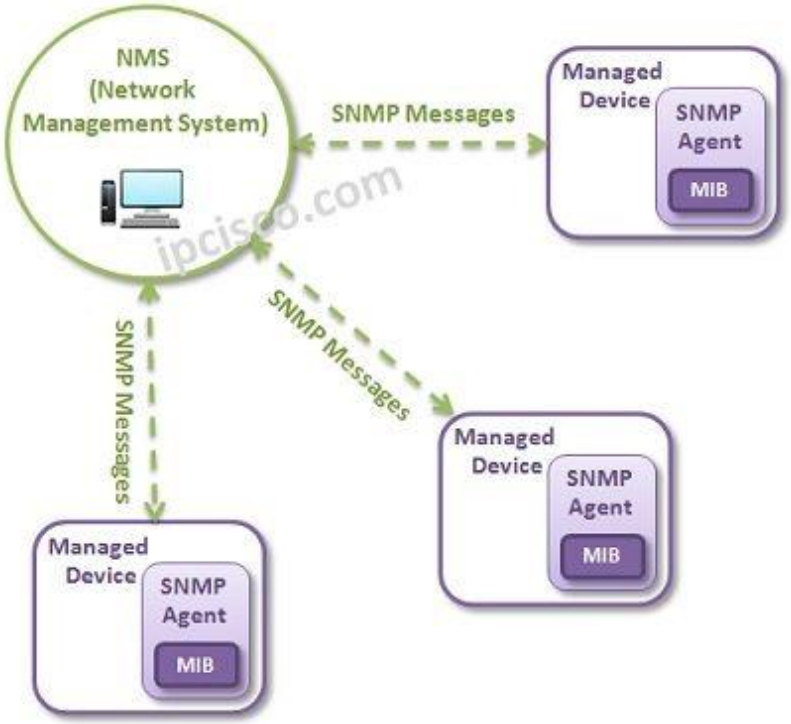
O SNMP não é um protocolo que segue o modelo cliente/servidor, pois a iniciativa da comunicação pode partir de qualquer dispositivo. Os termos mais apropriados a serem usados são gerente e agente, onde o primeiro indica a entidade que irá centralizar as informações de gerenciamento e o segundo o objeto ou dispositivo a ser gerenciado.



SNMP – arquitetura

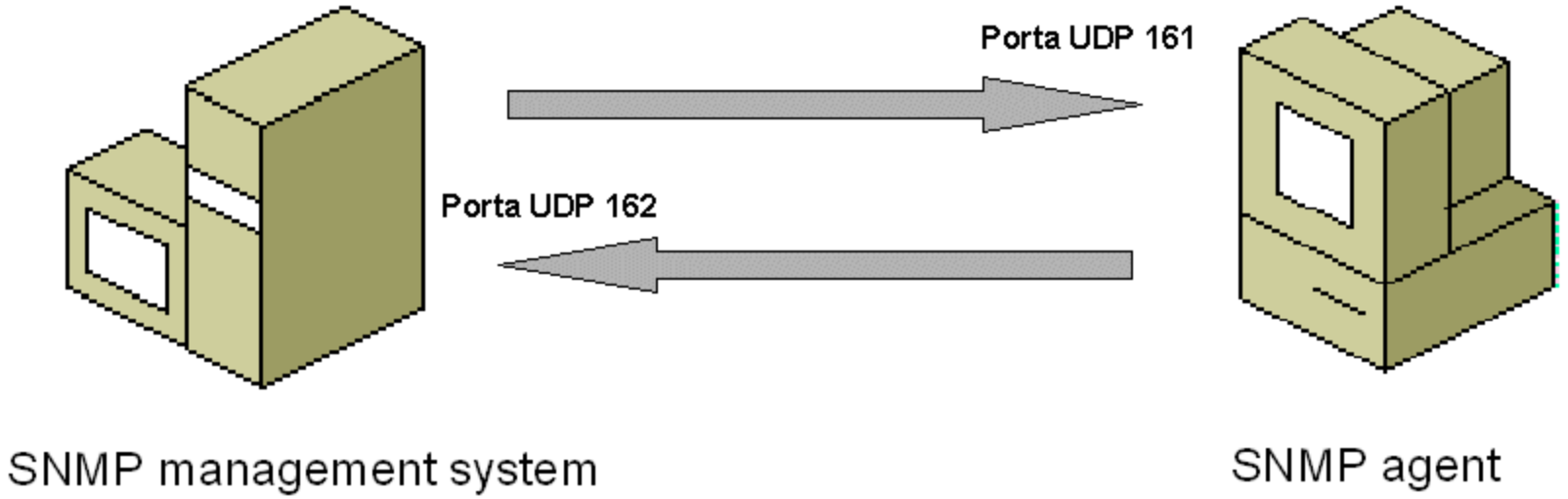
Na arquitetura SNMP o gerente também é conhecido como Network Management System (NMS), ou Sistema de Gerenciamento de Rede.

Nos dispositivos gerenciados devem ser instalados agentes que possuem uma Base de Informações de Gerenciamento, ou Management Information Base (MIB), que são as informações que aquele agente pode disponibilizar ao gerente NMS.



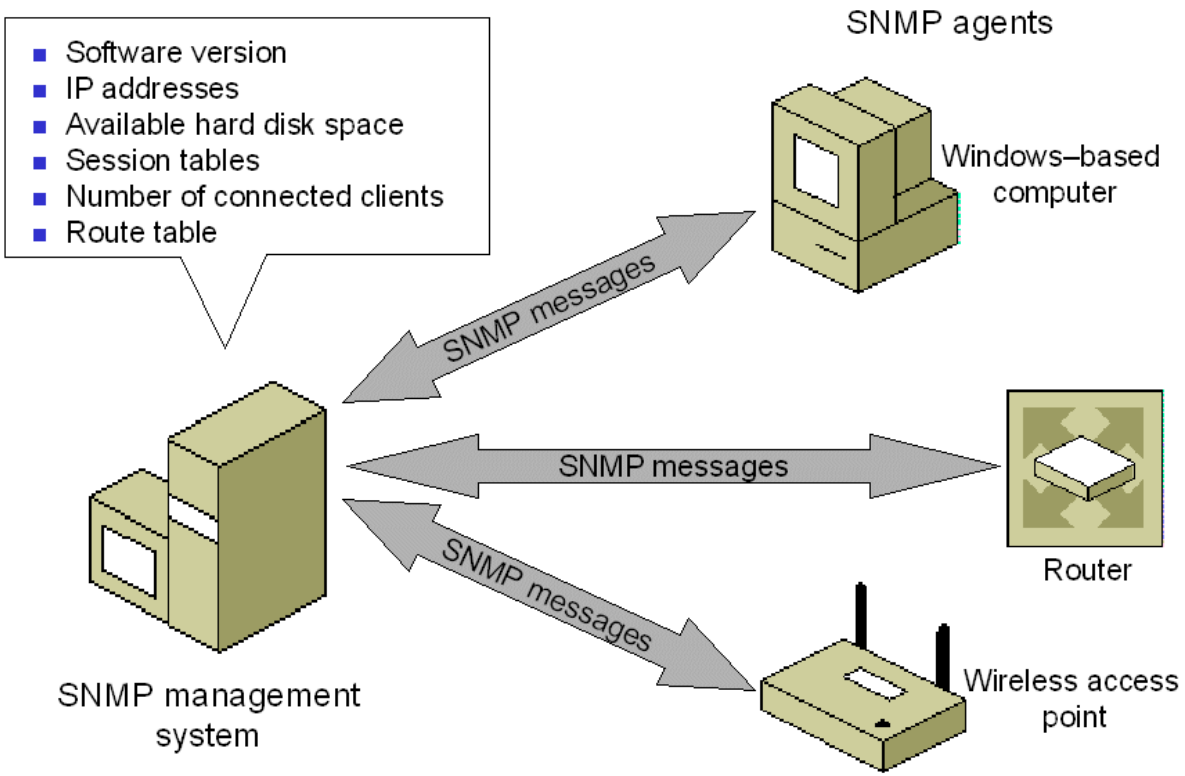
SNMP – portas de comunicação

Quando o sistema gerente deseja comunicar-se com o dispositivo gerenciado, o gerente envia uma requisição para a porta UDP 161 do dispositivo. Quando o dispositivo precisa enviar uma notificação para o sistema gerente, o agente envia uma mensagem para a porta UDP 162 do gerente.



SNMP – informações

O sistema de gerenciamento (gerente) pode obter informações de qualquer dispositivo de rede compatível com o protocolo SNMP.



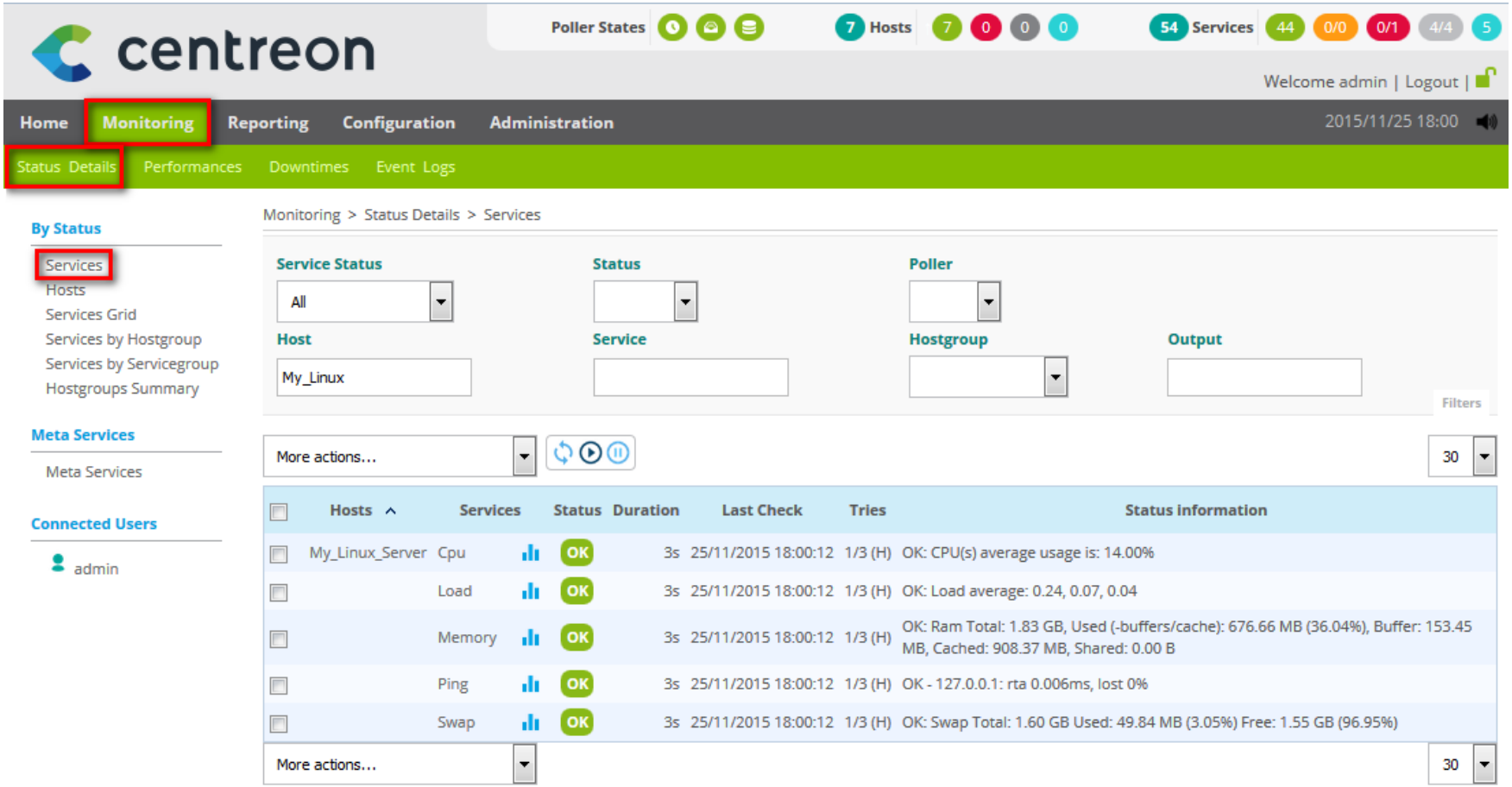
SNMP – versões

O protocolo SNMP possui três versões:

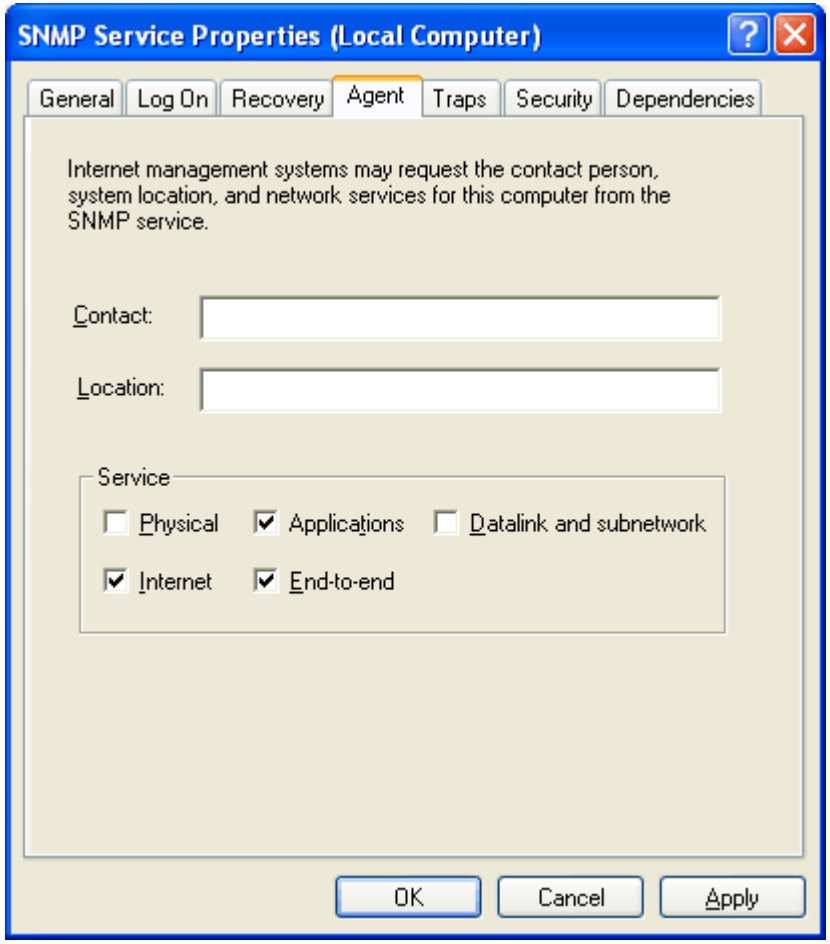
- SNMPv1 – é a primeira versão do SNMP. Requer apenas uma *string* de comunidade de texto simples para autenticação de pacotes. Tem limitações de desempenho e segurança.
- SNMPv2c – é a segunda versão do SNMP e a mais usada. Ela resolve a limitação do SNMPv1 e fornece mais desempenho. Ainda use *strings* da comunidade para autenticação. O SNMPv2 tem mais tipos de pacotes que a versão 1.
- SNMPv3 – é a última versão e concentra-se principalmente em questões de segurança. Adiciona o mecanismo de criptografia e autenticação às mensagens e não usa *strings* de comunidade. Esta versão também tem um formato de mensagem diferente.

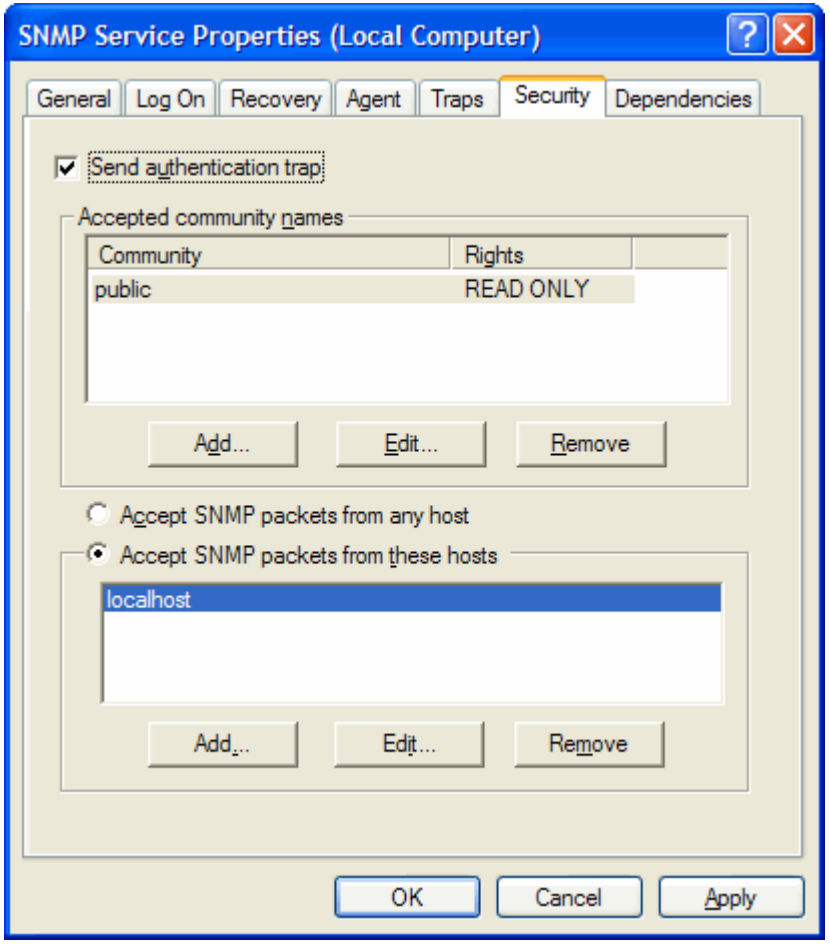
O sistema operacional Windows suporta somente até a versão SNMPv2c.

SNMP – exemplo de gerente (NMS)

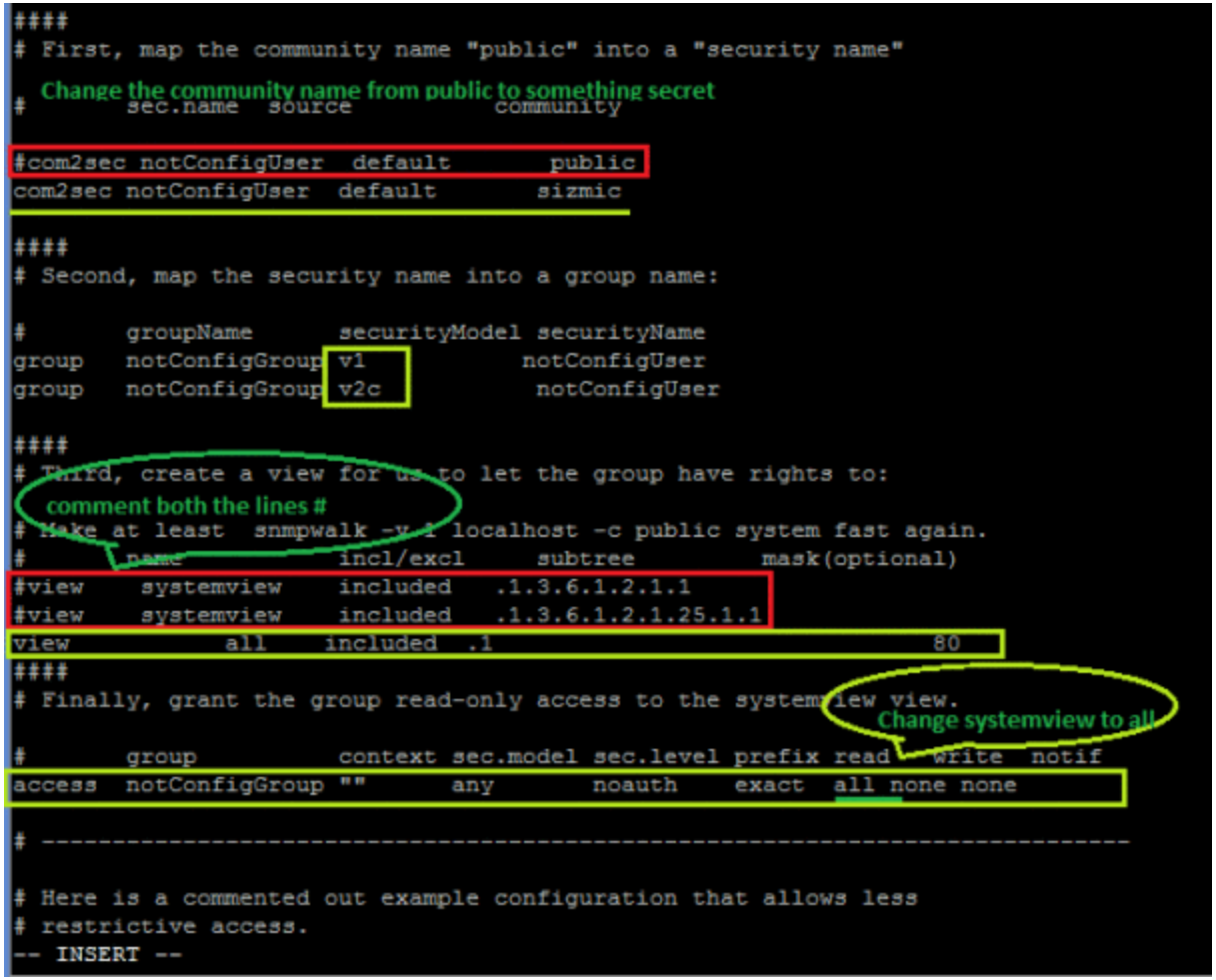


SNMP – configurando o agente no Windows





SNMP – configurando o agente no Linux




```
####
# First, map the community name "public" into a "security name"
#       sec.name  source          community

#com2sec notConfigUser  default       public
com2sec notConfigUser  default       sizmic

####
# Second, map the security name into a group name:

#       groupName      securityModel securityName
group   notConfigGroup v1           notConfigUser
group   notConfigGroup v2c           notConfigUser

####
# Third, create a view for us to let the group have rights to:
# Make at least  snmpwalk -v 1 localhost -c public system fast again.
#       name           incl/excl     subtree         mask(optional)
#view    systemview    included   .1.3.6.1.2.1.1
#view    systemview    included   .1.3.6.1.2.1.25.1.1
view            all    included  .1                               80
####
# Finally, grant the group read-only access to the systemview view.

#       group          context sec.model sec.level prefix read   write  notif
access  notConfigGroup ""      any       noauth    exact  all none none

# -----------------------------------------------------------------------

# Here is a commented out example configuration that allows less
# restrictive access.
-- INSERT --
```

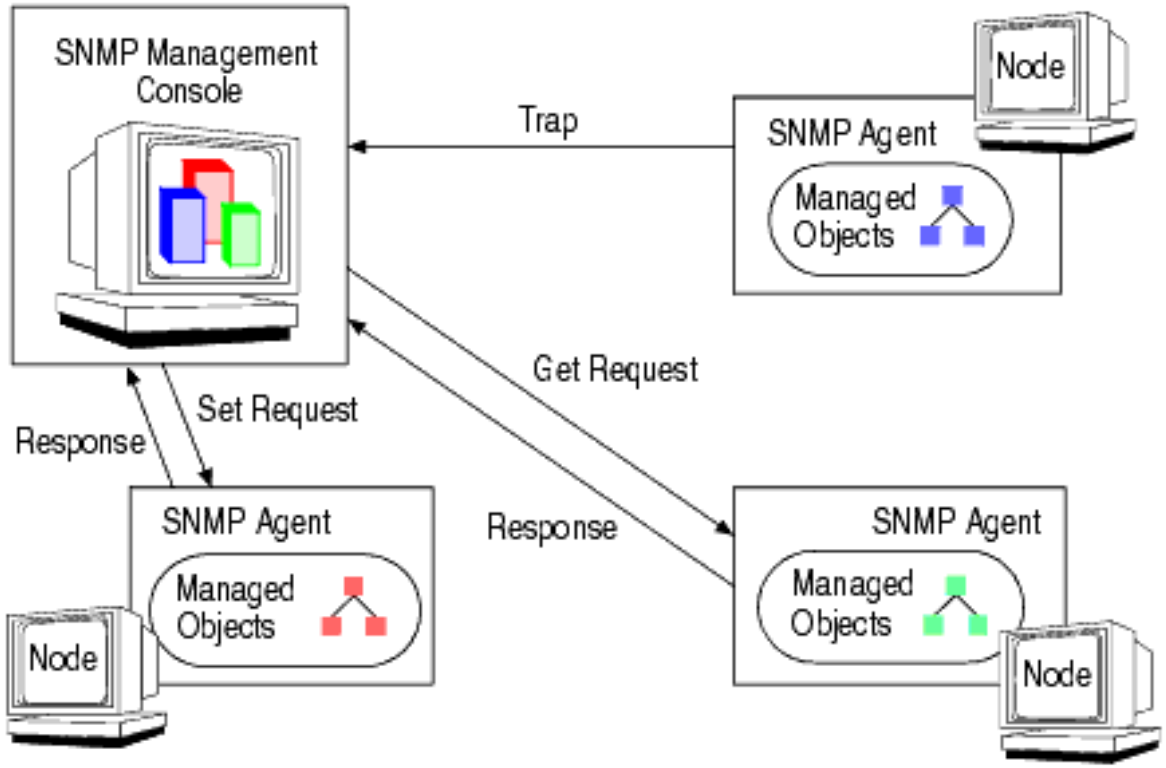
SNMP – configurando o agente no Cisco

Para configurar o agente SNMP em equipamentos Cisco, é necessário executar a seguinte sequencia de comandos na console do equipamento:

```
Router>enable
Router#configure terminal
Router(config)#snmp-server community <nome> ro
Router(config)#snmp-server community <nome> rw
```

SNMP – comandos

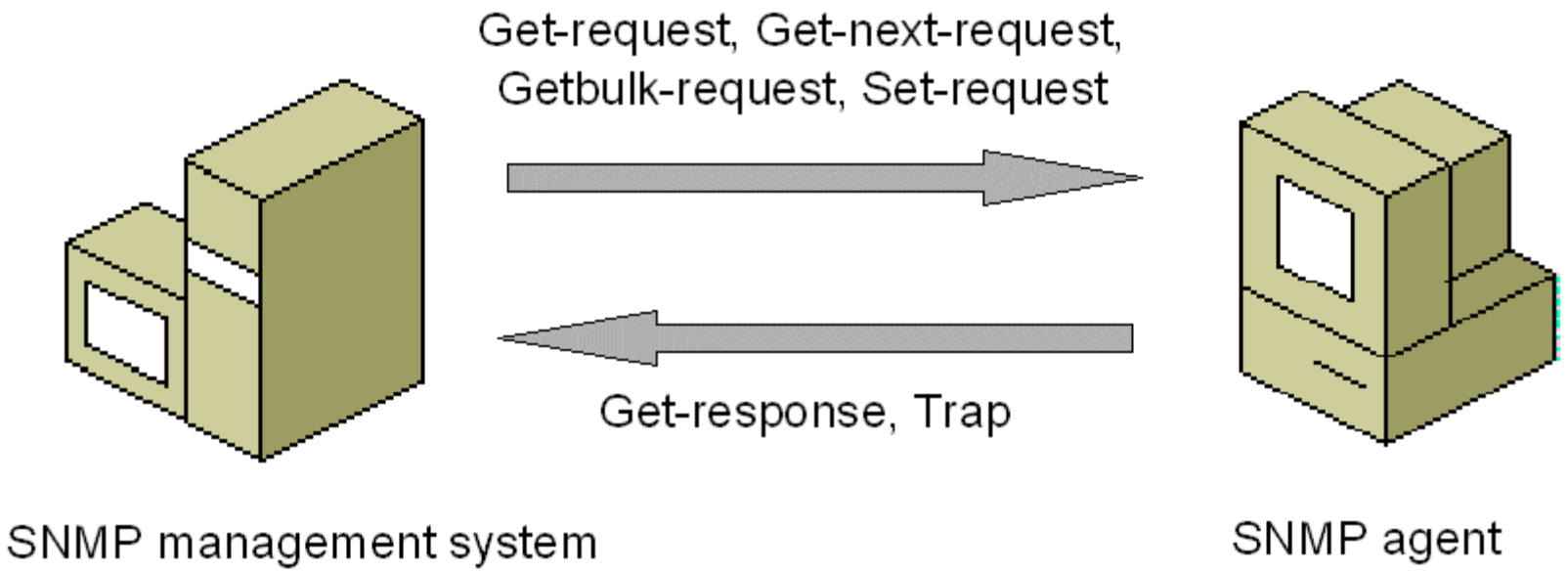
Em uma rede gerenciada por meio do SNMP, o gerente comunica-se com os agentes por meios dos comandos GET, SET e TRAP



SNMP – comandos

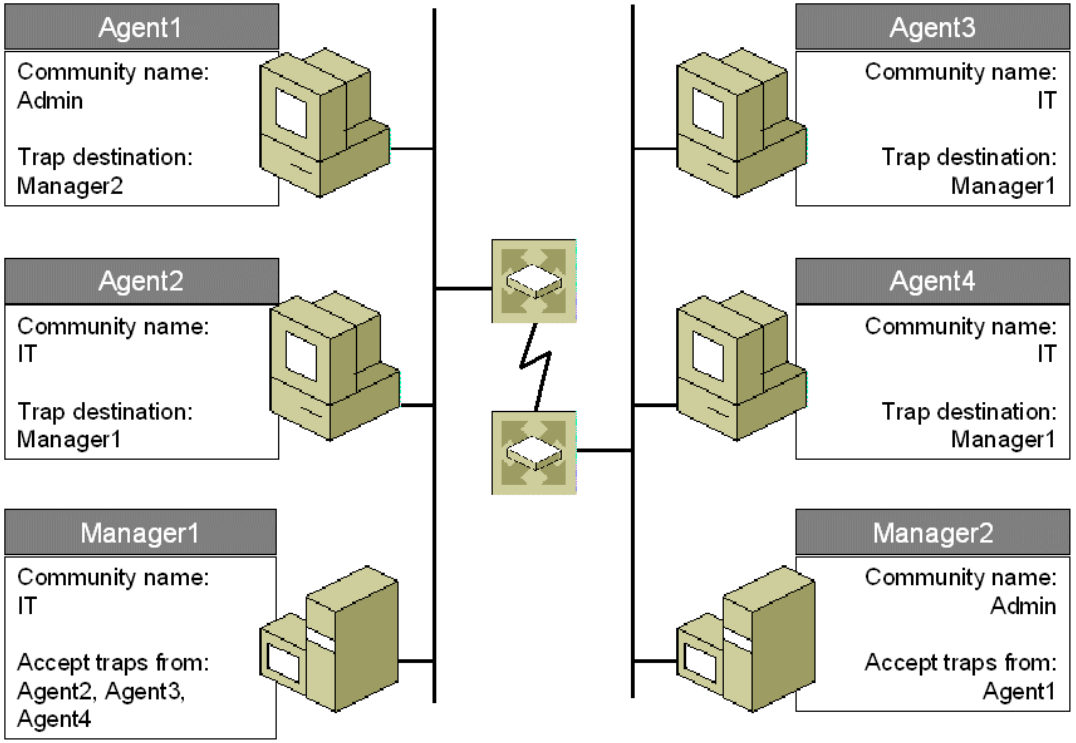
Os comandos Get-request, Get-next-request e Getbulk-request são enviados pelo gerente para obter informações dos agentes, que respondem com o comando Get-response.

O comando Set-request é enviado pelo gerente para fazer modificações nos agentes.

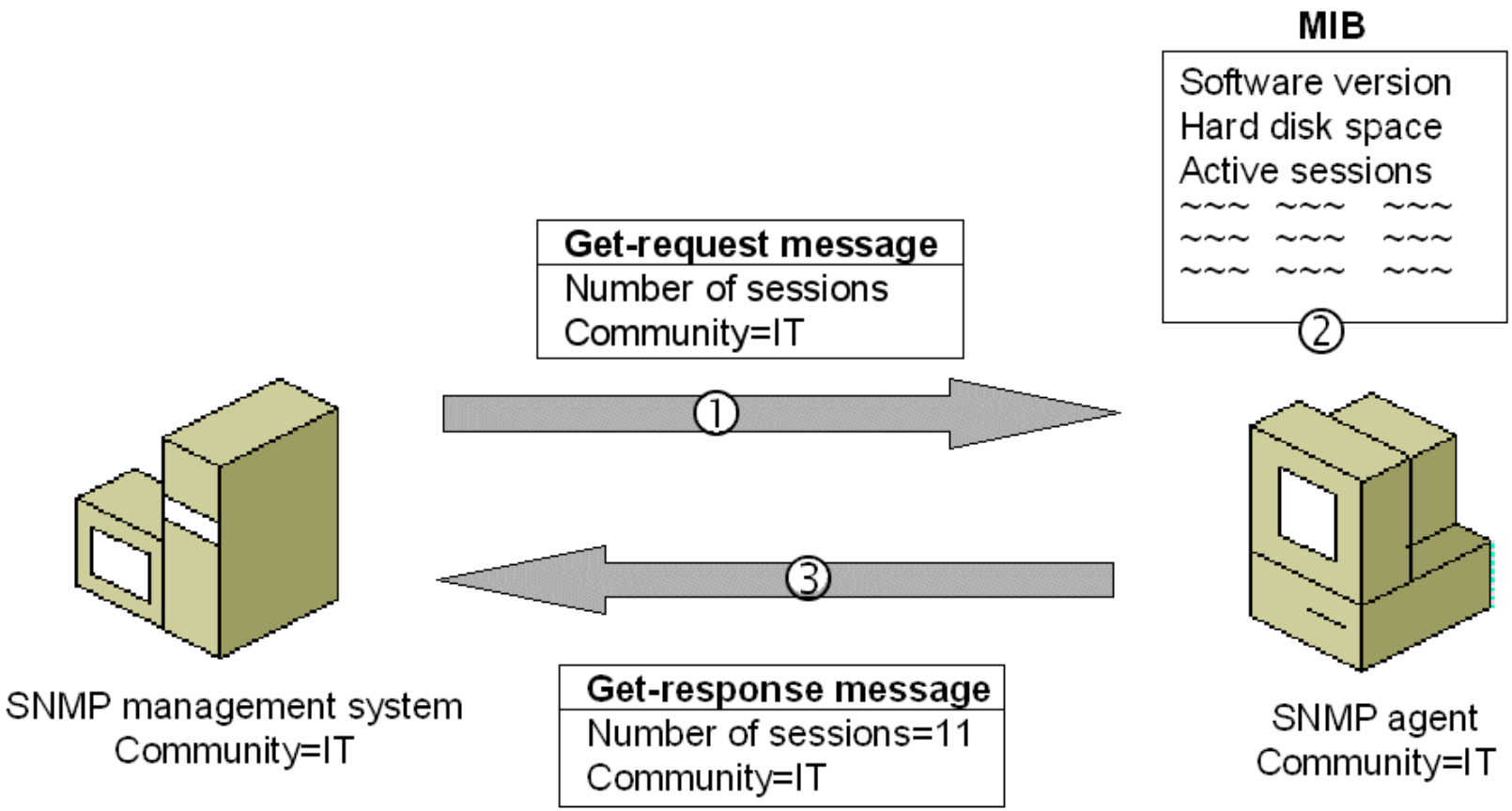


SNMP – comunidades

Quando se configura uma rede SNMP, pode-se optar por configurar comunidades, que são uma forma lógica de organizar como os gerentes e agentes de uma mesma rede irão se comunicar.

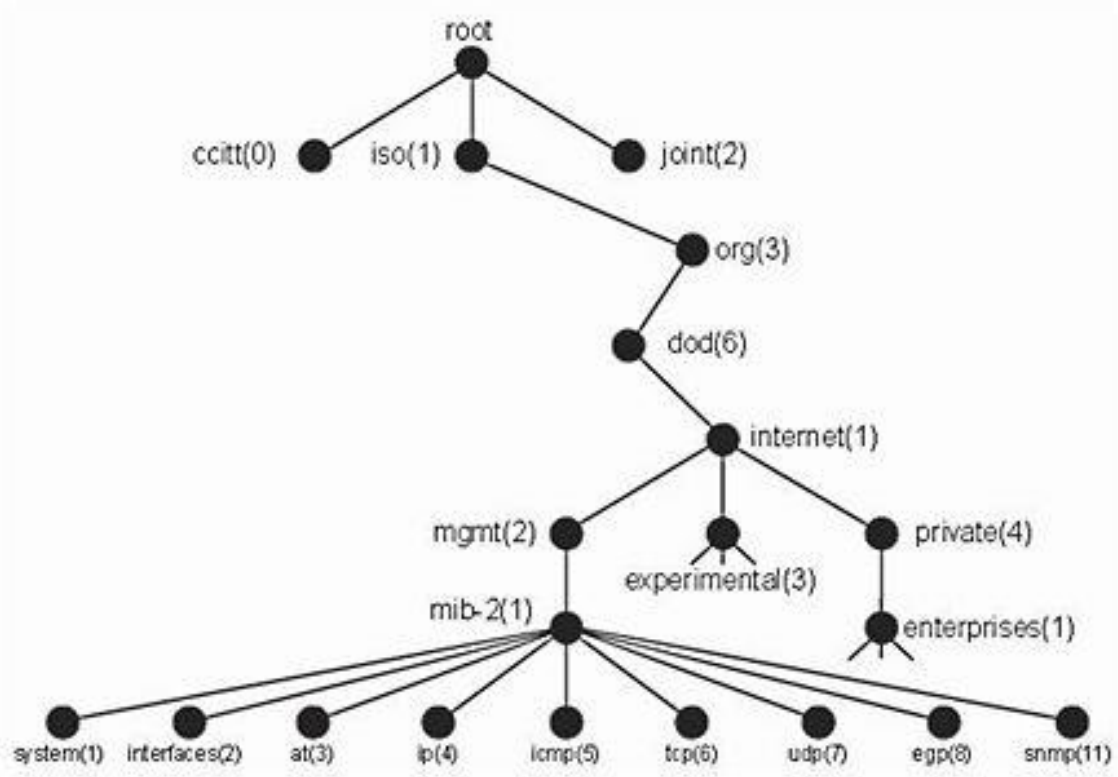


SNMP – exemplo



MIB

As informações que um gerente pode obter de um agente estão descritos na Management Information Base, ou Base de Informações de Gerenciamento.



MIB – exemplo

Em um host com sistema operacional Windows, por meio do utilitário de linha de comando snmputil.exe*, pode-se obter o tipo de hardware, o sistema operacional instalado e a sua versão por meio da seguinte OID (object identifier) da MIB da Microsoft:

```
snmputil get localhost public .1.3.6.1.2.1.1.1.0
Variable = system.sysDescr.0
Value    = String Hardware: Intel64 Family 6 Model 60 Stepping 3 AT/AT
COMPATIBLE - Software: Windows Version 6.3 (Build 15063 Multiprocessor
Free)
```

*SNMPutil é um utilitário disponível no “Windows 2000 Resource Kit Tools”.

Sintaxe: `snmputil <get|getnext|walk> <agente> <comunidade> <OID>`

MIB – exemplo

Neste mesmo host, pode-se obter a informação do tempo (em centésimos de segundos) decorrido desde que o agente foi reinicializado pela última vez.

```
snmputil get localhost public .1.3.6.1.2.1.1.3.0
Variable = system.sysUpTime.0
Value    = TimeTicks 15067632
```

Como o TimeTicks é dado em centésimos de segundo, para descobrir o tempo em horas basta multiplicá-lo por 0,01 e dividir por 3600 (60 segundos x 60 minutos):

$$Tempo\ de\ Atividade\ (uptime) = \frac{TimeTicks \times 0{,}01}{3600}$$

Neste caso, o tempo total decorrido para um TimeTicks igual a 15.067.632 é de 41,85 horas ou 41h51m.

MIB – exemplo

Neste mesmo host, pode-se obter a informação de quantidade de memória RAM (em kilobytes) instalada por meio da seguinte OID da MIB da Microsoft:

```
snmputil get localhost public .1.3.6.1.2.1.25.2.2.0
Variable = host.hrStorage.hrMemorySize.0
Value    = Integer32 16660144
```

Como a quantidade de memória RAM instalada é dada em kB, ao dividir 16.660.144 por 1.024 obtêm-se 16.269,7 MB. Dividindo-se novamente por 1.024 obtêm-se 15,9 GB.

MIB – exemplo

Neste mesmo host, pode-se obter informações sobre o(s) disco(s) por meio da seguinte OID da MIB da Microsoft:

```
snmputil get localhost public .1.3.6.1.2.1.25.2.3.1.3.1
Variable = host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageDescr.1
Value    = String C:\ Label:Windows10_OS  Serial Number f1a6d03c
```

Para verificar todos os discos instalados neste host, pode-se obter tal informação a partir da seguinte OID:

```
snmputil walk localhost public .1.3.6.1.2.1.25.2.3.1.3
Variable = host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageDescr.1
Value    = String C:\ Label:Windows10_OS  Serial Number f1a6d03c

Variable = host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageDescr.2
Value    = String D:\ Label:Lenovo_Recovery  Serial Number f2c7ba81
```

Note que foi usado o comando `walk` ao invés de `get` e que foi omitido o último número da OID.

MIB – exemplo

Para calcular o espaço disponível no disco, pode-se usar os seguintes OID da MIB da Microsoft:

```
snmputil get localhost public .1.3.6.1.2.1.25.2.3.1.4.1
Variable =
host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageAllocationUnits.1
Value    = Integer32 4096

snmputil get localhost public .1.3.6.1.2.1.25.2.3.1.5.1
Variable = host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageSize.1
Value    = Integer32 117884204

snmputil get localhost public .1.3.6.1.2.1.25.2.3.1.6.1
Variable = host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageUsed.1
Value    = Integer32 82822015
```

MIB – exemplo

Como o tamanho do disco (hrStorageSize) e o espaço usado (hrStorageUsed) é dado em unidades de alocação de armazenamento (hrStorageAllocationUnits), que é dado em bytes, para calcular o espaço livre procede-se da seguinte forma:

Dados:

- hrStorageAllocationUnits = 4.096 bytes;
- hrStorageSize = 117.884.204 unidades de alocação de armazenamento;
- hrStorageUsed = 82.822.015 unidades de alocação de armazenamento.

Tamanho do Disco:

$$Tamanho\ do\ Disco = hrStorageSize \times hrStorageAllocationUnits$$

$$Tamanho\ do\ Disco = 117.884.204 \times 4.096$$

$$Tamanho\ do\ Disco = 482.853.699.584\ bytes$$

-- ou --

$$Tamanho\ do\ Disco = \frac{482.853.699.584}{1.024^3} = 449.69\ GB$$

MIB – exemplo

Dados:

- hrStorageAllocationUnits = 4.096 bytes;
- hrStorageSize = 117.884.204 unidades de alocação de armazenamento;
- hrStorageUsed = 82.822.015 unidades de alocação de armazenamento.

Espaço Usado:

$$Espaço\ Usado = hrStorageUsed \times hrStorageAllocationUnits$$

$$Espaço\ Usado = 82.822.015 \times 4.096$$

$$Espaço\ Usado = 339.238.973.440\ bytes$$

-- ou --

$$Espaço\ Usado = \frac{339.238.973.440}{1.024^3} = 315{,}94\ GB$$

MIB – exemplo

Dados:

- hrStorageAllocationUnits = 4.096 bytes;
- hrStorageSize = 117.884.204 unidades de alocação de armazenamento;
- hrStorageUsed = 82.822.015 unidades de alocação de armazenamento.

Espaço Livre:

$$Espaço\ Livre = (hrStorageSize - hrStorageUsed) \times hrStorageAllocationUnits$$

$$Espaço\ Livre = (117.884.204 - 82.822.015) \times 4.096$$

$$Espaço\ Livre = 143.614.726.144\ bytes$$

-- ou --

$$Espaço\ Livre = \frac{143.614.726.144}{1.024^3} = 133{,}75\ GB$$

MIB – exemplo

Neste mesmo host, pode-se obter a informação do endereço IP da placa de rede por meio da seguinte OID:

```
snmputil walk localhost public .1.3.6.1.2.1.4.20.1.1
Variable = ip.ipAddrTable.ipAddrEntry.ipAdEntAddr.192.168.0.20
Value    = IpAddress 192.168.0.20

Variable = ip.ipAddrTable.ipAddrEntry.ipAdEntAddr.10.0.0.20
Value    = IpAddress 10.0.0.20
```

Note que ao invés de `get` usou-se `walk`, o que significa que se houver mais de uma interface de rede todas serão mostradas.

Para saber mais...

… leia o Tutorial sobre Protocolo de Gerenciamento SNMP, de Beethovem Zanella Dias e Nilton Alves Jr.

… leia o Documento sobre Simple Network Management Protocol, da Microsoft.

Módulo 9

Serviço de Diretório

Introdução

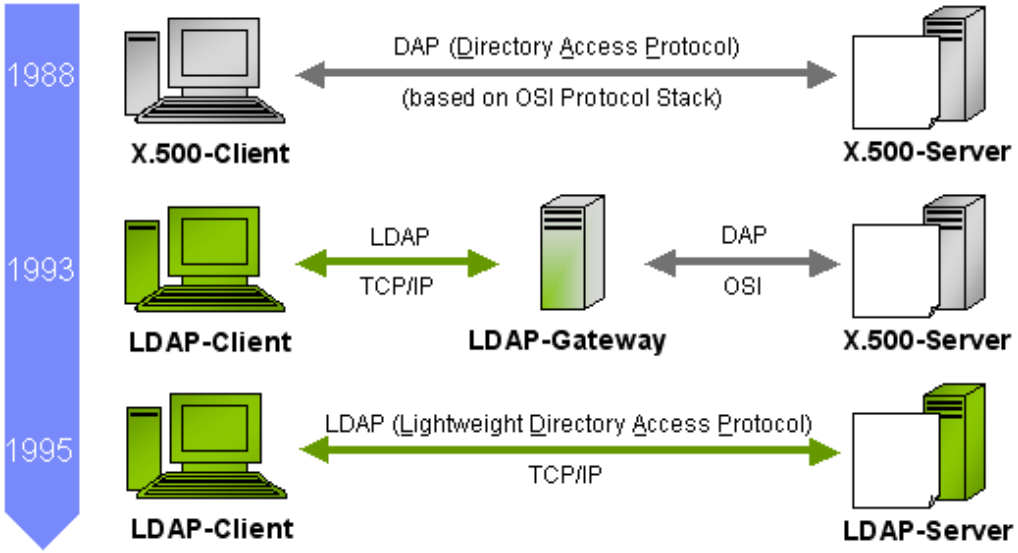
Serviço de diretório é um sistema que armazena e organiza informações sobre usuários, computadores e recursos compartilhados em uma rede de computadores.

Um serviço de diretório é útil para administrar e gerenciar usuários e recursos em uma rede de forma organizada e centralizada.

LDAP

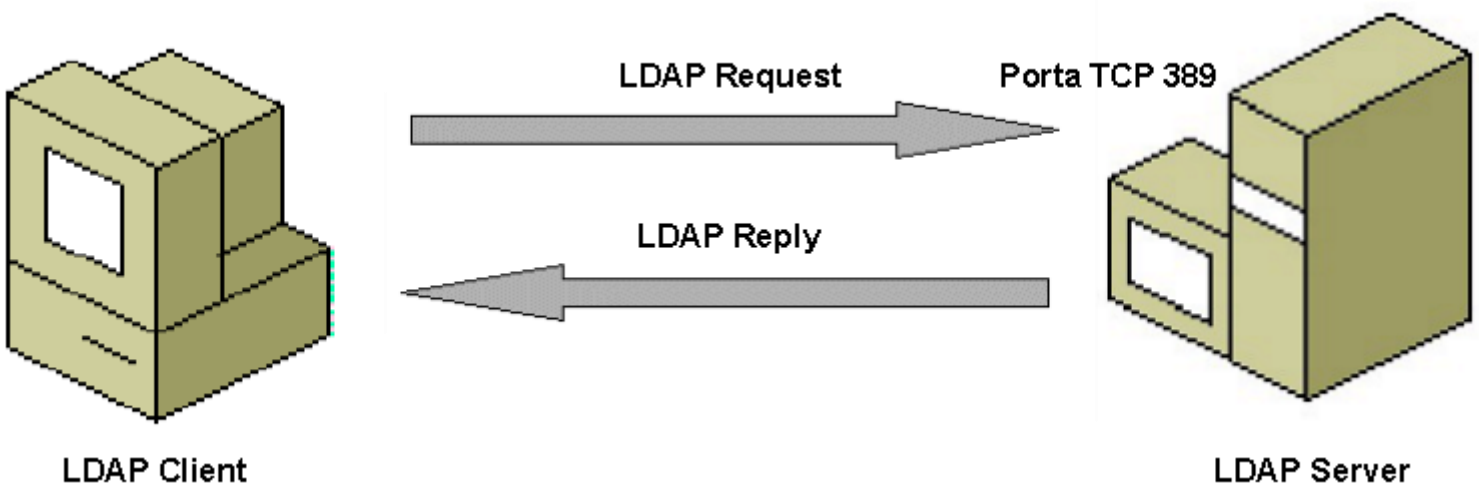
LDAP (Lightweight Directory Access Protocol) ou Protocolo Leve de Acesso à Diretórios tem a função de definir como as informações sobre usuários, computadores e recursos são armazenadas no banco de dados do repositório central do serviço de diretório.

O LDAP é um protocolo baseado no modelo cliente/servidor e foi desenvolvido como alternativa ao protocolo X.500, desenvolvido pela ITU-T e pela ISO.



LDAP

O LDAP é um protocolo que segue o modelo cliente/servidor. O cliente LDAP conecta-se ao servidor LDAP por meio da porta TCP 389.



LDAP

Dentre as diversas implementações do protocolo LDAP, podemos destacar o eDirectory da Novell, o OpenLDAP da comunidade GNU/Linux e o Active Directory da Microsoft.

Novell eDirectory™

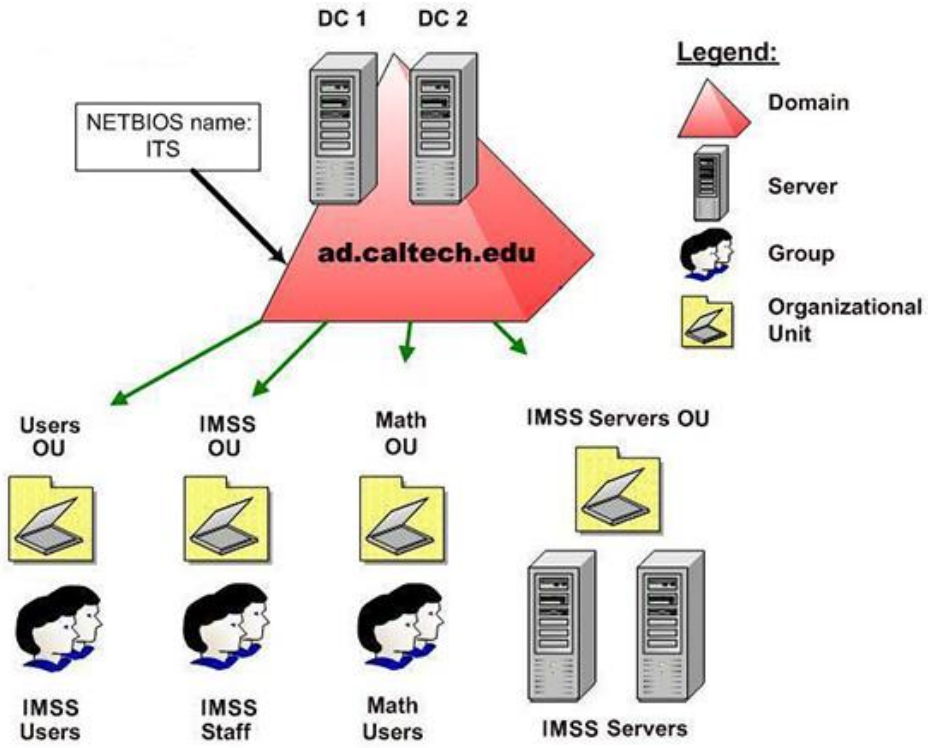
Windows Server®
Active Directory

Active Directory

O Active Directory é a implementação da Microsoft para o serviço de diretório baseado no protocolo LDAP.

Também conhecido como AD, foi introduzido a partir do Windows Server 2000.

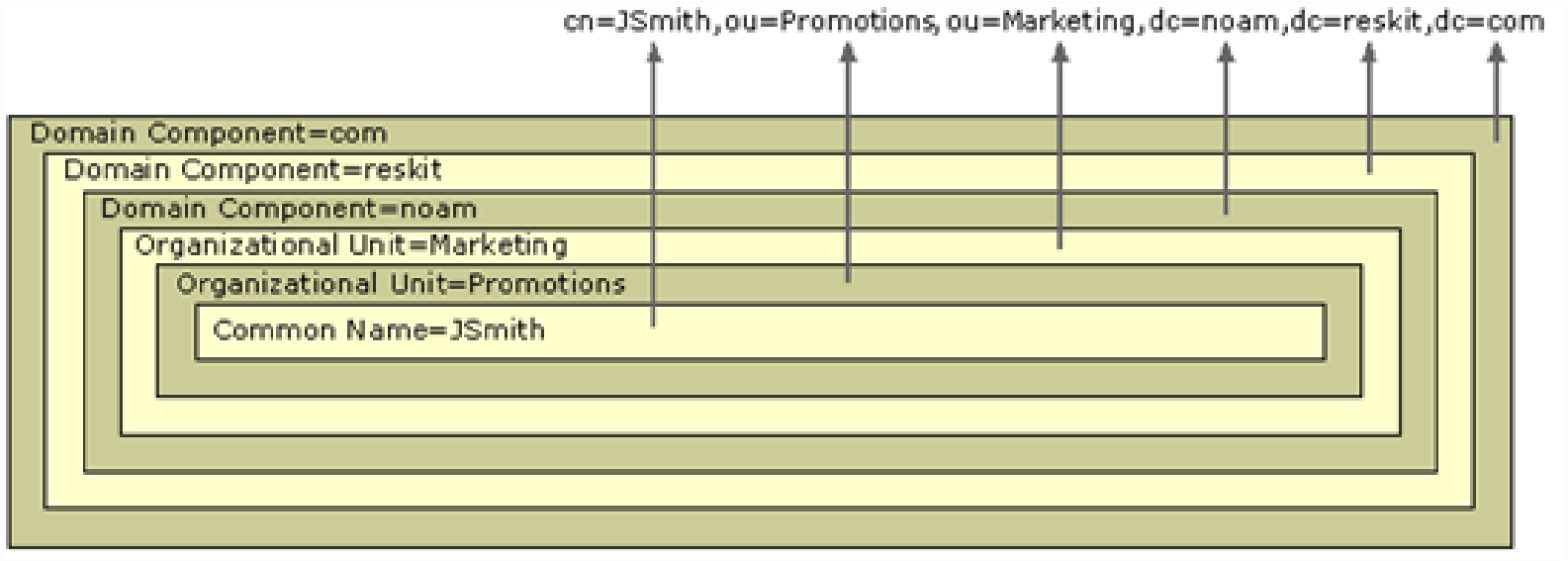
Na nomenclatura da Microsoft, uma unidade administrativa denomina-se Domínio, e é representada por um triângulo. Todo domínio deve ter, no mínimo, um controlador de domínio, também conhecido como DC, que é responsável por conter o banco de dados do serviço de diretório. Os demais servidores do domínio são conhecidos como servidores membros ou members servers.



Active Directory – objetos

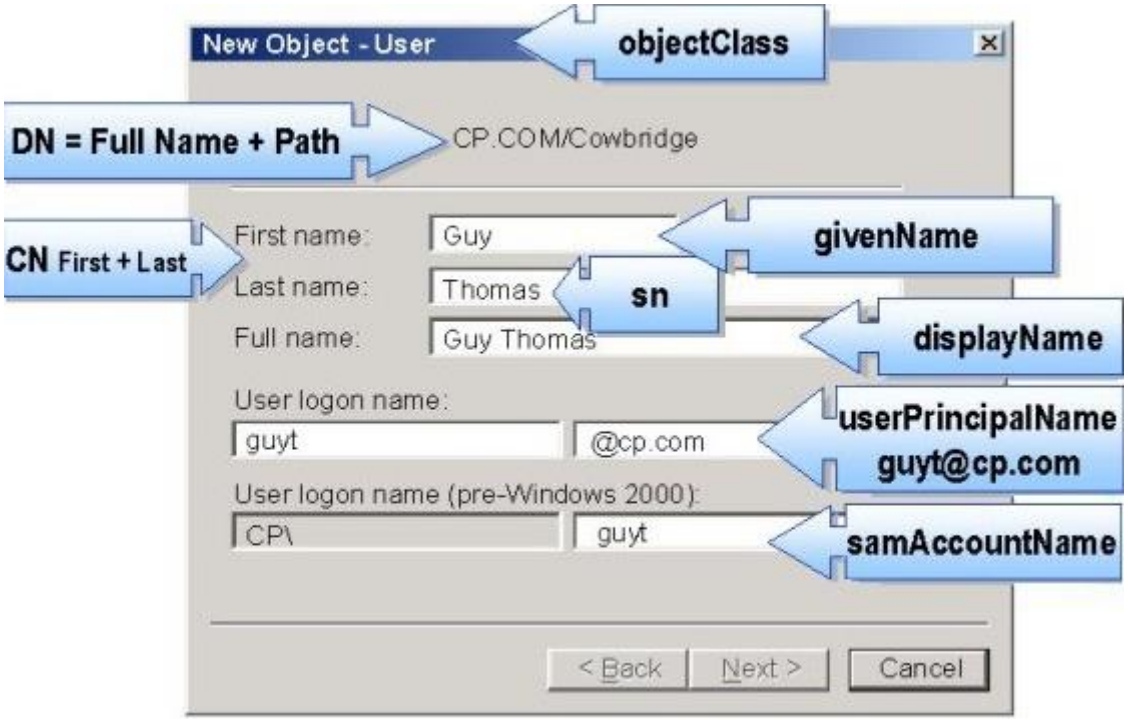
Todo objeto no Active Directory deve possuir um Distinguished Name (nome distinto), que deve ser único e exclusivo.

Isso é possível usando-se o caminho completo do objeto, incluindo o nome do objeto e todos os objetos pai para até a raiz do domínio. Desta forma o cliente LDAP consegue recuperar as informações do objeto do diretório.



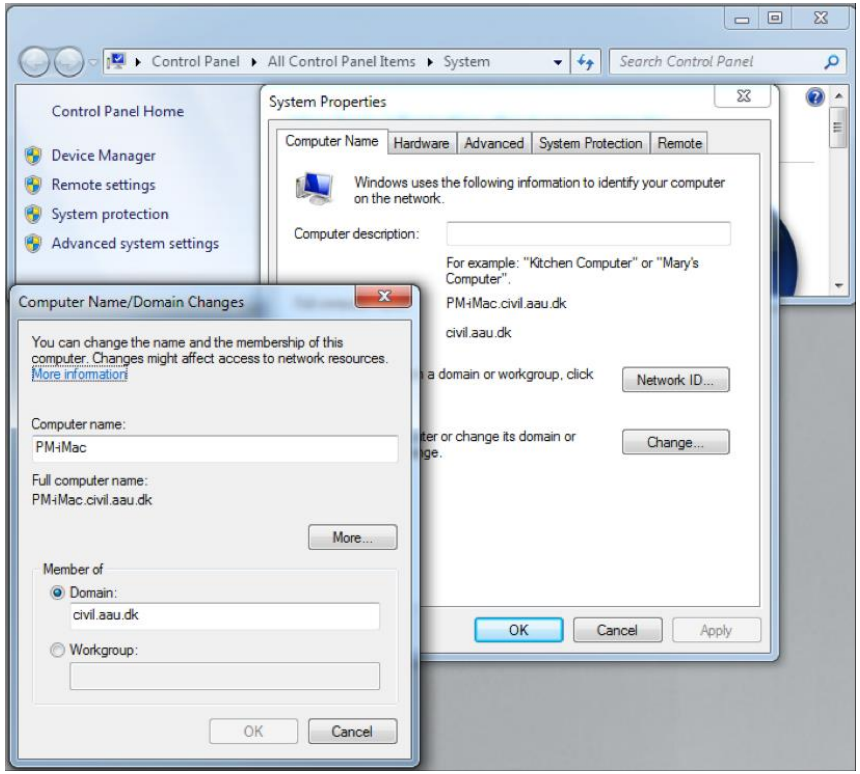
Active Directory – atributos

Atributos são informações sobre um usuário, organização, grupo ou qualquer outro tipo de objeto. Cada atributo é associado a um tipo que fornece diversas propriedades sobre como os clientes e o servidor de diretórios devem interagir com esse atributo.



Active Directory – logon

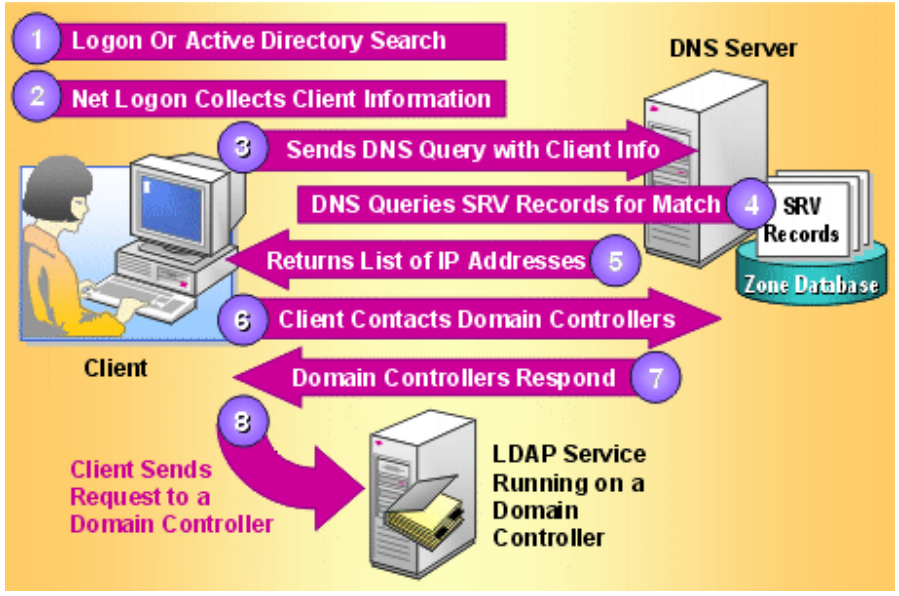
Para que os usuários possam conectar-se no domínio, as estações de trabalho devem estar registradas no domínio e os usuários devem possuir contas cadastradas no serviço de diretório.



Active Directory – DNS

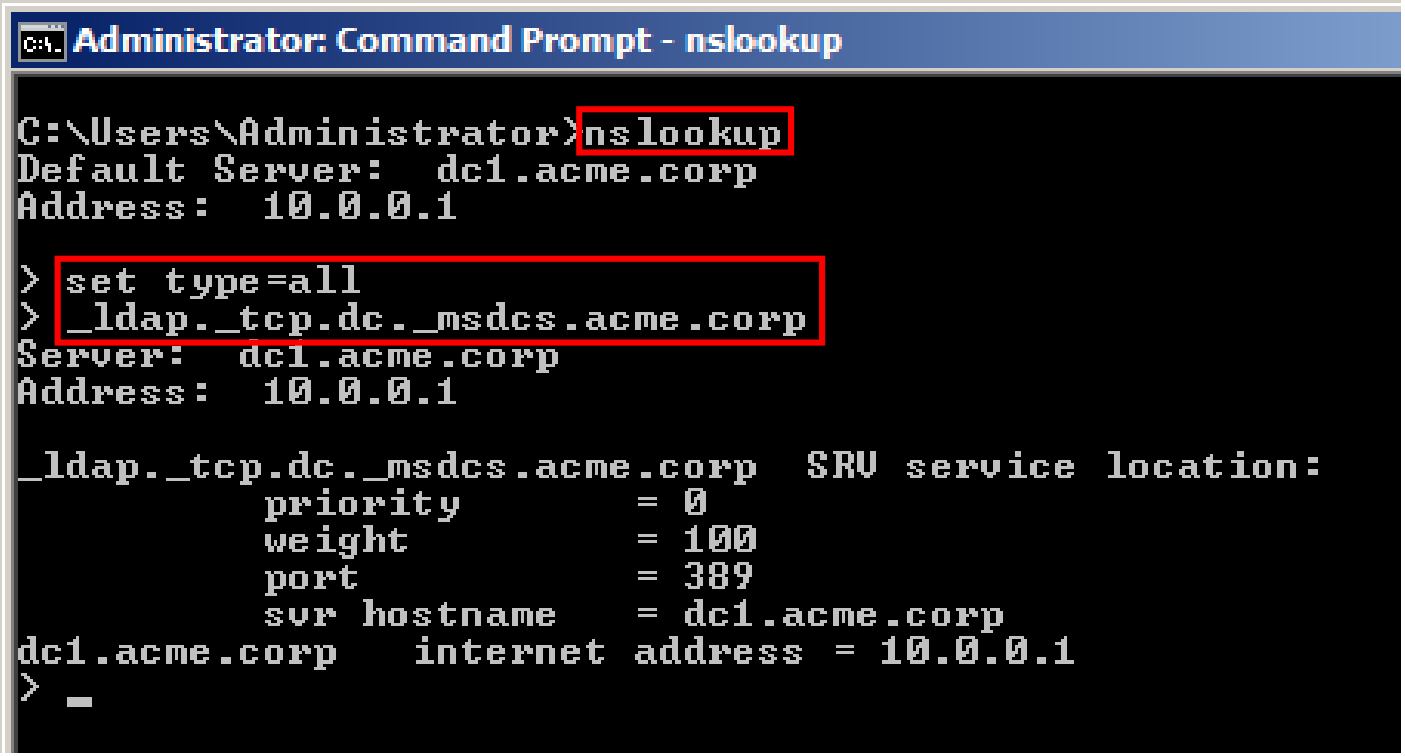
Para que a estação de trabalho possa encontrar o controlador de domínio da rede quando o usuário insere suas credencias, a estação faz uma consulta ao servidor DNS.

O Active Directory é dependente do serviço de DNS, pois sem ele a estação de trabalho não tem como encontrar o controlador de domínio responsável por autenticar aquele usuário.



Active Directory – consulta DNS

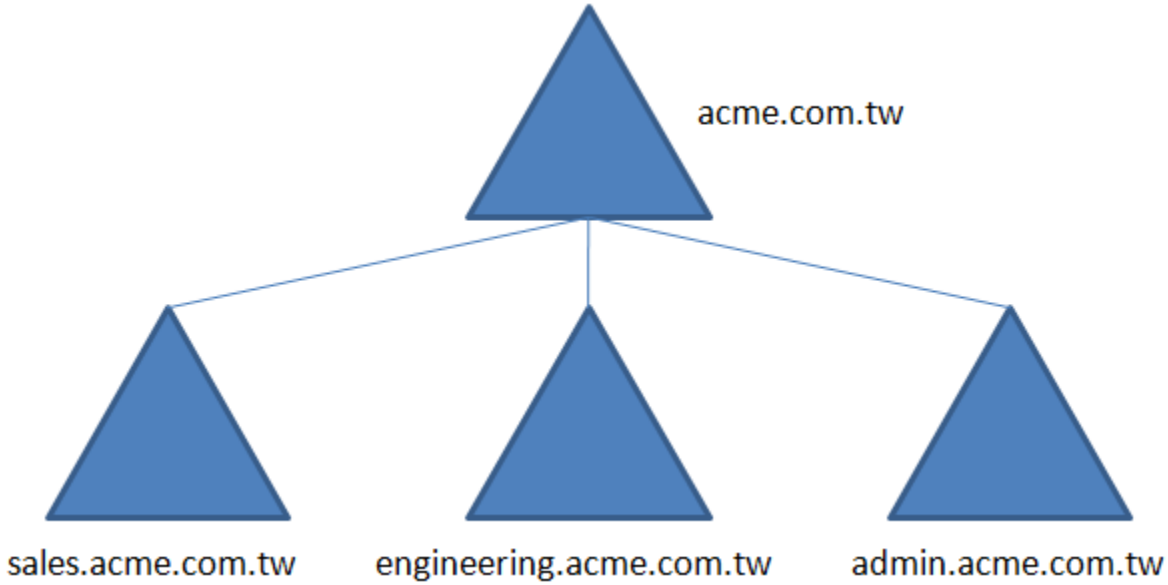
Para consultar o controlador de domínio que atende uma determinada rede, neste exemplo a rede ACME.CORP, pode-se usar o comando `nslookup`:



Active Directory – árvore

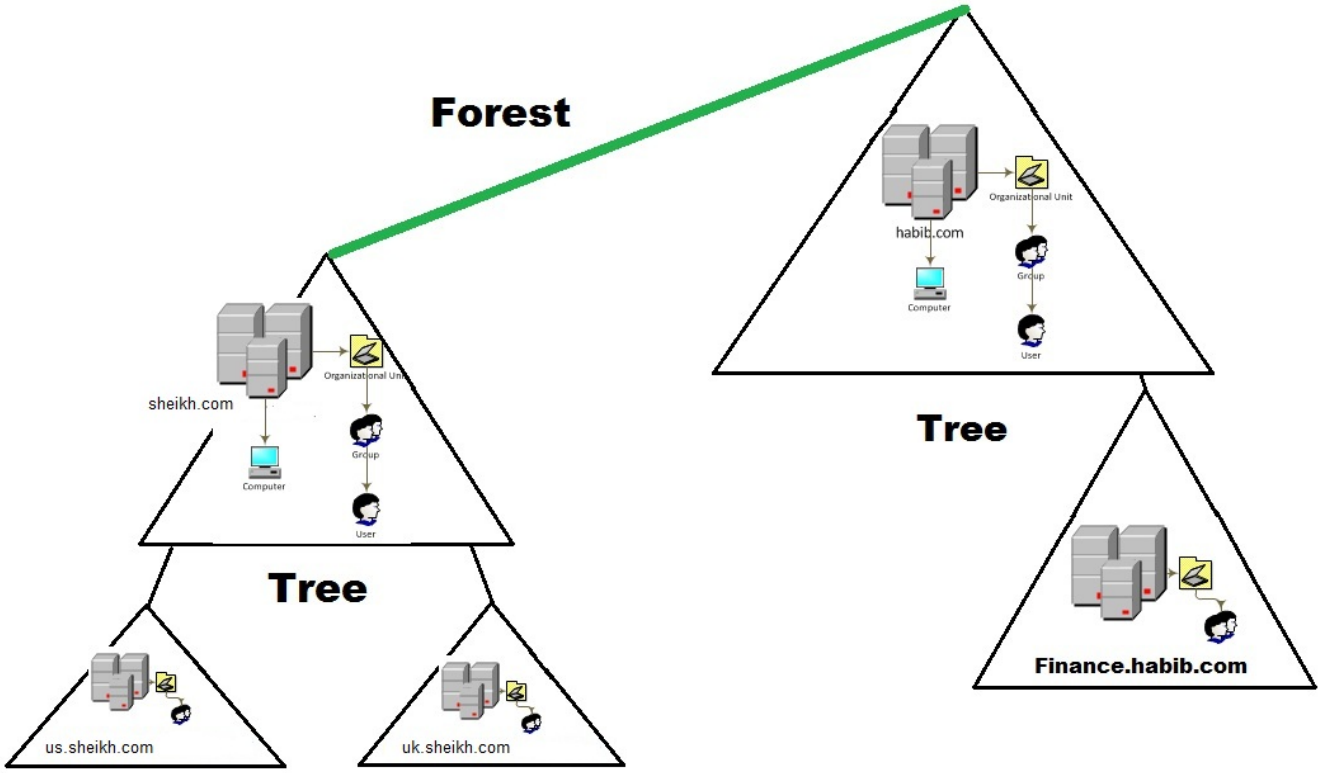
Várias unidades administrativas, ou domínios, podem ser combinados desde que compartilhem o mesmo espaço de nomes, de modo que tenhamos um domínio pai ou raiz e domínios filhos ou subdomínios. A este conjunto de domínios dá-se o nome de Árvore.

No exemplo abaixo, os domínios sales, engineering e admin são subdomínios do domínio raiz acme.com.tw.



Active Directory – floresta

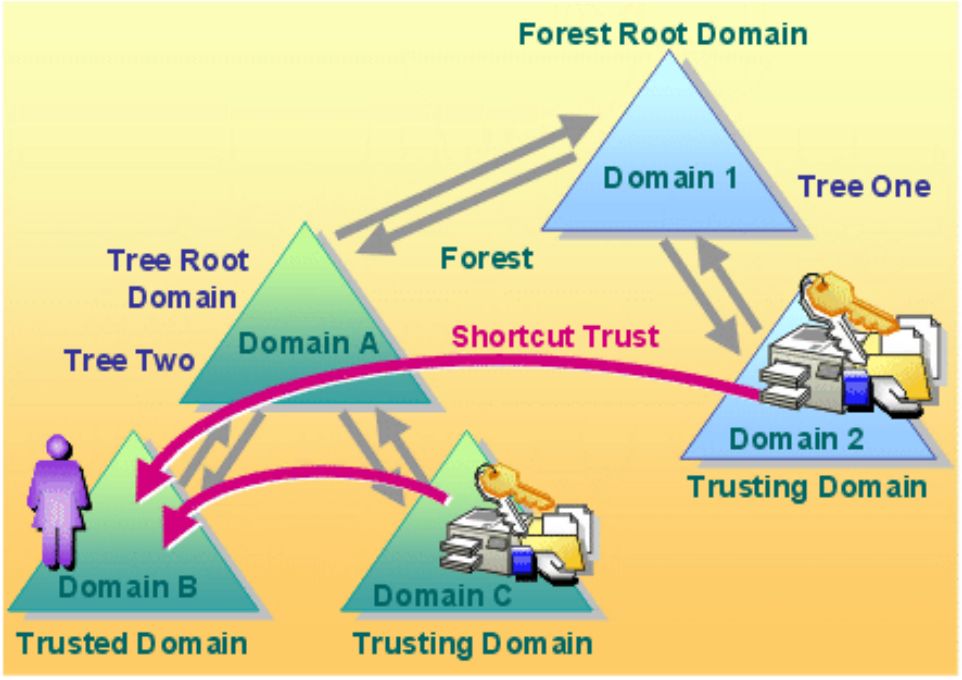
Unidades administrativas ou domínios, que não compartilham o mesmo espaço de nomes, também podem ser combinados. Neste caso teremos uma Floresta.



Active Directory – trust

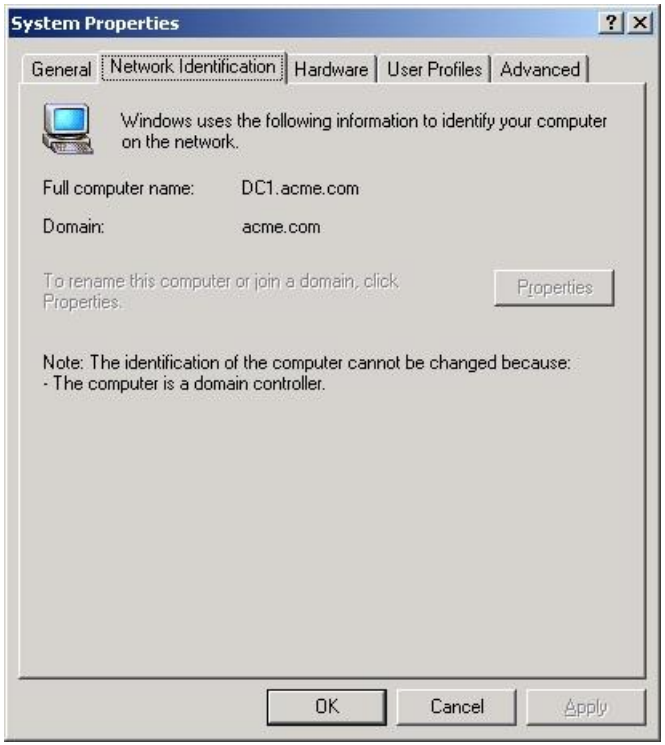
O trust ou relação de confiança é um canal de autenticação que permite que usuários de um domínio possam acessar recursos em outro domínio.

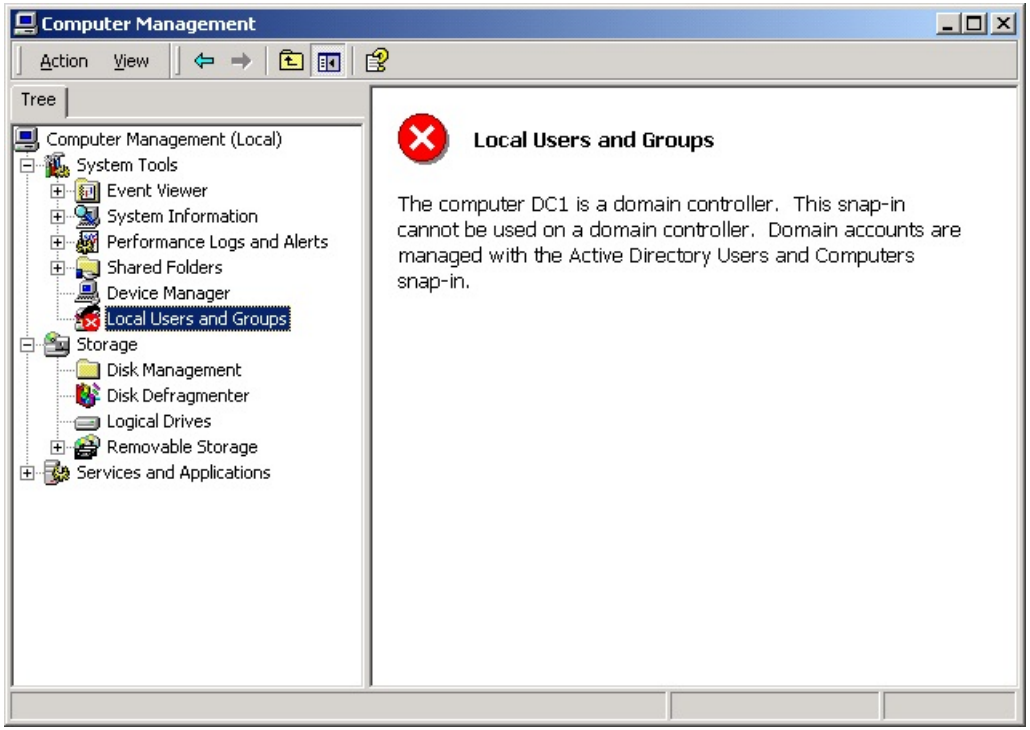
Pode ser do tipo direta, quando um domínio é subdomínio de outro; ou transitiva, quando dois domínios são subdomínios de uma mesma raiz.



Active Directory – exemplo

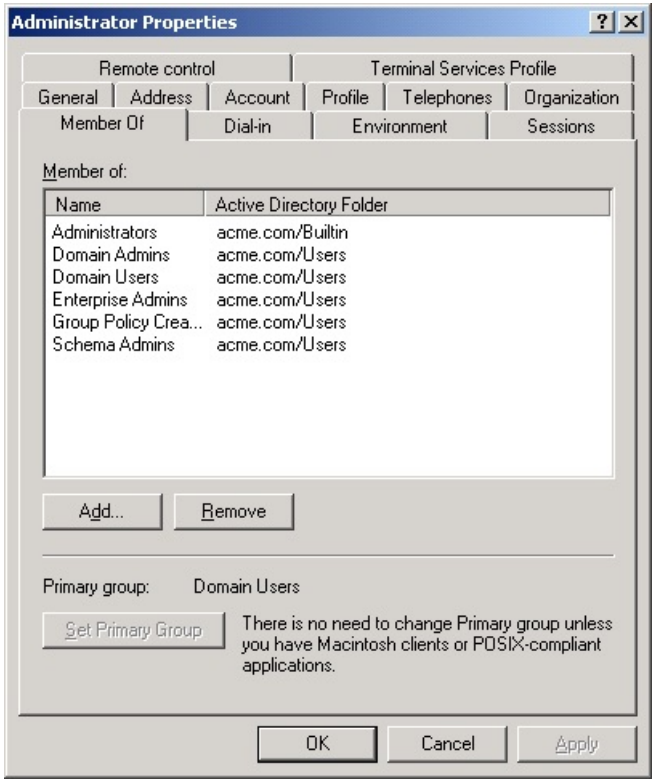
Todo controlador de domínio tem seus usuários locais e grupos desabilitados, pois as contas de usuário passam a ser administradas pelo Active Directory.





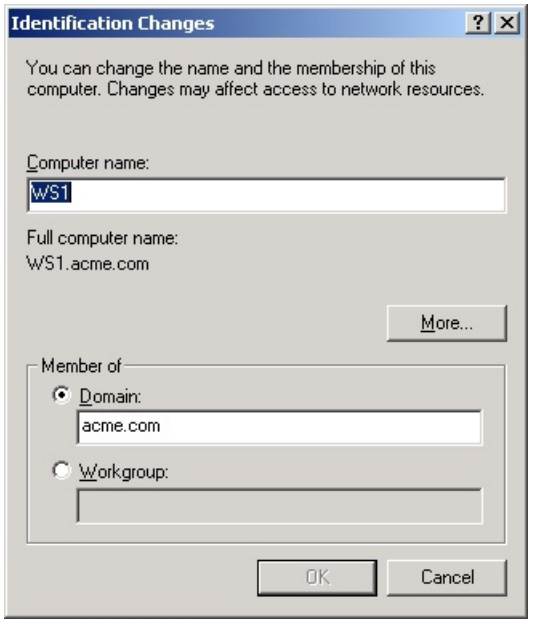
Active Directory – exemplo

Todo novo usuário criado no domínio passa a pertencer a um grupo de domínio.



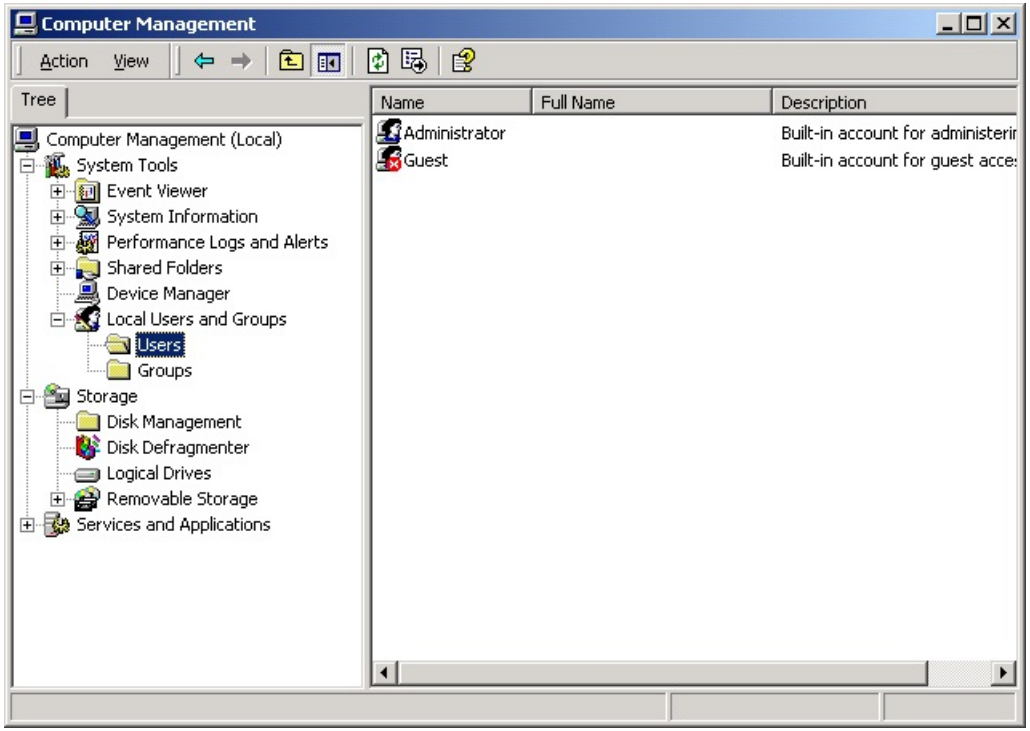
Active Directory – exemplo

Toda estação de trabalho passa a ter a possibilidade de fazer parte de uma rede apartada (workgroup) ou do domínio, a partir de onde poderá compartilhar as configurações de segurança com as outras estações e servidores da rede.



Active Directory – exemplo

Mesmo fazendo parte do domínio, as estações de trabalho continuam a ter seus usuários locais e grupos habilitados, abrindo a possibilidade de se poder usar contas de usuários locais ou de domínio.



Para saber mais...

… leia o documento sobre Arquitetura do Active Directory, da Microsoft.

Módulo 10

Análise e Avaliação de Riscos

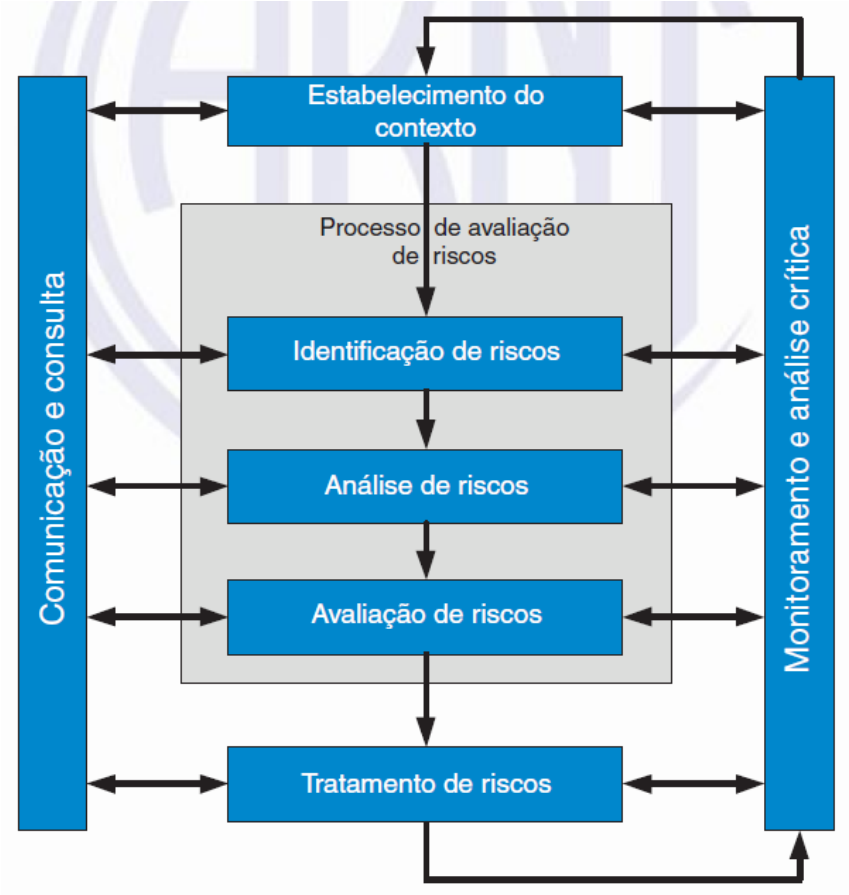
Análise e avaliação de riscos

As análises/avaliações de riscos devem:

- Identificar, quantificar e priorizar os riscos com base em critérios para aceitação dos mesmos, para orientar e determinar as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos de segurança da informação;
- Incluir um enfoque sistemático para estimar a magnitude do risco (análise de riscos) e o processo de comparar os riscos estimados contra os critérios de risco para determinar a significância do risco (avaliação do risco);
- Ser realizadas periodicamente para contemplar as mudanças nos requisitos de segurança da informação e na situação de risco. Essas análises/avaliações de riscos devem ser realizadas de forma metódica, capaz de gerar resultados comparáveis e reproduzíveis.
- Ter um escopo claramente definido para ser eficaz e incluir os relacionamentos com as análises/avaliações de riscos em outras áreas, se necessário.

Fonte: NBR ISO/IEC 27002:2005

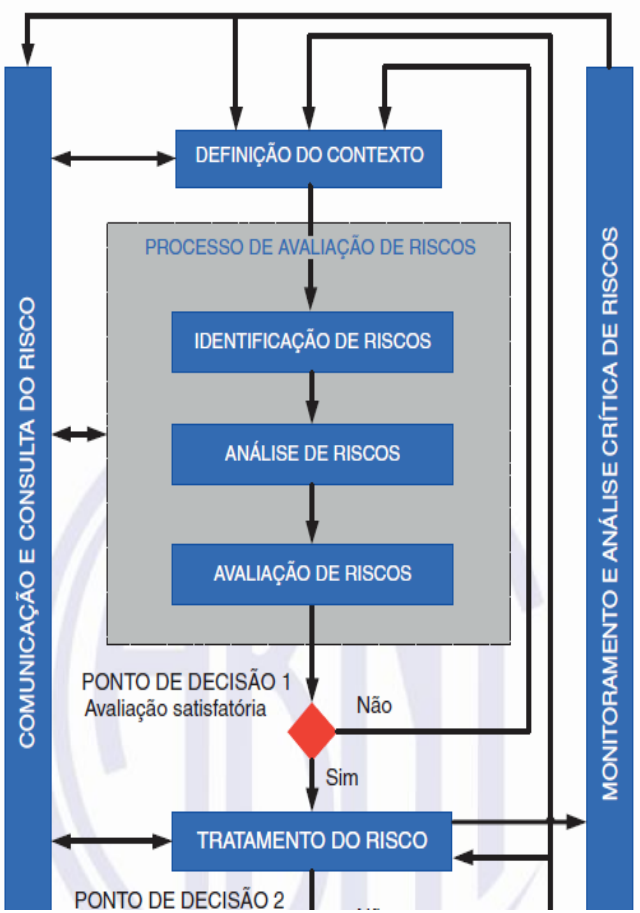
ISO/IEC 27005 – gestão de riscos



Processo de Gestão de Riscos

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – gestão de riscos



Processo de Gestão de Riscos Iterativo

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – gestão de riscos

Processo do SGSI	Processo de gestão de riscos de segurança da informação
Planejar	Definição do contexto Processo de avaliação de riscos Definição do plano de tratamento do risco Aceitação do risco
Executar	Implementação do plano de tratamento do risco
Verificar	Monitoramento contínuo e análise crítica de riscos
Agir	Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação

Alinhamento do processo do SGSI e do processo de Gestão de Riscos

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – definição do contexto

O contexto externo e interno para gestão de riscos de segurança da informação deve ser estabelecido, o que envolve a definição dos critérios básicos necessários para a gestão de riscos, a definição do escopo e dos limites e o estabelecimento de uma organização apropriada para operar a gestão de riscos.

É essencial determinar o propósito da gestão de riscos de segurança da informação, pois ele afeta o processo em geral e a definição do contexto em particular. Esse propósito pode ser:

- Suporte a um SGSI;
- Conformidade legal;
- Preparação de um plano de continuidade de negócios;
- Preparação de um plano de resposta a incidentes;
- Descrição dos requisitos de segurança da informação para um produto, um serviço ou um mecanismo.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – critérios básicos

Abordagem da gestão de riscos

- Executar o processo de avaliação de riscos e estabelecer um plano de tratamento de riscos;
- Definir e implementar políticas e procedimentos, incluindo implementação dos controles selecionados;
- Monitorar controles;
- Monitorar o processo de gestão de riscos de segurança da informação.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – critérios básicos

Critérios para avaliação de riscos

- O valor estratégico do processo que trata as informações de negócio;
- A criticidade dos ativos de informação envolvidos;
- Requisitos legais e regulatórios, bem como as obrigações contratuais;
- Importância, do ponto de vista operacional e dos negócios, da disponibilidade, da confidencialidade e da integridade;
- Expectativas e percepções das partes interessadas e consequências negativas para o valor de mercado (em especial, no que se refere aos fatores intangíveis desse valor), a imagem e a reputação.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – critérios básicos

Critérios de impacto

- Nível de classificação do ativo de informação afetado;
- Ocorrências de violação da segurança da informação (por exemplo, perda da disponibilidade, da confidencialidade e/ou da integridade);
- Operações comprometidas (internas ou de terceiros);
- Perda de oportunidades de negócio e de valor financeiro;
- Interrupção de planos e o não cumprimento de prazos;
- Dano à reputação;
- Violações de requisitos legais, regulatórios ou contratuais.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – critérios básicos

Critérios para aceitação de riscos

- Critérios para a aceitação do risco podem incluir mais de um limite, representando um nível desejável de risco, porém precauções podem ser tomadas por gestores seniores para aceitar riscos acima desse nível desde que sob circunstâncias definidas;
- Critérios para a aceitação do risco podem ser expressos como a razão entre o lucro estimado (ou outro benefício ao negócio) e o risco estimado
- Diferentes critérios para a aceitação do risco podem ser aplicados a diferentes classes de risco, por exemplo, riscos que podem resultar em não conformidade com regulamentações ou leis podem não ser aceitos, enquanto riscos de alto impacto podem ser aceitos se isto for especificado como um requisito contratual;
- Critérios para a aceitação do risco podem incluir requisitos para um tratamento adicional futuro, por exemplo, um risco pode ser aceito se for aprovado e houver o compromisso de que ações para reduzi-lo a um nível aceitável serão tomadas dentro de um determinado período de tempo.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – processo de avaliação de riscos

Descrição geral do processo de avaliação de riscos de segurança da informação

O processo de avaliação de riscos determina o valor dos ativos de informação, identifica as ameaças e vulnerabilidades aplicáveis existentes (ou que poderiam existir), identifica os controles existentes e seus efeitos no risco identificado, determina as consequências possíveis e, finalmente, prioriza os riscos derivados e ordena-os de acordo com os critérios de avaliação de riscos estabelecidos na definição do contexto.

O processo de avaliação de riscos consiste nas seguintes atividades:

- Identificação de riscos;
- Análise de riscos;
- Avaliação de riscos.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – processo de avaliação de riscos

Identificação de riscos

O propósito da identificação de riscos é determinar eventos que possam causar uma perda potencial e deixar claro como, onde e por que a perda pode acontecer.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – processo de avaliação de riscos

Ativos

Um ativo é algo que tem valor para a organização e que, portanto, requer proteção. Para a identificação dos ativos convém que se tenha em mente que um sistema de informação compreende mais do que *hardware* e *software*.

De acordo com a ISO/IEC 27002:2005, ativos podem ser de vários tipos, incluindo:

- ativos de informação: base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;
- ativos de software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;
- ativos físicos: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;
- serviços: serviços de computação e comunicações, utilidades gerais, por exemplo aquecimento, iluminação, eletricidade e refrigeração;
- pessoas e suas qualificações, habilidades e experiências;
- intangíveis, tais como a reputação e a imagem da organização.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – processo de avaliação de riscos

Ameaças

Uma ameaça tem o potencial de comprometer ativos (como informações, processos e sistemas) e, por isso, também as organizações. Ameaças podem ser de origem natural ou humana e podem ser acidentais ou intencionais. Convém que tanto as fontes das ameaças acidentais quanto as das intencionais, sejam identificadas. Uma ameaça pode surgir de dentro ou de fora da organização.

Vulnerabilidades

A presença de uma vulnerabilidade não causa prejuízo por si só, pois precisa haver uma ameaça presente para explorá-la. Uma vulnerabilidade que não tem uma ameaça correspondente pode não requerer a implementação de um controle no presente momento, mas convém que ela seja reconhecida como tal e monitorada, no caso de haver mudanças.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – processo de avaliação de riscos

CONTROLE

ISO/IEC 27005 – processo de avaliação de riscos

Identificação das vulnerabilidades

Vulnerabilidades podem ser identificadas nas seguintes áreas:

- Organização;
- Processos e procedimentos;
- Rotinas de gestão;
- Recursos humanos;
- Ambiente físico;
- Configuração do sistema de informação;
- *Hardware*, *software* ou equipamentos de comunicação;
- Dependência de entidades externas.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – processo de avaliação de riscos

Identificação das consequências

As organizações devem identificar as consequências operacionais de cenários de incidentes em função de (mas não limitado a):

- Investigação e tempo de reparo;
- Tempo (de trabalho) perdido;
- Oportunidade perdida;
- Saúde e segurança;
- Custo financeiro das competências específicas necessárias para reparar o prejuízo;
- Imagem, reputação e valor de mercado.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – análise de riscos

Análise qualitativa

A análise qualitativa de riscos utiliza uma escala com atributos qualificadores que descrevem a magnitude das consequências potenciais (por exemplo, pequena, média e grande) e a probabilidade dessas consequências ocorrerem. Uma vantagem da análise qualitativa é sua facilidade de compreensão por todas as pessoas envolvidas, enquanto que uma desvantagem é a dependência da escolha subjetiva da escala.

Essas escalas podem ser adaptadas ou ajustadas para se adequarem às circunstâncias, e descrições diferentes podem ser usadas para riscos diferentes. A análise qualitativa pode ser utilizada:

- Como uma verificação inicial a fim de identificar riscos que exigem uma análise mais detalhada;
- Quando esse tipo de análise é suficiente para a tomada de decisões;
- Quando os dados numéricos ou recursos são insuficientes para uma análise quantitativa.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – análise de riscos

Análise quantitativa

A análise quantitativa utiliza uma escala com valores numéricos (e não as escalas descritivas usadas na análise qualitativa) tanto para as consequências quanto para a probabilidade, usando dados de diversas fontes. A qualidade da análise depende da exatidão e da integralidade dos valores numéricos e da validade dos modelos utilizados. A análise quantitativa, na maioria dos casos, utiliza dados históricos dos incidentes, proporcionando a vantagem de poder ser relacionada diretamente aos objetivos da segurança da informação e interesses da organização. Uma desvantagem é a falta de tais dados sobre novos riscos ou sobre fragilidades da segurança da informação. Uma desvantagem da abordagem quantitativa ocorre quando dados factuais e auditáveis não estão disponíveis. Nesse caso, a exatidão do processo de avaliação de riscos e os valores associados tornam-se ilusórios.

A forma na qual as consequências e a probabilidade são expressas e a forma em que elas são combinadas para fornecer um nível de risco irão variar de acordo com o tipo de risco e do propósito para o qual os resultados do processo de avaliação de riscos serão usados. Convém que a incerteza e a variabilidade tanto das consequências, quanto da probabilidade, sejam consideradas na análise e comunicadas de forma eficaz.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – análise de riscos

Avaliação das consequências

O valor do impacto ao negócio pode ser expresso de forma qualitativa ou quantitativa, porém um método para designar valores monetários geralmente pode fornecer mais informações úteis para a tomada de decisões e, consequentemente, permitir que o processo de tomada de decisão seja mais eficiente.

A valoração dos ativos começa com a sua classificação de acordo com a criticidade, em função da importância dos ativos para a realização dos objetivos de negócios da organização. A valoração é então determinada de duas maneiras:

- o valor de reposição do ativo: o custo da recuperação e da reposição da informação (se for possível), e
- as consequências ao negócio relacionadas à perda ou ao comprometimento do ativo, como as possíveis consequências adversas de caráter empresarial, legal ou regulatórias causadas pela divulgação indevida, modificação, indisponibilidade e/ou destruição de informações ou de outros ativos de informação.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – análise de riscos

Avaliação da probabilidade dos incidentes

Depois de identificar os cenários de incidentes, é necessário avaliar a probabilidade de cada cenário e do impacto correspondente, usando técnicas de análise qualitativas ou quantitativas.

- a experiência passada e estatísticas aplicáveis referentes à probabilidade da ameaça;
- para fontes de ameaças intencionais: a motivação e as competências, que mudam ao longo do tempo, os recursos disponíveis para possíveis atacantes, bem como a percepção da vulnerabilidade e o poder da atração dos ativos para um possível atacante;
- para fontes de ameaças acidentais: fatores geográficos (como por exemplo, proximidade a fábricas e refinarias de produtos químicos e petróleo), a possibilidade de eventos climáticos extremos e fatores que poderiam acarretar erros humanos e o mau funcionamento de equipamentos;
- vulnerabilidades, tanto individualmente como em conjunto;
- os controles existentes e a eficácia com que eles reduzem as vulnerabilidades.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – análise de riscos

Determinação do nível de risco

A análise de riscos designa valores para a probabilidade e para as consequências de um risco. Esses valores podem ser de natureza quantitativa ou qualitativa. A análise de riscos é baseada nas consequências e na probabilidade estimadas. Além disso, ela pode considerar o custo-benefício, as preocupações das partes interessadas e outras variáveis, conforme apropriado para a avaliação de riscos. O risco estimado é uma combinação da probabilidade de um cenário de incidente e suas consequências.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – análise de riscos

Exemplo – Matriz com valores pré-definidos

Para cada ativo, as vulnerabilidades relevantes e respectivas ameaças são consideradas. Se houver uma vulnerabilidade sem uma ameaça correspondente, ou uma ameaça sem uma vulnerabilidade correspondente, então não há risco nesse momento (mas convém que cuidados sejam tomados no caso dessas situações mudarem).

	Probabilidade de ocorrência (Ameaça)	BAIXA			MÉDIA			ALTA		
	Facilidade de exploração (Vulnerabilidade)	B	M	A	B	M	A	B	M	A
VALOR DO ATIVO	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

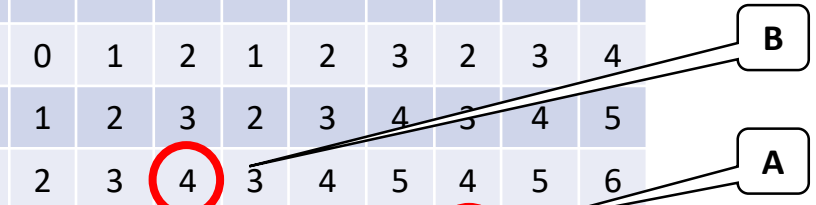
Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – análise de riscos

Exemplo – Matriz com valores pré-definidos

Por exemplo, se o ativo tiver o valor **3**, a ameaça é "**alta**" e a vulnerabilidade é "**baixa**", a medida do risco é **5** (**A**). Supondo que um ativo tenha o valor **2**, o nível de ameaça é "**baixo**" e a facilidade de exploração é "**alta**", logo, a medida de risco é **4** (**B**).

	Probabilidade de ocorrência (Ameaça)	BAIXA			MÉDIA			ALTA		
	Facilidade de exploração (Vulnerabilidade)	B	M	A	B	M	A	B	M	A
VALOR DO ATIVO	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8



Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – avaliação de riscos

A natureza das decisões relativas à avaliação de riscos e os critérios de avaliação de riscos que irão ser usados para tomar essas decisões teriam sido decididos durante a definição do contexto. Convém que essas decisões e o contexto sejam revisados detalhadamente nesse estágio em que se conhece mais sobre os riscos identificados. Para avaliar os riscos, convém que as organizações comparem os riscos estimados com os critérios de avaliação de riscos definidos durante a definição do contexto.

Convém que os critérios de avaliação de riscos utilizados na tomada de decisões sejam consistentes com o contexto definido, externo e interno, relativo à gestão de riscos de segurança da informação e levem em conta os objetivos da organização, o ponto de vista das partes interessadas etc. As decisões tomadas durante a atividade de avaliação de riscos são baseadas principalmente no nível de risco aceitável. No entanto, convém que as consequências, a probabilidade e o grau de confiança na identificação e análise de riscos também sejam considerados. A agregação de vários pequenos ou médios riscos pode resultar em um risco total bem mais significativo e precisa ser tratada adequadamente.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – avaliação de riscos

Convém que os seguintes itens sejam considerados:

- Propriedades da segurança da informação: se um critério não for relevante para a organização (por exemplo, a perda da confidencialidade), logo todos os riscos que provocam esse tipo de impacto podem ser considerados irrelevantes;
- Importância do processo de negócios ou da atividade suportada por um determinado ativo ou conjunto de ativos: se o processo for considerado de baixa importância, convém que os riscos associados a ele sejam menos considerados do que os riscos que causam impactos em processos ou atividades mais importantes.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – avaliação de riscos

A avaliação de riscos usa o entendimento do risco obtido através da análise de riscos para a tomada de decisões sobre ações futuras. Convém que as decisões incluam:

- Se convém que uma atividade seja empreendida;
- As prioridades para o tratamento do risco, levando-se em conta os níveis estimados de risco.

Durante a etapa de avaliação de riscos, além dos riscos estimados, convém que requisitos contratuais, legais e regulatórios também sejam considerados.

Fonte: NBR ISO/IEC 27005:2011

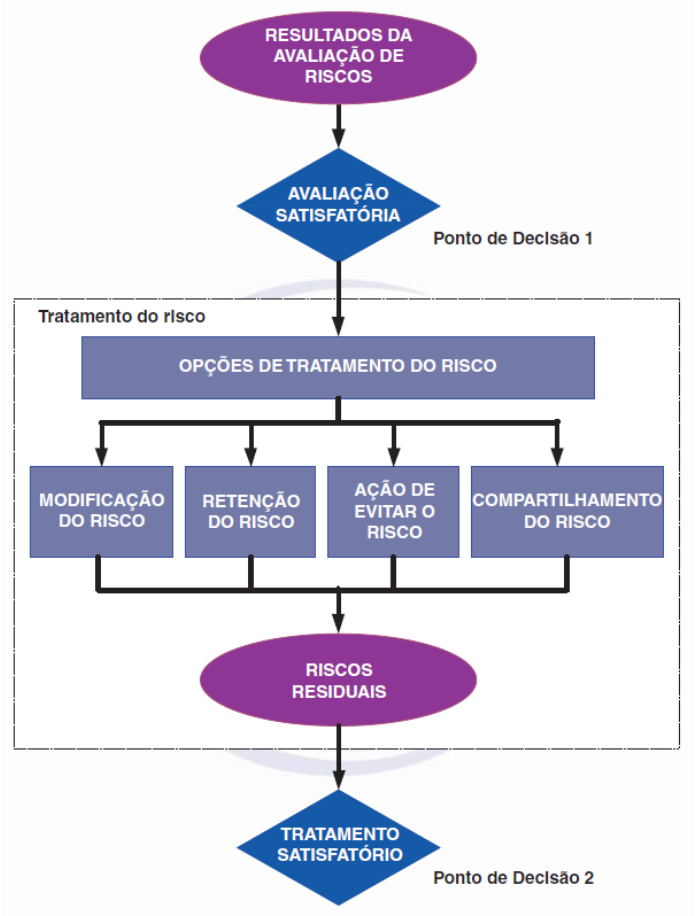
ISO/IEC 27005 – tratamento dos riscos

As opções de tratamento dos riscos devem ser selecionadas com base no resultado do processo de avaliação de riscos, no custo esperado para implementação dessas opções e nos benefícios previstos.

Quando uma grande modificação do risco pode ser obtida com uma despesa relativamente pequena, convém que essas opções sejam implementadas. Outras opções para melhorias podem ser muito dispendiosas e uma análise precisa ser feita para verificar suas justificativas.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – tratamento dos riscos



Atividade de Tratamento de Risco

Fonte: NBR ISO/IEC 27005:2011

Resposta aos riscos

Evitar, prevenir ou eliminar	• Elimina a causa raiz do problema a fim de evitar a exposição ao risco. Pode afetar a utilidade do ativo.
Transferir	• Não trata o risco, apenas transfere o ônus para um terceiro, de modo parcial ou total, como num seguro. Há a necessidade de se pagar um prêmio para a parte que assume o risco.
Mitigar	• Reduz a probabilidade de ocorrência de um incidente ou o seu impacto até um nível aceitável.
Aceitar	• Quando a probabilidade de ocorrência e o impacto são baixos ou quando não é possível aplicar nenhuma estratégia e decide-se arcar com as consequências.

Resposta aos riscos *vs* tratamento dos riscos

Evitar, prevenir ou eliminar	• Ação de evitar o risco
Transferir	• Compartilhamento do risco
Mitigar	• Modificação do risco
Aceitar	• Retenção do risco

Para saber mais...

...

Módulo 11

Plano de Continuidade do Negócio

Introdução

Continuidade do Negócio, ou Business Continuity, é o processo que prepara para uma paralisação do sistema que pode afetar de modo adverso as operações de negócios, responde a essa paralisação e recupera as operações.

- O processo de Continuidade do Negócio permite a disponibilidade contínua das informações e dos serviços em caso de não atendimento do SLA requerido;
- Continuidade do Negócio envolve várias contramedidas proativas e reativas;
- É importante automatizar o processo de Continuidade do Negócio para reduzir a intervenção manual;
- O objetivo da Continuidade do Negócio é garantir a disponibilidade das informações.

Fonte: EMC Information Storage and Management v3

Plano

O Plano de Continuidade de Negócios, ou Business Continuity Plan, é o desenvolvimento preventivo de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre, e até o retorno à situação normal de funcionamento da empresa dentro do contexto do negócio do qual faz parte.

O Plano de Continuidade de Negócios é constituído pelos seguintes planos:

- Plano de Contingência (Emergência);
- Plano de Administração de Crises (PAC);
- Plano de Recuperação de Desastres (PRD);
- Plano de Continuidade Operacional (PCO).

Fonte: NBR 15999-1:2007

Estrutura

Plano de Contingência (Emergência): deve ser utilizado em último caso, quando todas as prevenções tiverem falhado. Define as necessidades e ações mais imediatas.

Plano de Administração ou Gerenciamento de Crises (PAC): define funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência, antes durante e após a ocorrência.

Plano de Recuperação de Desastres (PRD): determina o planejamento para que, uma vez controlada a contingência e passada a crise, a empresa retome seus níveis originais de operação.

Plano de Continuidade Operacional (PCO): seu objetivo é reestabelecer o funcionamento dos principais ativos que suportam as operações de uma empresa, reduzindo o tempo de queda e os impactos provocados por um eventual incidente. Um exemplo simples é a queda de conexão à internet.

Fonte: www.venki.com.br

Disponibilidade das informações

Disponibilidade das informações é a capacidade de uma infraestrutura de TI funcionar de acordo com os requisitos dos negócios e com as expectativas do cliente durante seu tempo de operação especificado, e pode ser definida em termos de:

Acessibilidade	• As informações devem estar acessíveis para o usuário certo quando necessário
Confiabilidade	• As informações devem ser confiáveis e corretas em todos os aspectos
Agilidade	• Define a janela de tempo durante a qual as informações devem estar acessíveis

Fonte: EMC Information Storage and Management v3

Causas da indisponibilidade

- Falha de aplicativo
  - Por exemplo, devido a exceções catastróficas causadas por uma lógica ruim
- Perda de dados
- Falha de componentes da infraestrutura
- Datacenter ou local inativo
  - Devido a falta de energia ou desastre
- Atualização da infraestrutura de TI

Fonte: EMC Information Storage and Management v3

Impacto da indisponibilidade das informações

Perda de produtividade

- Número de funcionários afetados x horas de inatividade x custo por hora

Saiba o custo do tempo de inatividade (por hora, dia, dois dias e assim por diante).

Receita perdida

- Perda direta
- Pagamentos compensatórios
- Perda de receita futura
- Perda de faturamento
- Perda de investimentos

Reputação prejudicada

- Clientes
- Fornecedores
- Mercados financeiros
- Bancos
- Parceiros de negócios

Desempenho financeiro

- Reconhecimento de receita
- Fluxo de caixa
- Perda de descontos
- Garantias de pagamentos
- Classificação de crédito
- Preços de ações

Outras despesas

- Funcionários temporários, locação de equipamentos, custos de horas extras, custos extras de remessas, despesas de viagens, etc.

Fonte: EMC Information Storage and Management v3

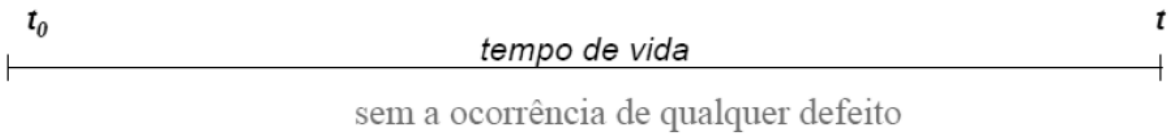
Confiabilidade e disponibilidade

Confiabilidade é a habilidade de um sistema ou equipamento exercer sua função sob uma determinada condição durante um período específico de tempo.

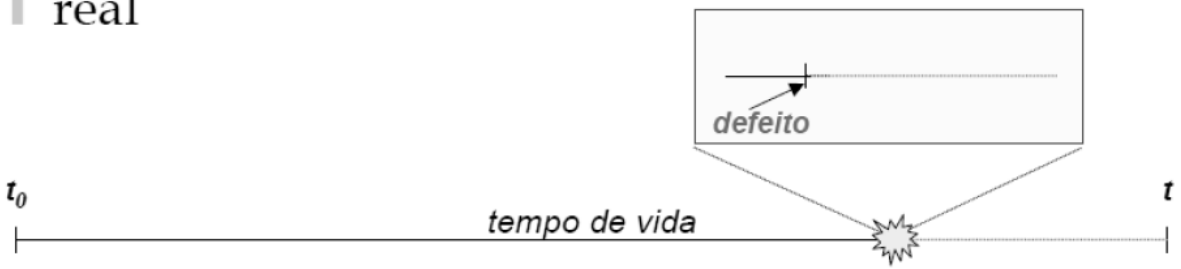
Disponibilidade é o quanto um sistema ou equipamento está operacional e acessível quando solicitado.

Falhas em equipamentos

- ideal



- real



Comportamento ideal e real de um componente

Falhas em equipamentos

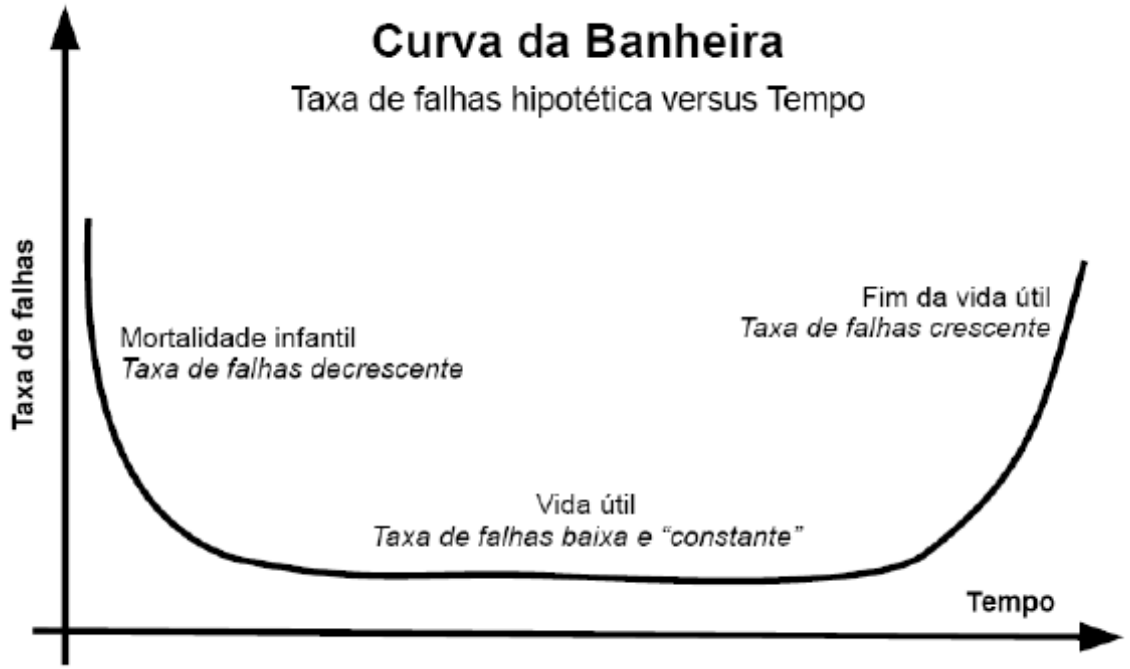
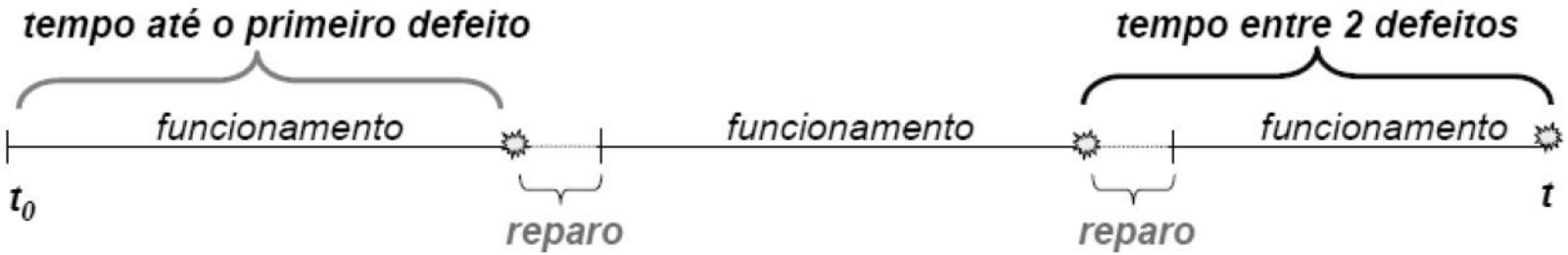


Gráfico da Curva da banheira

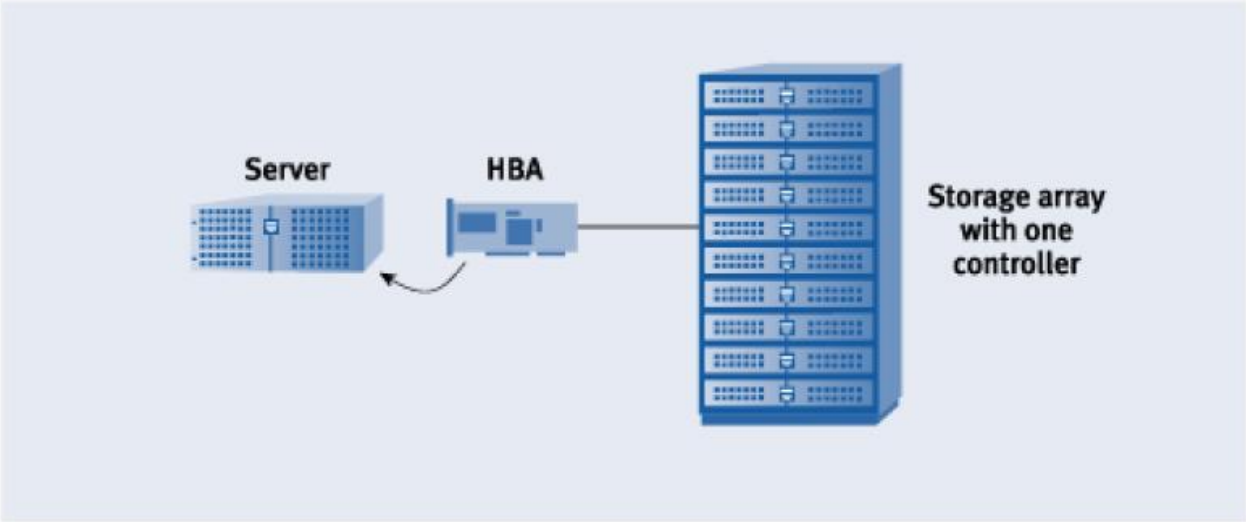
Medindo a disponibilidade

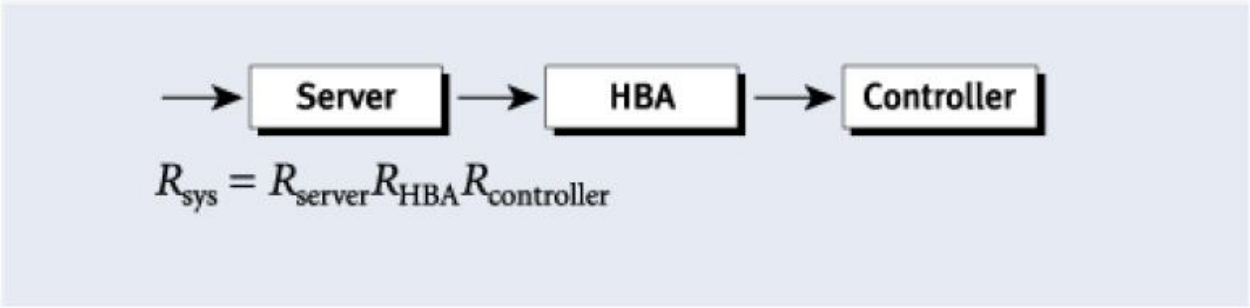
O tempo para ocorrer o primeiro defeito durante a vida útil de um equipamento ou produto é chamado de MTTF (*Mean Time to Failure*). O tempo de reparo (ou troca) deste equipamento é conhecido como MTTR (*Mean Time to Repair*), que inclui o tempo necessário para a notificação da falha, o tempo gasto com o deslocamento do técnico de campo, o tempo gasto com o transporte da nova peça do almoxarifado até o local de instalação e o tempo gasto no reparo ou troca propriamente dito. No MTTR devemos considerar também as paradas planejadas para manutenção. O intervalo entre as falhas do equipamento é chamado MTBF (*Mean Time Between Failures*).



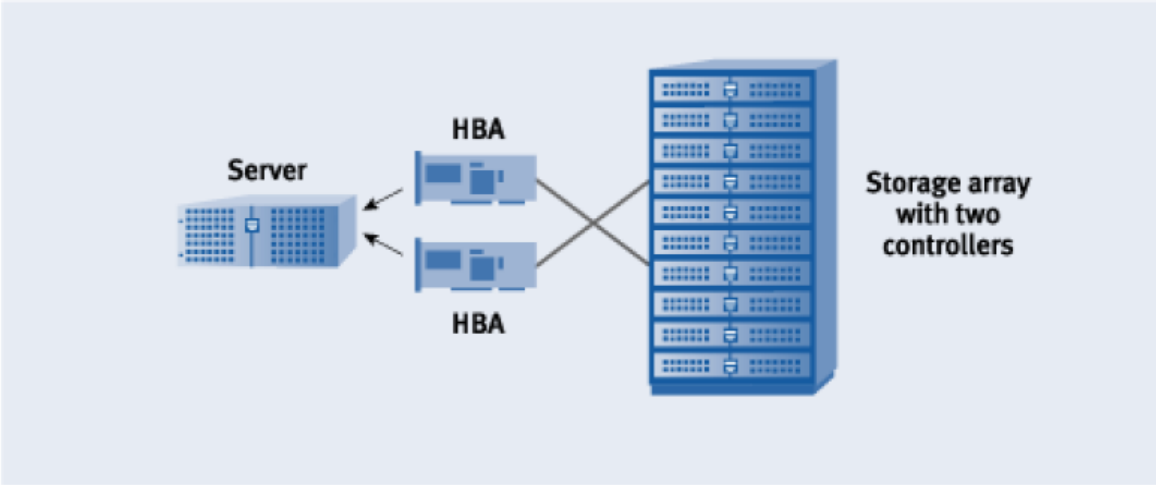
Linha do tempo para falhas de um equipamento

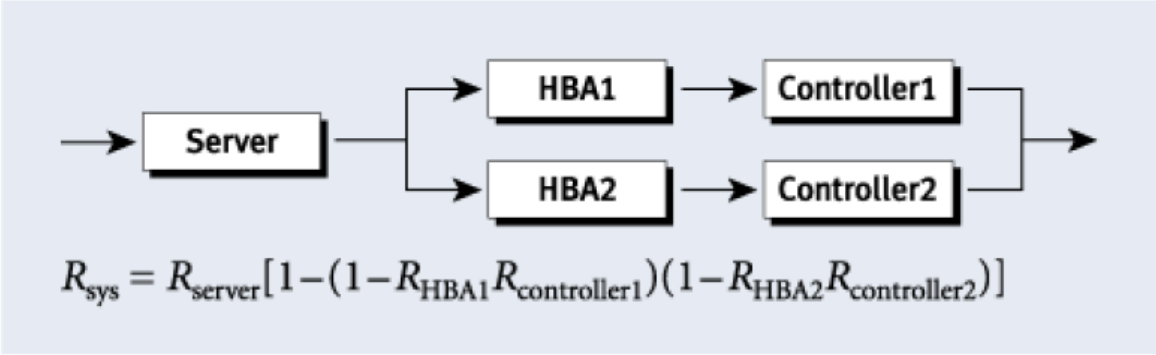
Associação de elementos em série





Associação de elementos em paralelo





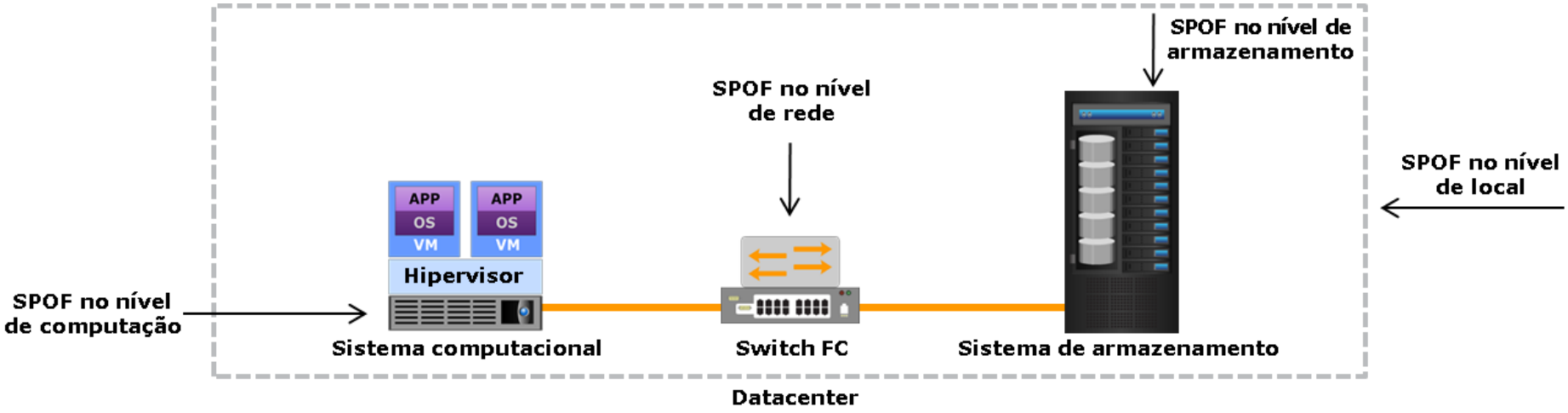
$$R_{sys} = R_{server}[1-(1-R_{HBA1}R_{controller1})(1-R_{HBA2}R_{controller2})]$$

Disponibilidades típicas

Disponibilidade	Tempo de parada
90%	36,5 dias/ano
99%	3,65 dias/ano
99,9%	8,76 horas/ano
99,99%	52 minutos/ano
99,999%	5 minutos/ano
99,9999%	31 segundos/ano

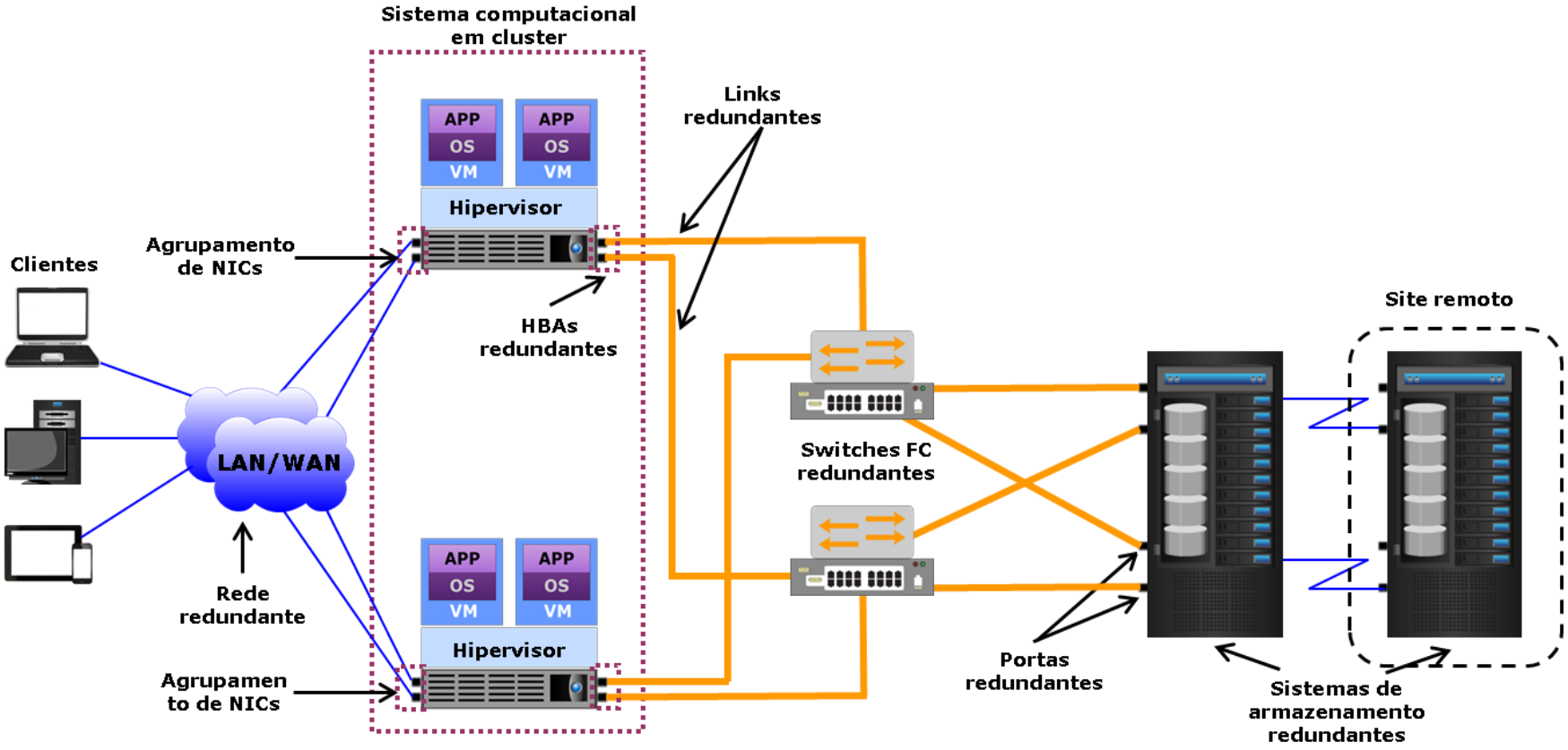
Ponto único de falha

Ponto único de falha, ou single point of failure (SPOF), refere-se a qualquer componente individual ou aspecto de uma infraestrutura cuja falha pode tornar todo o sistema ou serviço indisponível.



Fonte: EMC Information Storage and Management v3

Implementando redundância



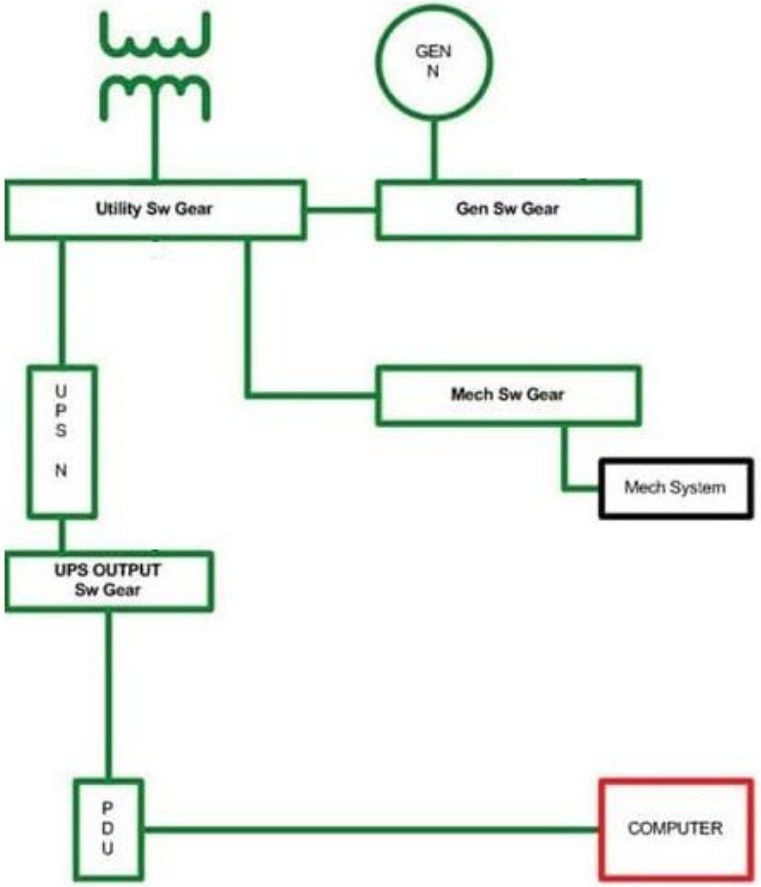
Fonte: EMC Information Storage and Management v3

Datacenter – Tier 1

- O mais simples dos quatro níveis para data centers
- Tempo de atividade de 99,671%
- Possui componentes de capacidade não redundantes, como uplink e servidores únicos
- Tem uma disponibilidade esperada de 99,671%
- Caminho de distribuição único não redundante que atende ao equipamento de TI
- 8 horas de inatividade por ano
- Tem um único caminho para energia e refrigeração para o equipamento do servidor
- Faltam os recursos vistos em data centers maiores, como um sistema de resfriamento de backup ou gerador

Fonte: Tier Classification Define Site Infrastructure Performance. W. Pitt Turner IV et al.

Datacenter – Tier 1



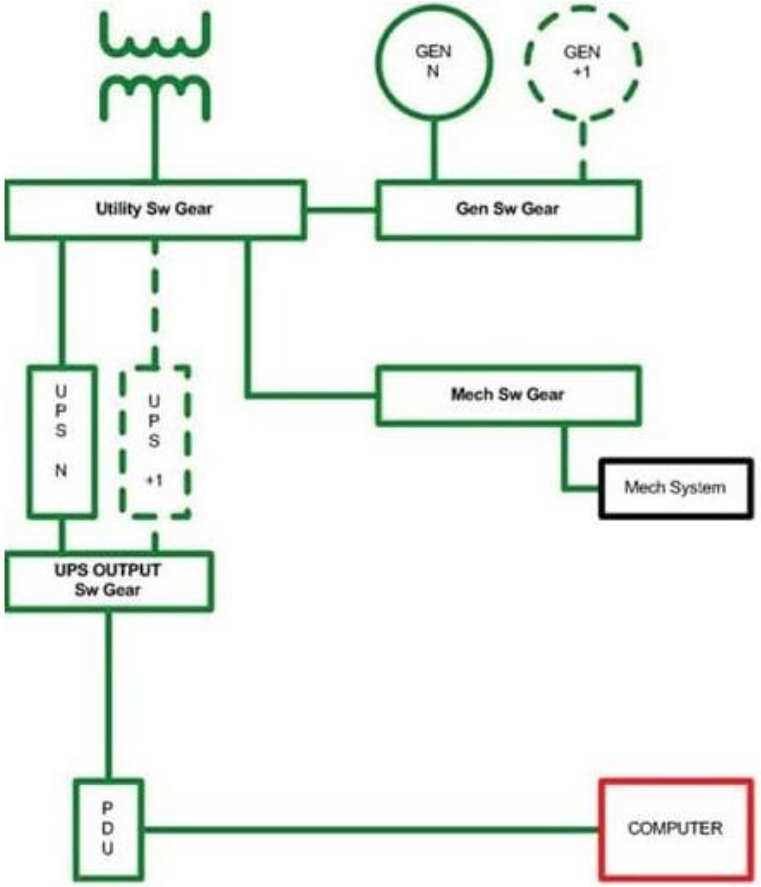
Fonte: Tier Classification Define Site Infrastructure Performance. W. Pitt Turner IV et al.

Datacenter – Tier 2

- 99,741% de tempo de atividade
- Redundância parcial em energia e refrigeração (capacidade de infraestrutura do site redundante)
- Equipamento de alimentação dupla e vários uplinks
- Experimente 22 horas de inatividade por ano
- Possui 12 horas de energia de backup no local
- Todas as fontes de alimentação redundantes podem ser removidas da instalação sem causar qualquer interrupção no equipamento de computação
- Só precisa de manutenção uma vez por ano

Fonte: Tier Classification Define Site Infrastructure Performance. W. Pitt Turner IV et al.

Datacenter – Tier 2



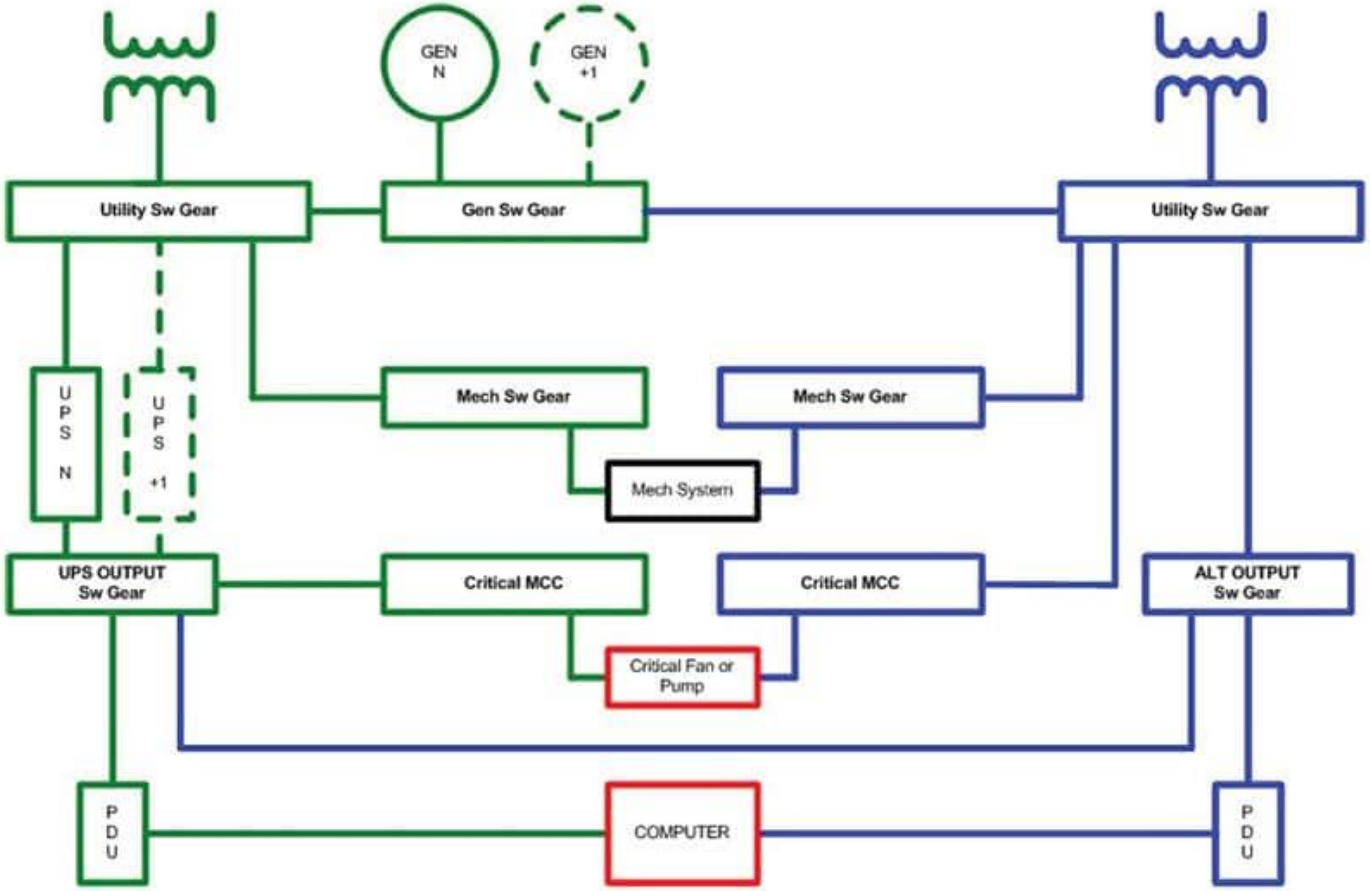
Fonte: Tier Classification Define Site Infrastructure Performance. W. Pitt Turner IV et al.

Datacenter – Tier 3

- Tempo de atividade de 99,982%
- Menos de 1,6 horas de tempo de inatividade anualmente
- Tolerante a N+1, fornecendo assim pelo menos 72 horas de proteção contra falta de energia
- O equipamento de computador é servido por um caminho de sinal de cada vez
- Todo o equipamento de TI é de alimentação dupla e totalmente compatível com a topologia da arquitetura de um site

Fonte: Tier Classification Define Site Infrastructure Performance. W. Pitt Turner IV et al.

Datacenter – Tier 3



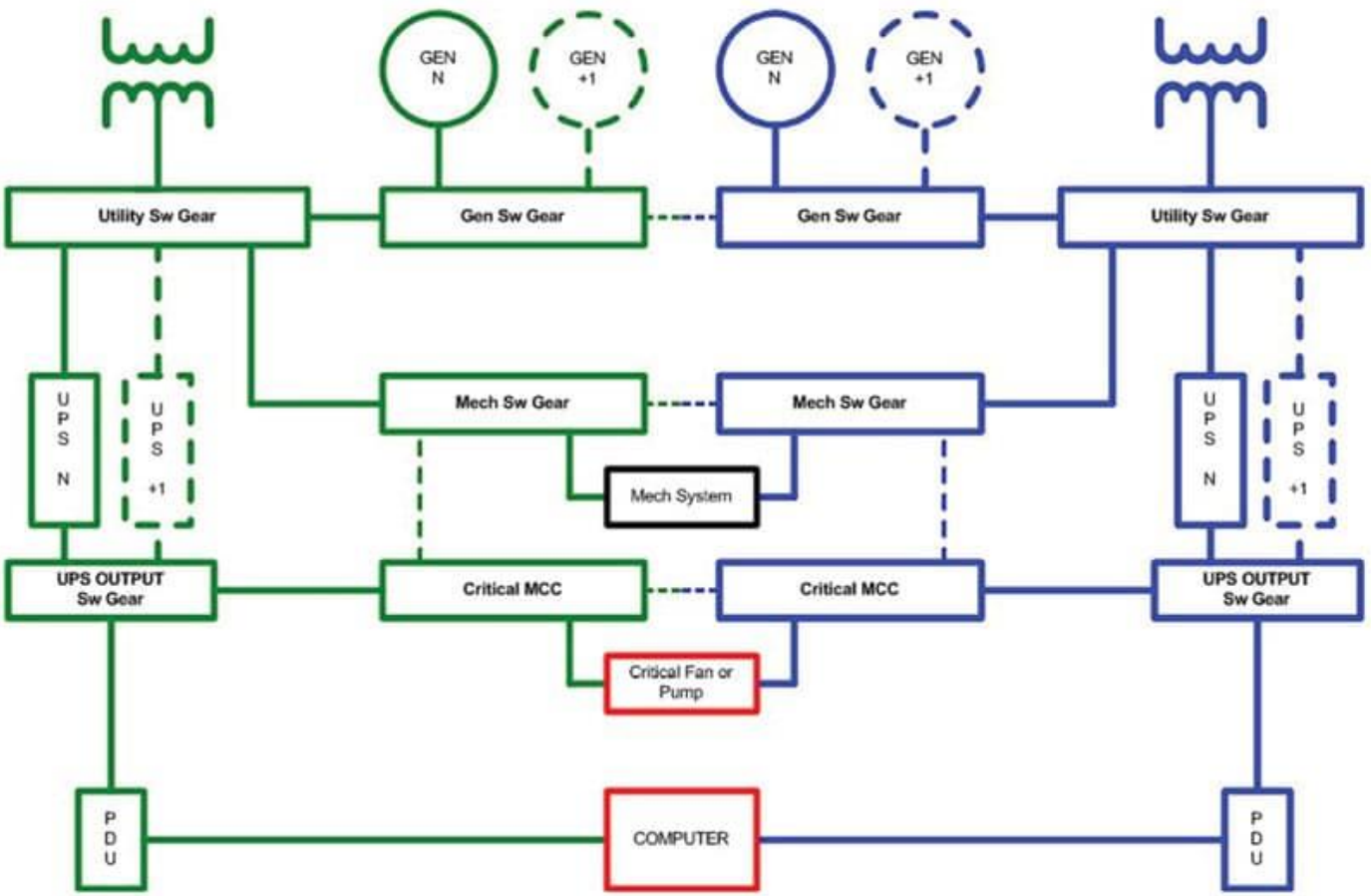
Fonte: Tier Classification Define Site Infrastructure Performance. W. Pitt Turner IV et al.

Datacenter – Tier 4

- 99,995% de tempo de atividade por ano
- 2N+1, ou seja, infraestrutura totalmente redundante
- Proteção contra queda de energia de 96 horas
- Sistemas de refrigeração que estão continuamente disponíveis 24x7x365
- Infraestrutura de local tolerante a falhas com instalações de armazenamento e distribuição de energia elétrica
- Caminhos de distribuição são fisicamente isolados uns dos outros e são frequentemente referidos como caminhos de distribuição "compartimentalizados", evitando danos de um único evento que pode ocorrer no local
- 12 horas no local de armazenamento de combustível

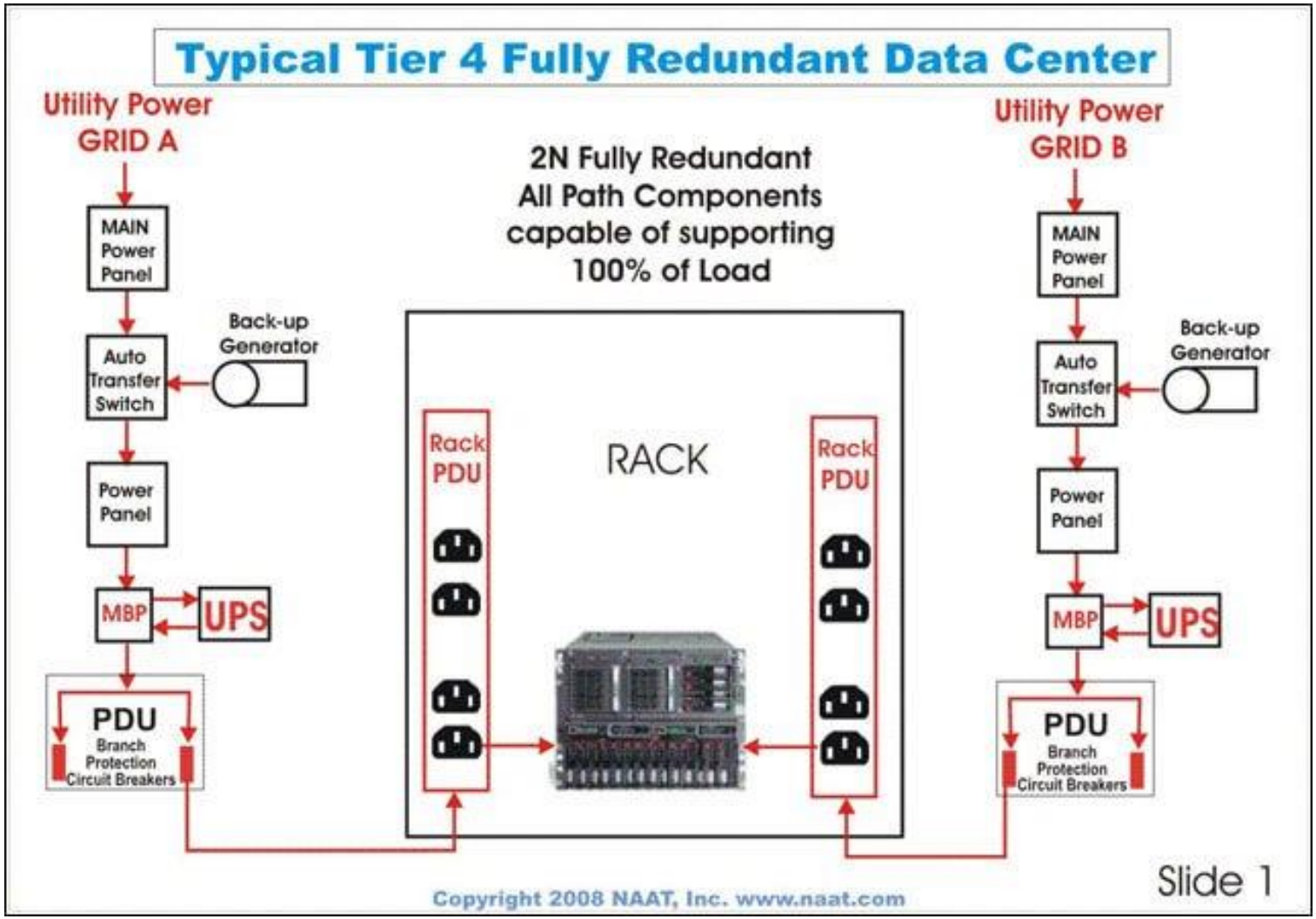
Fonte: Tier Classification Define Site Infrastructure Performance. W. Pitt Turner IV et al.

Datacenter – Tier 4

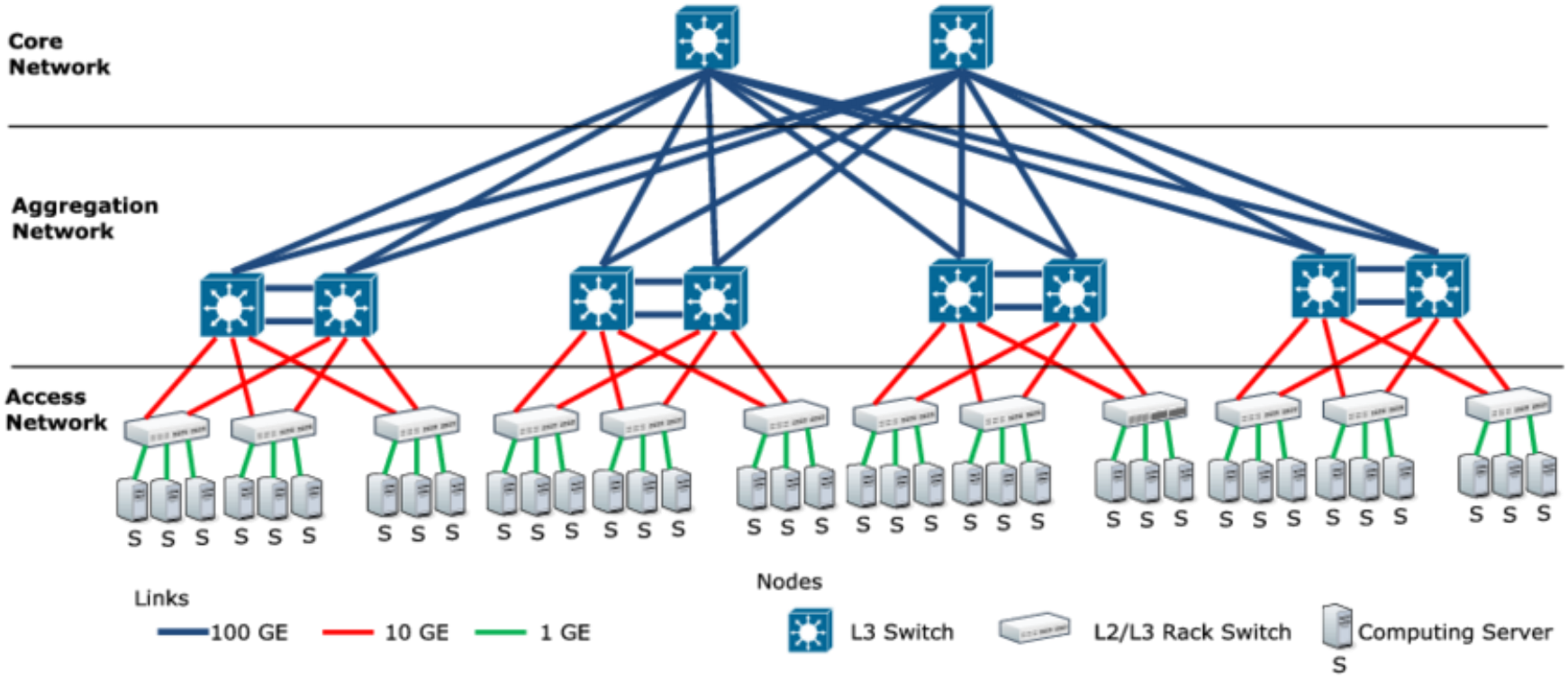


Fonte: Tier Classification Define Site Infrastructure Performance. W. Pitt Turner IV et al.

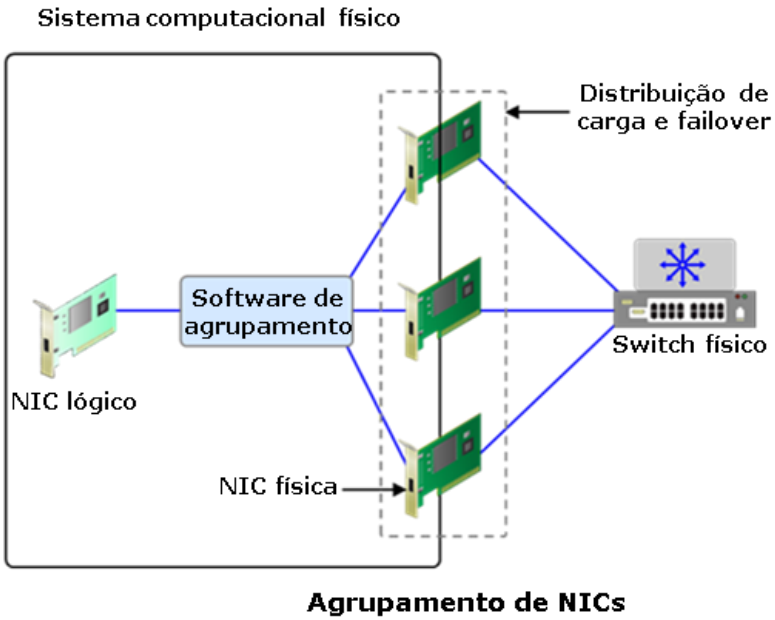
Datacenter – Tier 4



Redundância de rede

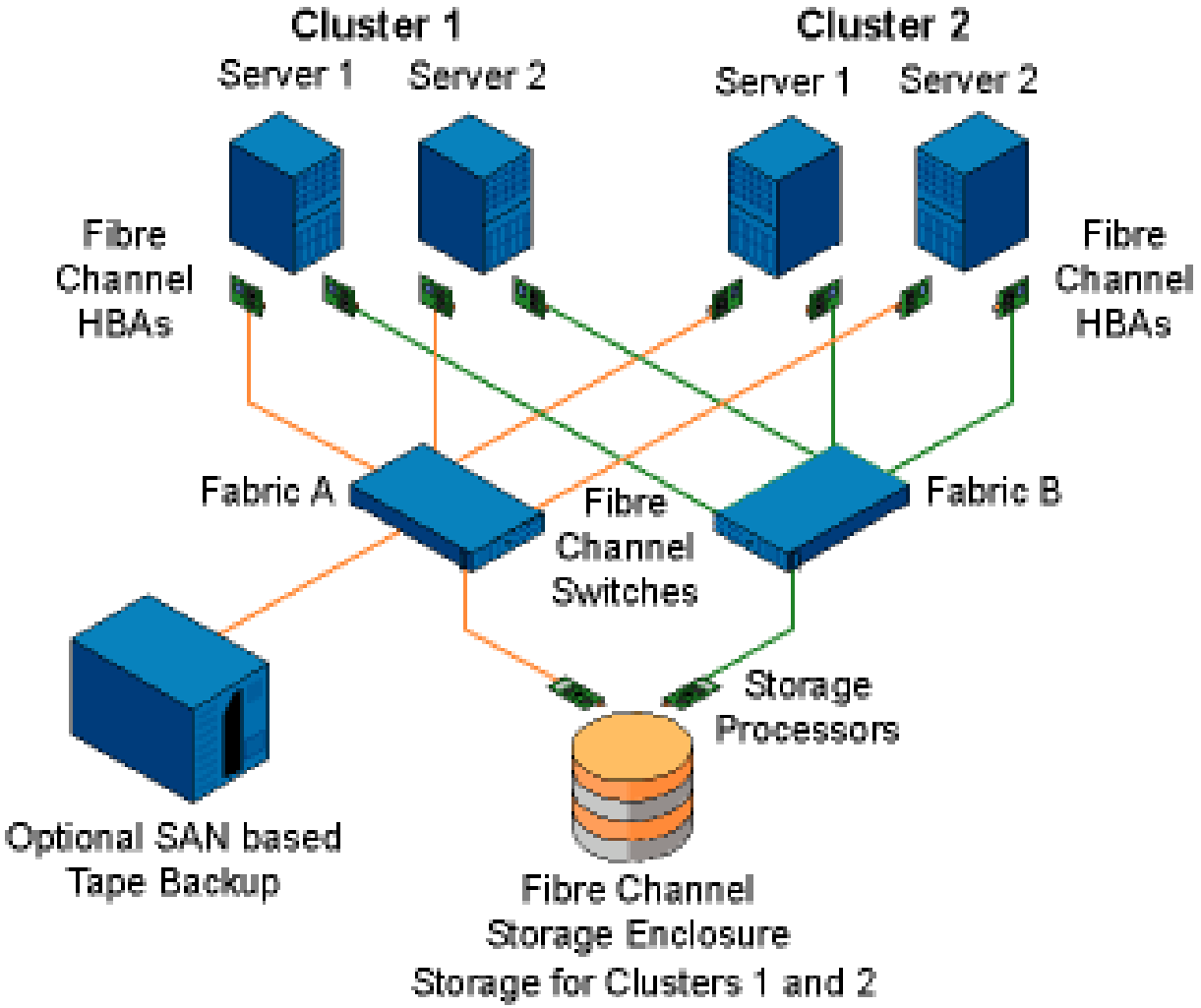


Agregação de enlaces

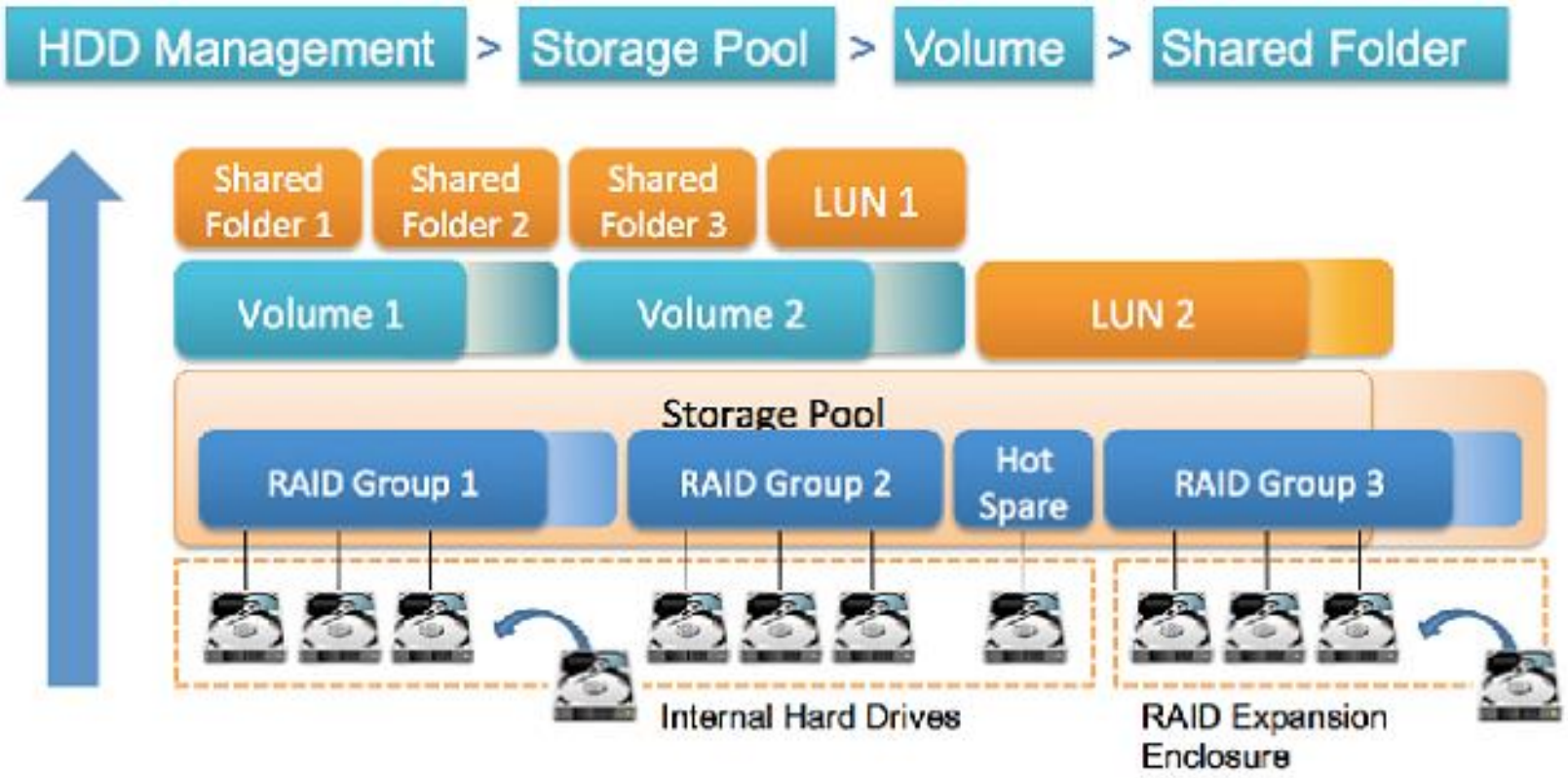


Fonte: EMC Information Storage and Management v3

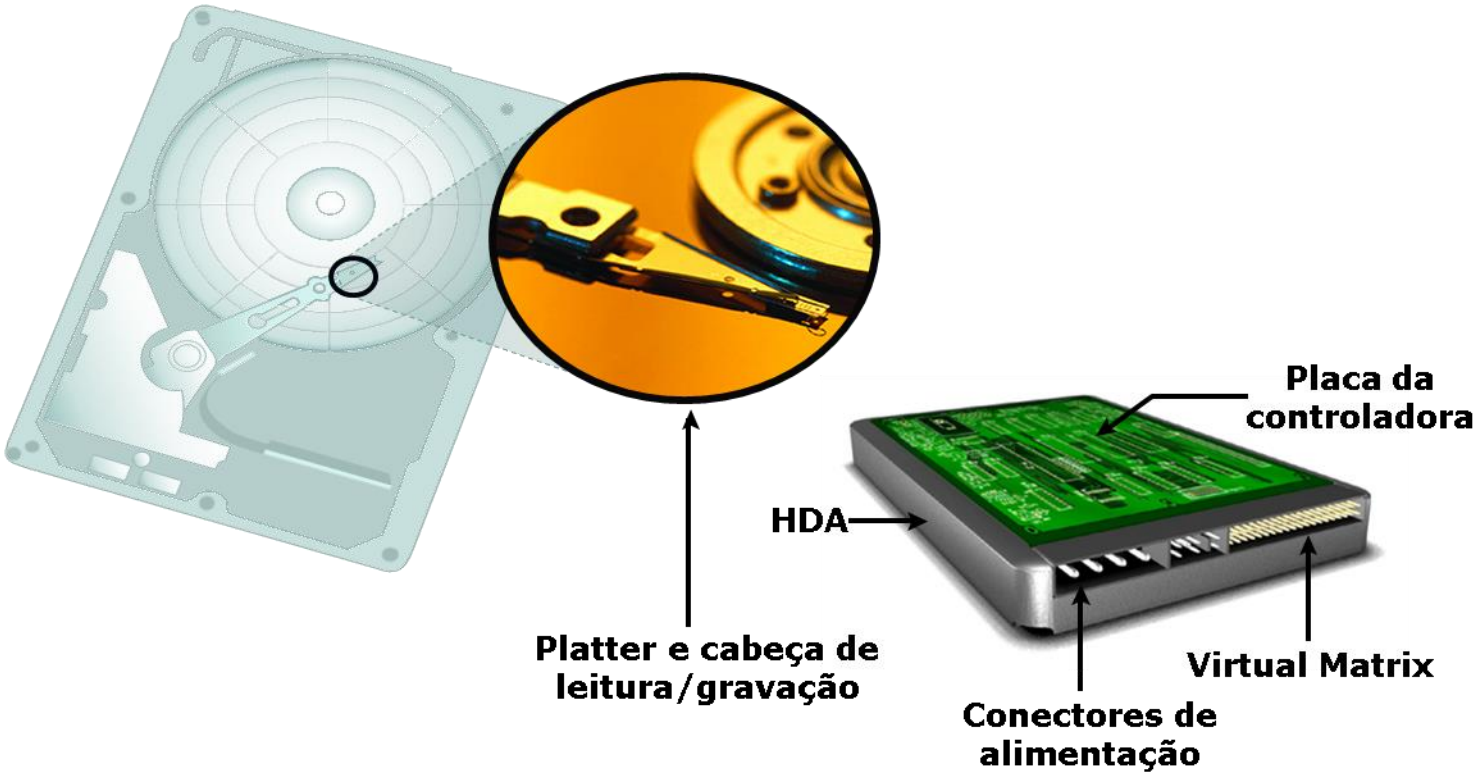
Cluster


Cluster 1
Server 1
Server 2
Cluster 2
Server 1
Server 2
Fibre Channel HBAs
Fibre Channel HBAs
Fabric A
Fabric B
Fibre Channel Switches
Storage Processors
Optional SAN based Tape Backup
Fibre Channel Storage Enclosure
Storage for Clusters 1 and 2

Array de discos

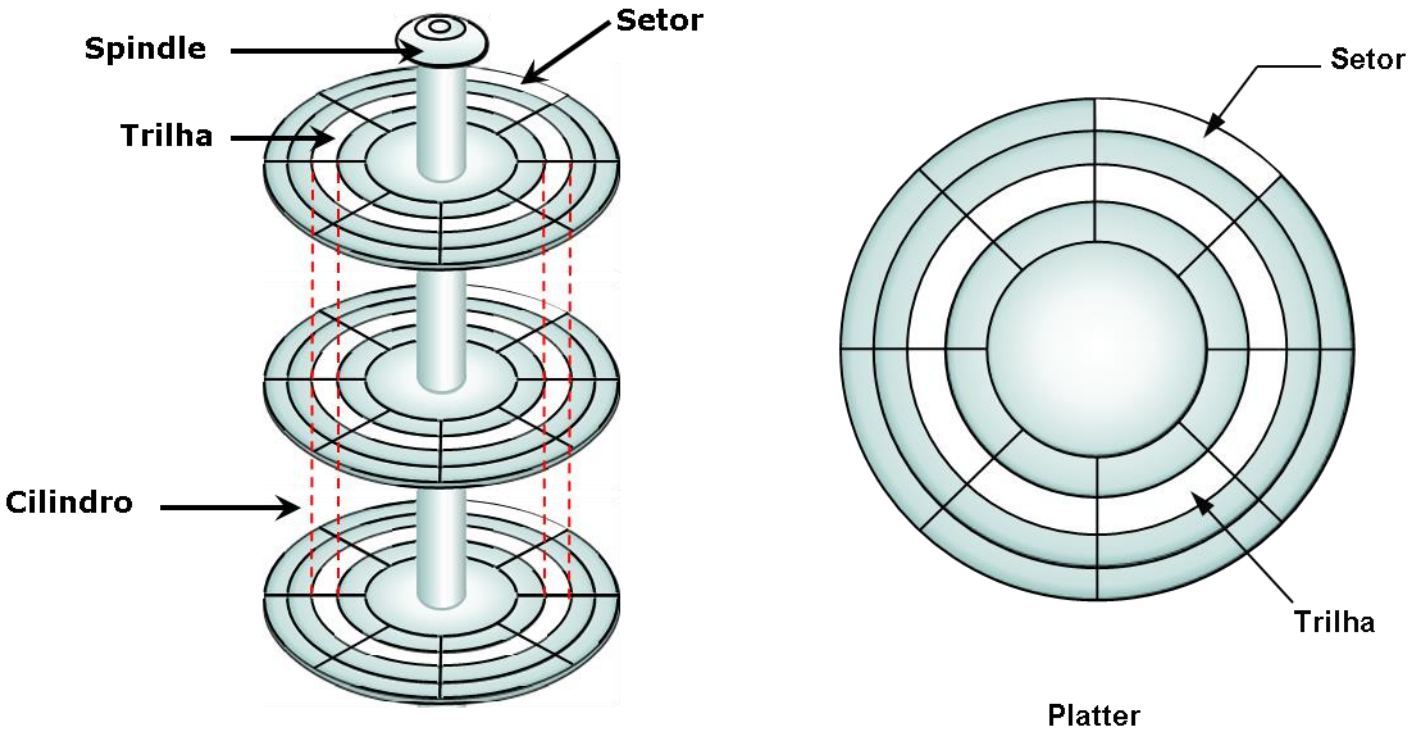


Componentes de disco



Fonte: EMC Information Storage and Management v3

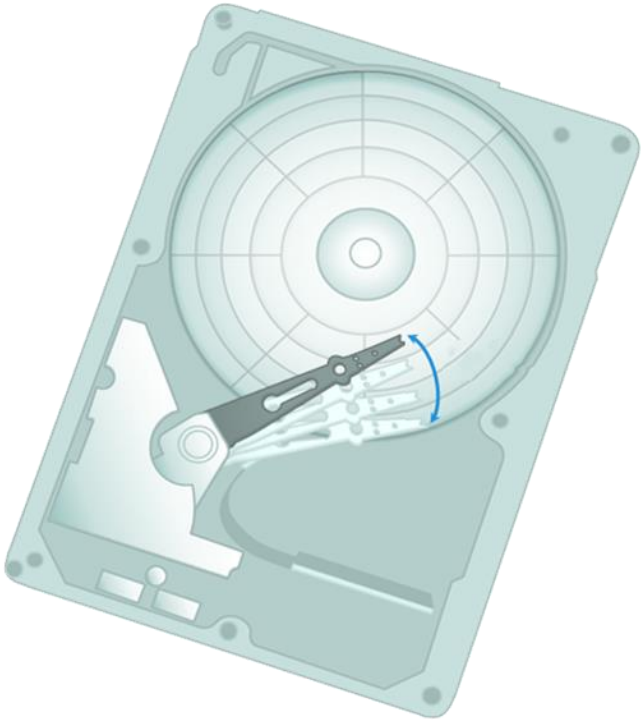
Estrutura do disco



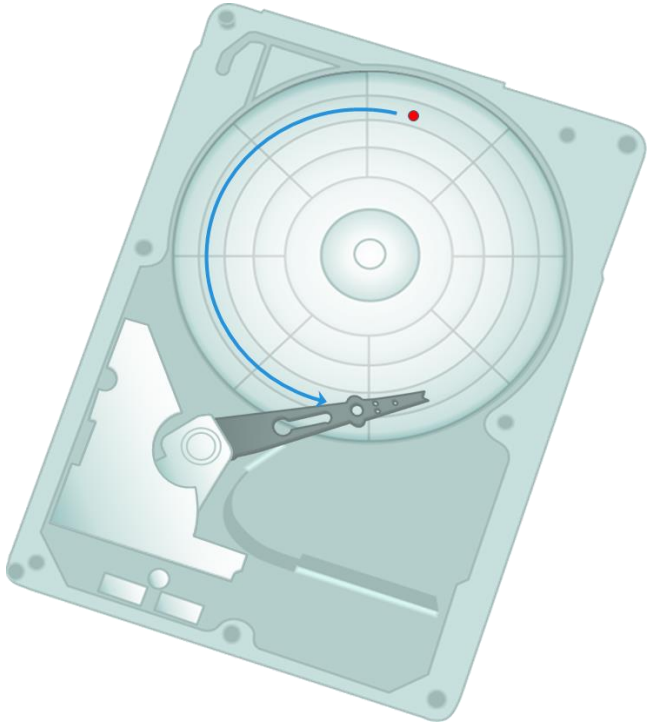
Fonte: EMC Information Storage and Management v3

Estrutura do disco

- Tempo de busca



- Latência rotacional



Fonte: EMC Information Storage and Management v3

Array de discos

O termo RAID (redundant array of independent disks)* refere-se a uma técnica que combina múltiplos discos em uma unidade lógica (conjunto de RAIDs) e fornece proteção, desempenho ou ambos.

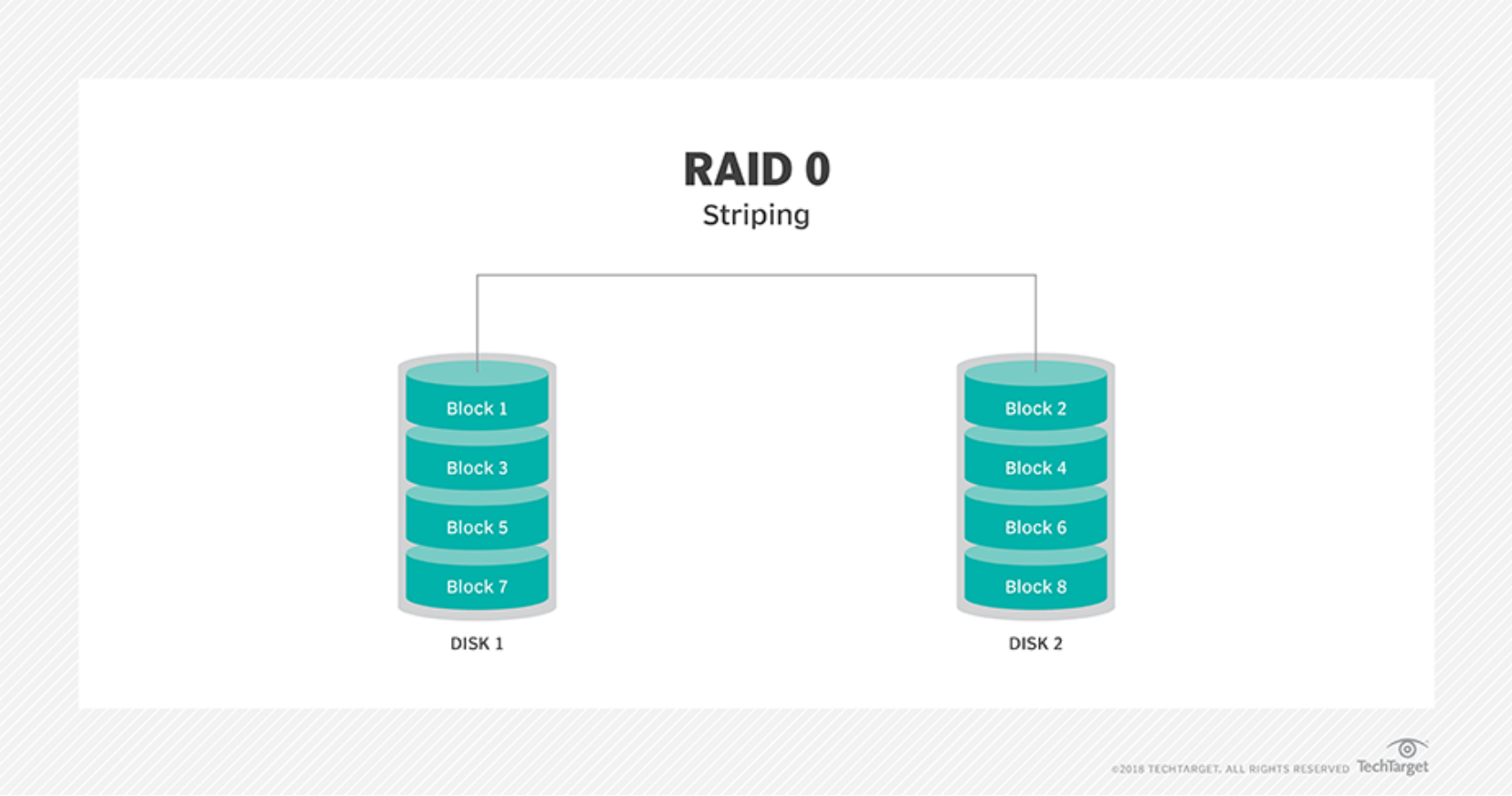
Os níveis de RAID comumente usados são:

- RAID 0: Conjunto fracionado sem tolerância para falhas;
- RAID 1: Espelhamento do disco;
- RAID 1+0: RAID aninhado;
- RAID 3: Conjunto fracionado com acesso paralelo e disco de paridade dedicado;
- RAID 5: Conjunto fracionado com acesso independente ao disco e uma paridade distribuída;
- RAID 6: Conjunto fracionado com acesso independente ao disco e dupla paridade distribuída.

*no passado RAID significava *redundant array of inexpensive disks*.

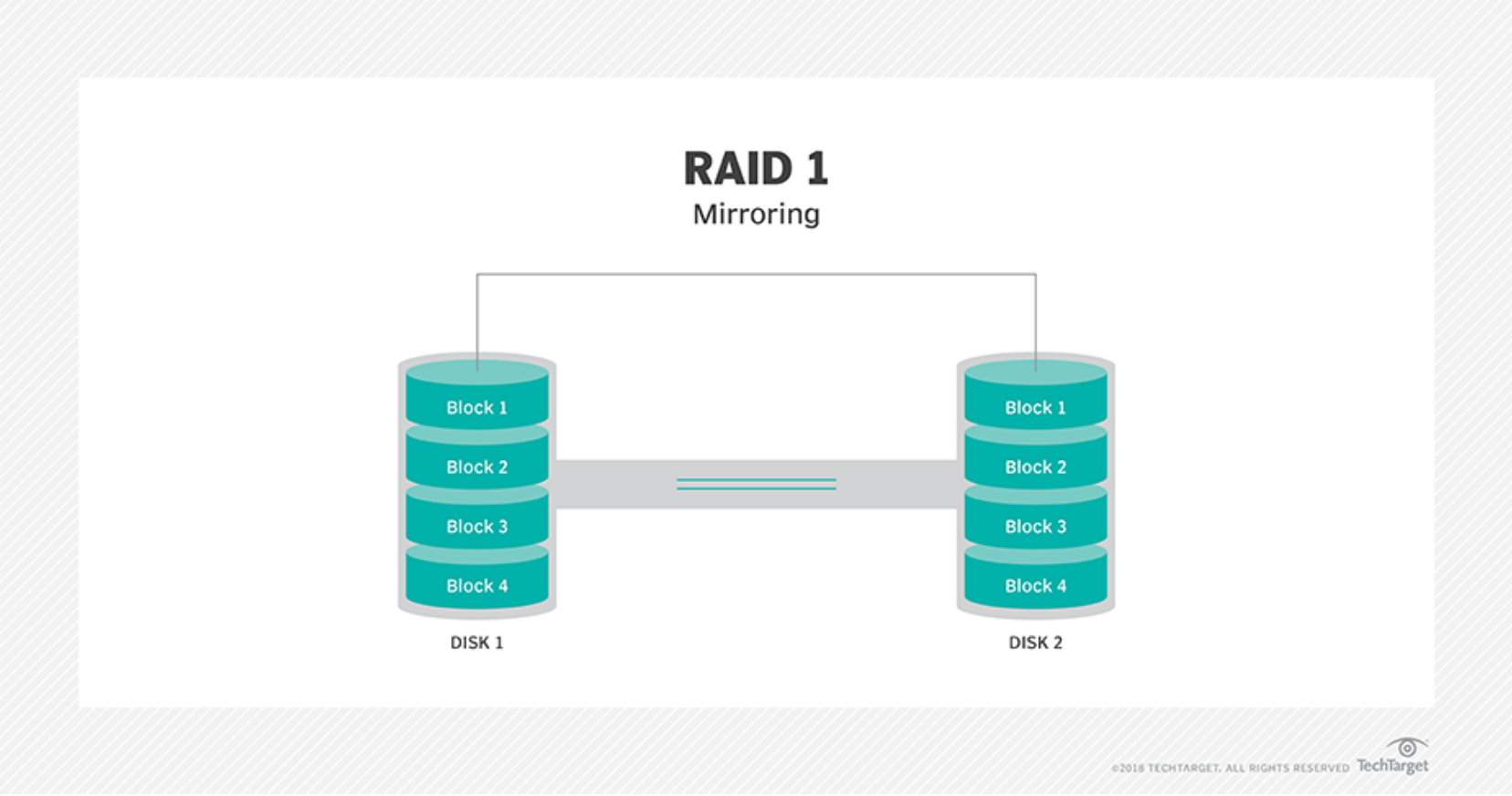
Fonte: EMC Information Storage and Management v3

RAID 0



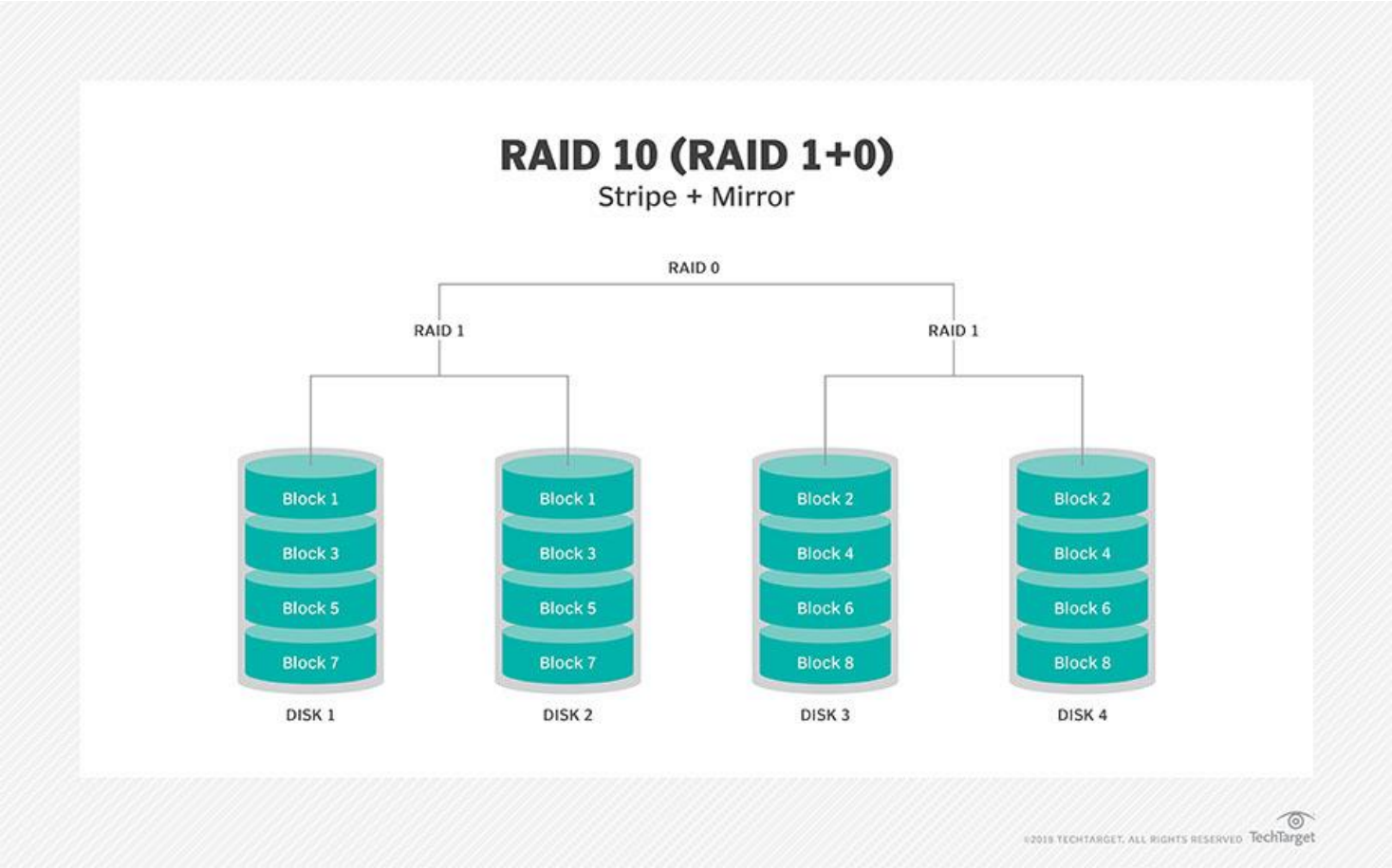
Fonte: searchstorage.techtarget.com

RAID 1



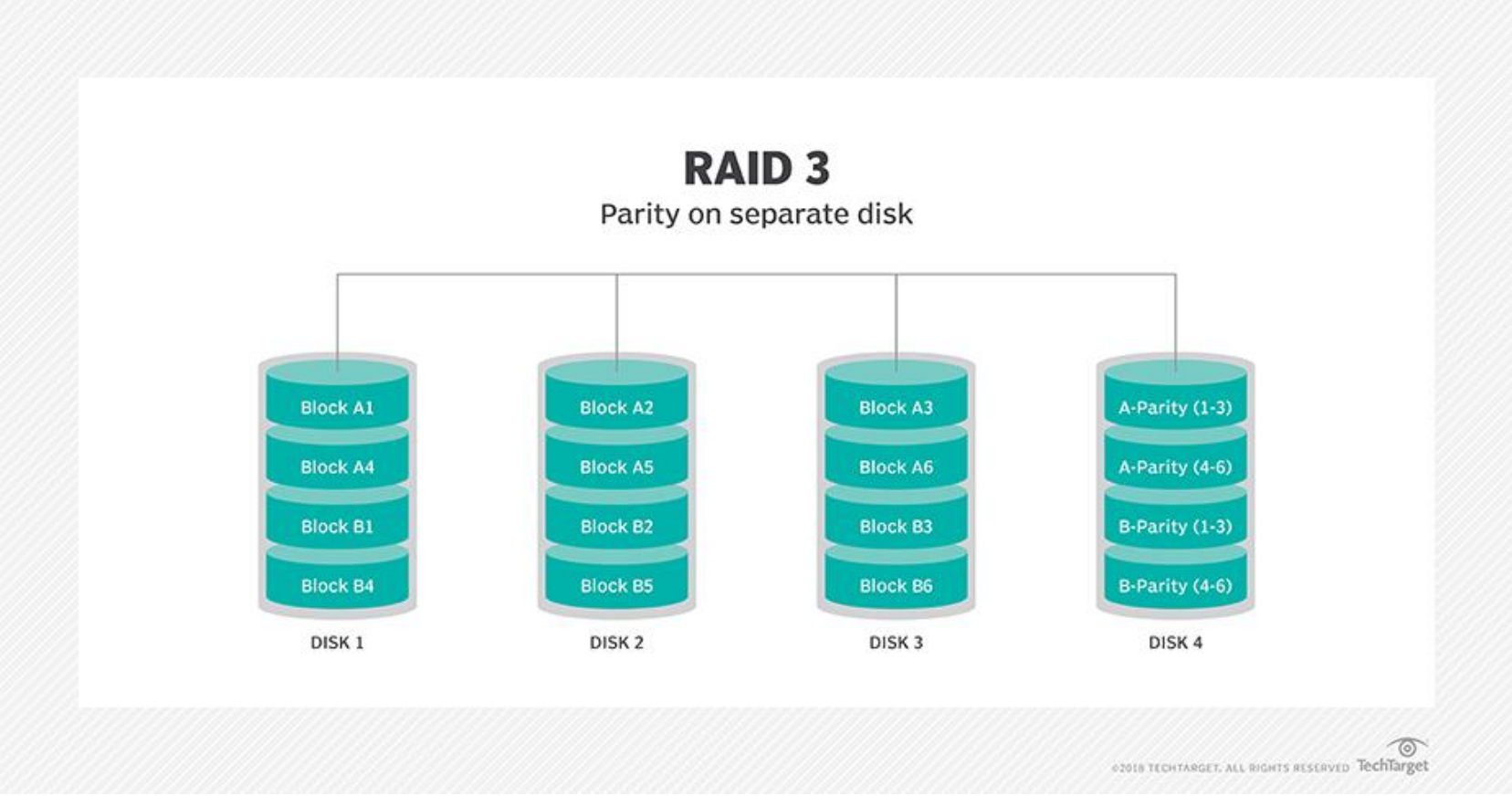
Fonte: searchstorage.techtarget.com

RAID 1+0



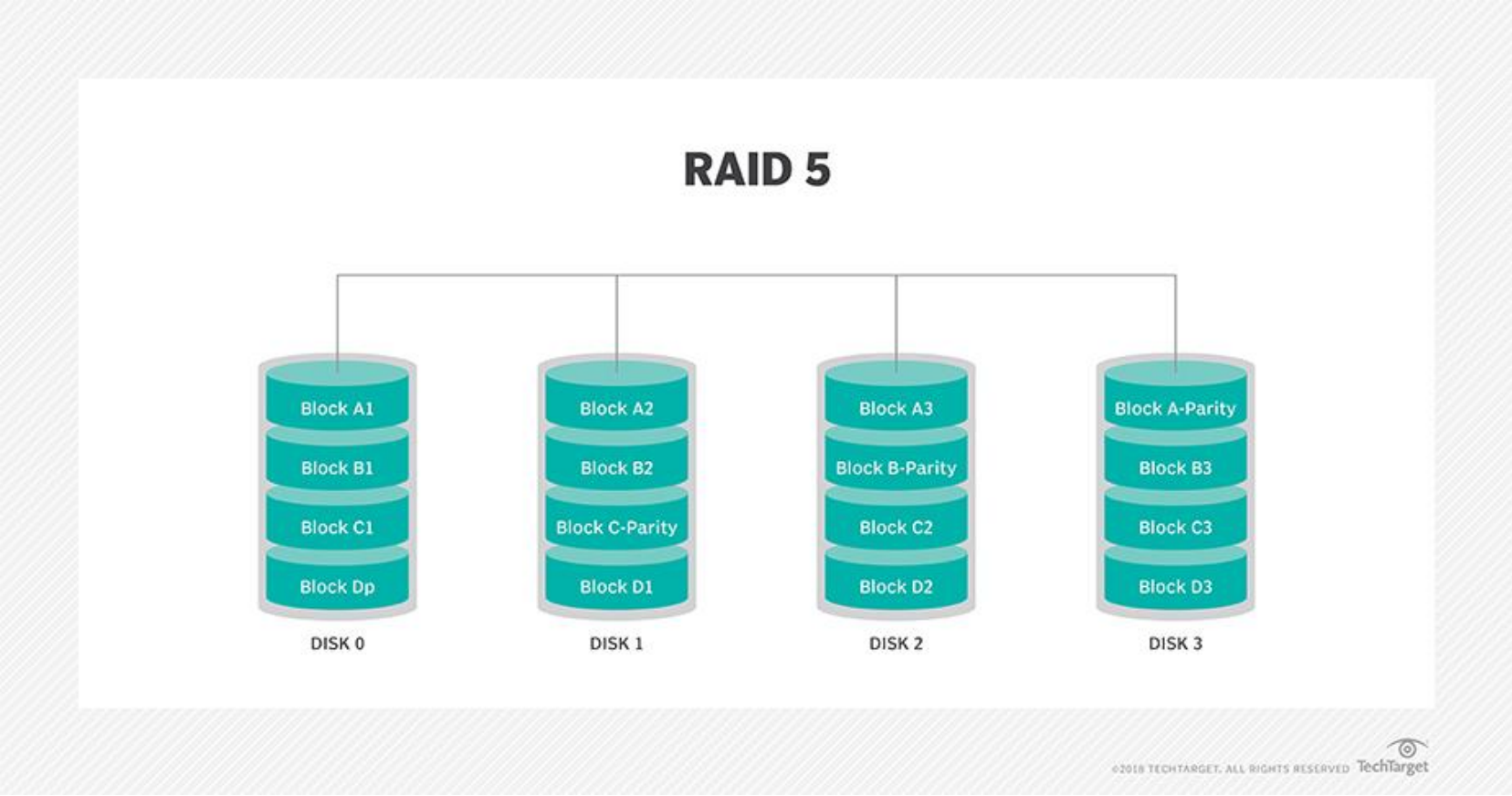
Fonte: searchstorage.techtarget.com

RAID 3



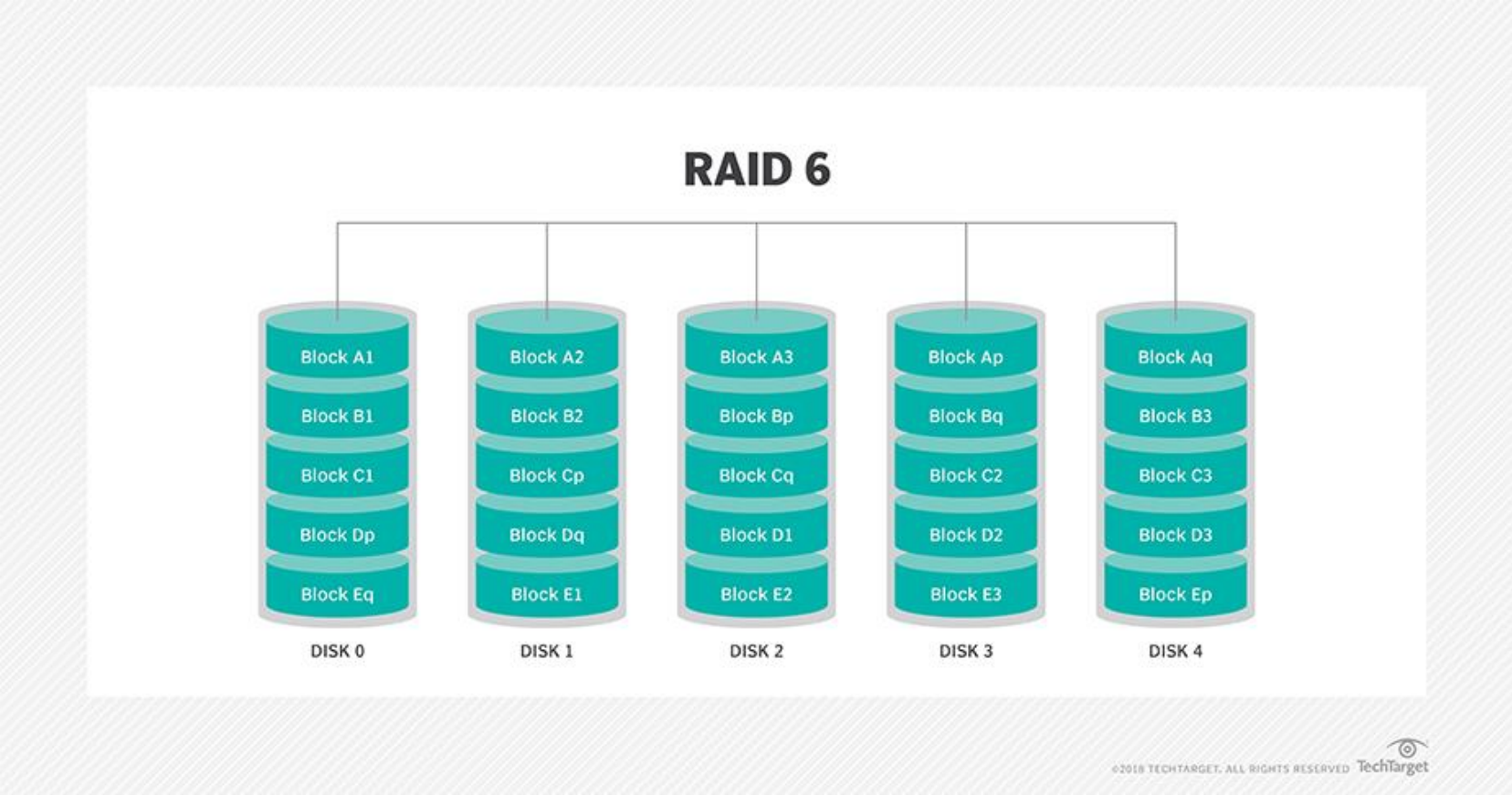
Fonte: EMC Information Storage and Management v3

RAID 5



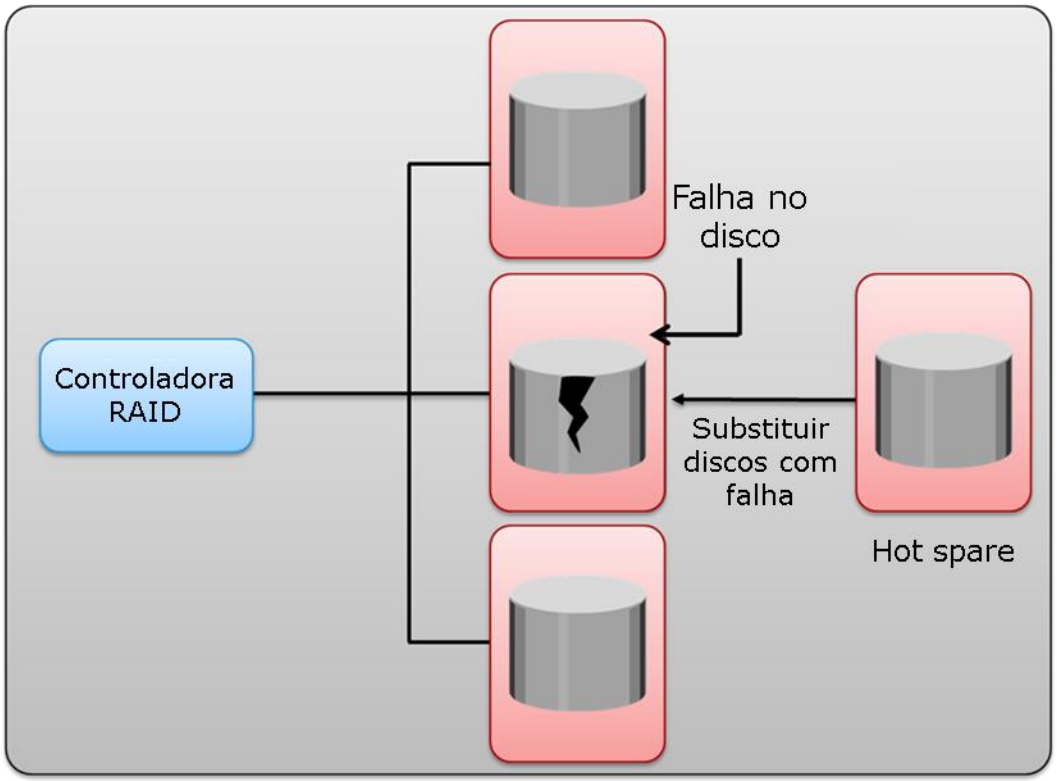
Fonte: searchstorage.techtarget.com

RAID 6



Fonte: searchstorage.techtarget.com

Hot spare



Fonte: EMC Information Storage and Management v3

Servidor rack – visão frontal

Fonte: Dell Server Demo Installer

Servidor rack – visão frontal

Fonte: Dell Server Demo Installer

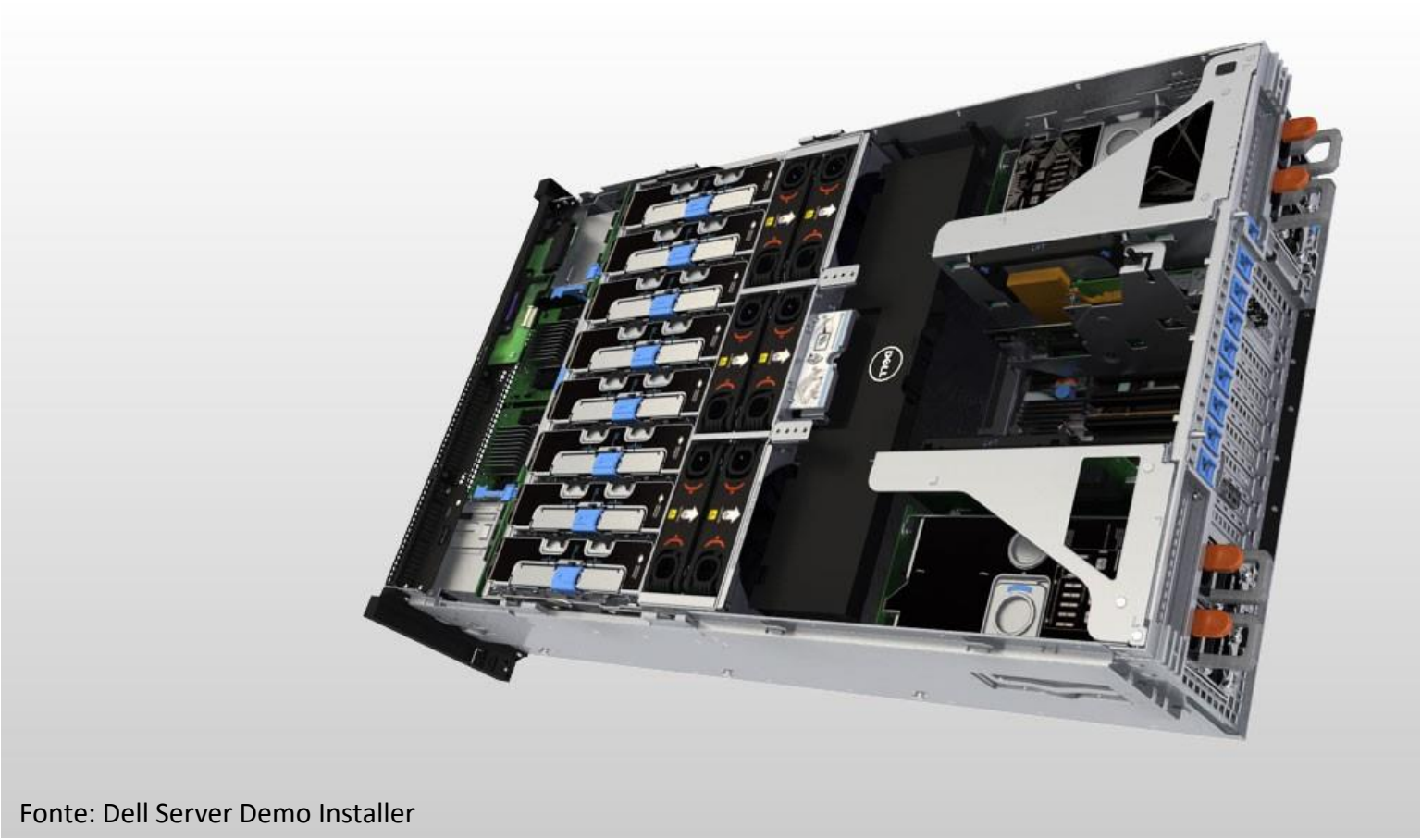
Discos hot-plug

Fonte: Dell Server Demo Installer

Servidor rack – visão superior

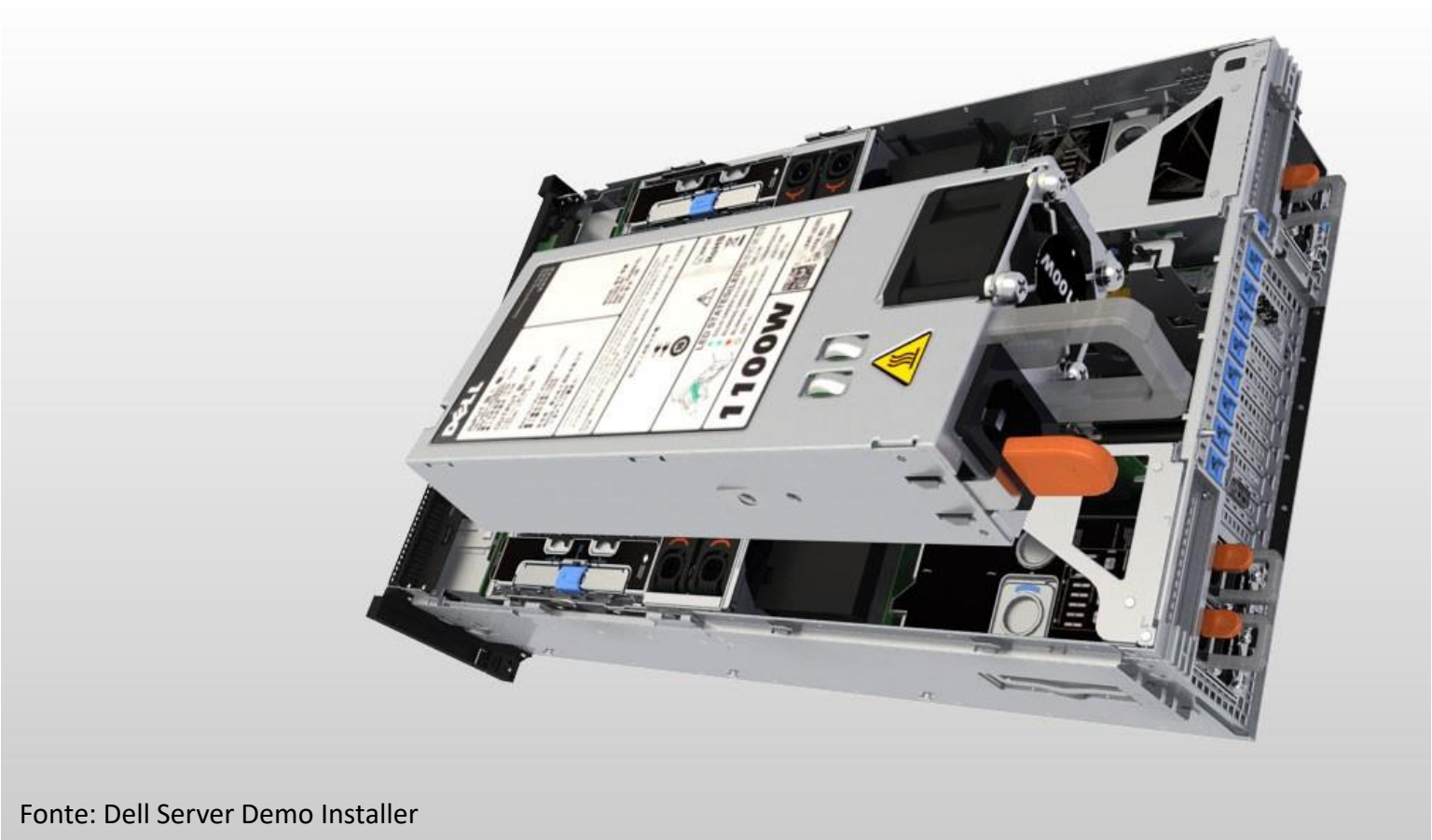
Fonte: Dell Server Demo Installer

Servidor rack – visão superior



Fonte: Dell Server Demo Installer

Fonte redundante

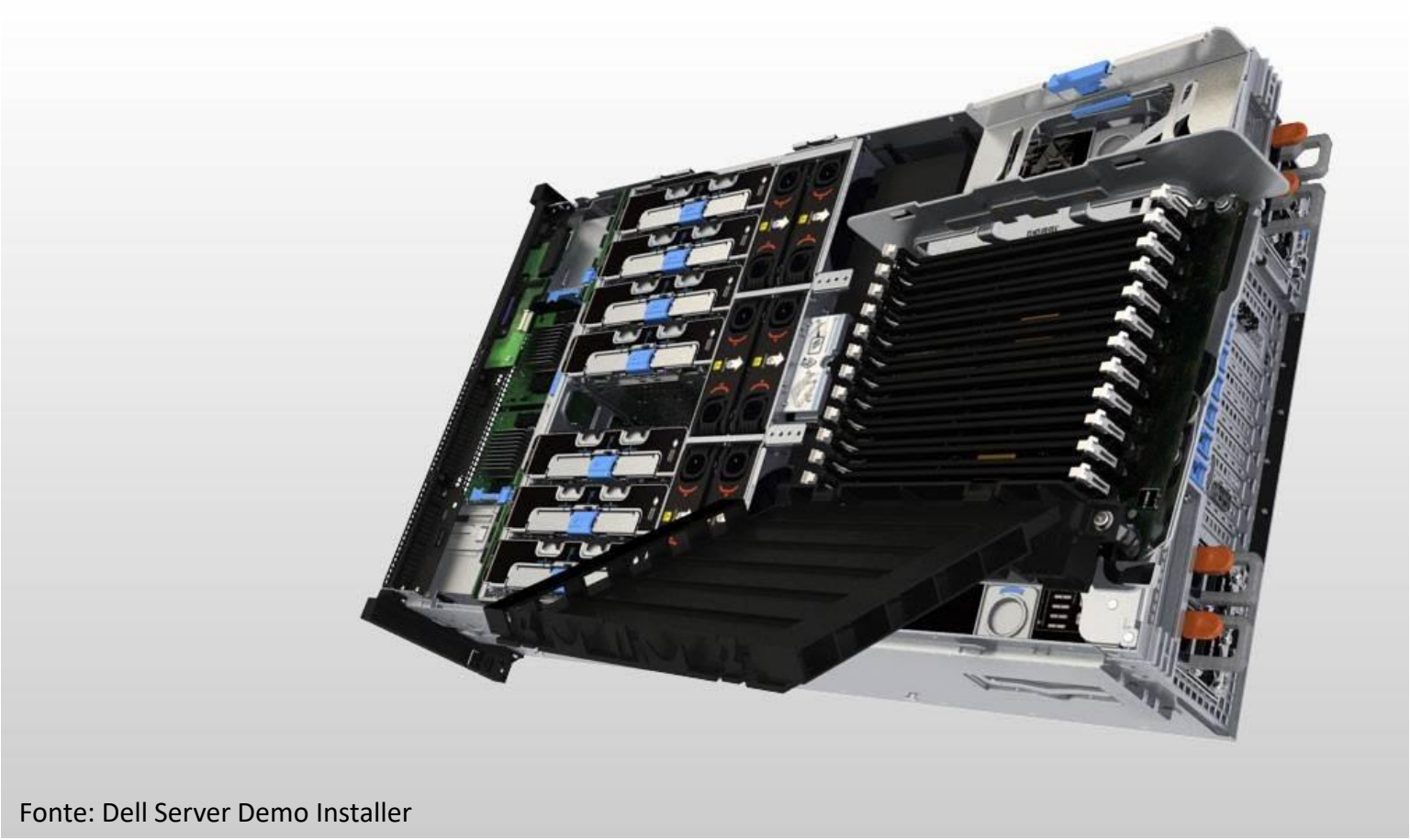


Fonte: Dell Server Demo Installer

Ventilador hot-plug

Fonte: Dell Server Demo Installer

Banco de memória



Fonte: Dell Server Demo Installer

Para saber mais...

... leia o Guia de Boas Práticas para Planos de Continuidade de Negócios, da Associação Brasileira das Entidades Fechadas de Previdência Complementar

… leia o artigo Tier Classifications Define Site Infrastructure Performance, de W. Pitt Turner IV et al.

Módulo 12

Plano de Recuperação de Desastres

Introdução

À medida que mais aplicativos críticos são virtualizados e os datacenters se movem em direção ao enfoque definido por software, é importante que as organizações saibam que nem todos os aplicativos têm os mesmos requisitos de recuperação.

Ao projetar uma estratégia de continuidade de negócios, as empresas devem considerar os dois parâmetros importantes que estão intimamente associados com a recuperação. São eles o RPO (Recovery Point Objective, ou Objetivo de Ponto de Recuperação) e o RTO (Recovery Time Objective, ou Objetivo de Tempo de Recuperação).

O RPO e o RTO são contados em minutos, horas ou dias, e estão diretamente relacionados com a criticidade dos serviços de TI e dos dados.

Quanto menor for o número de RTO e RPO, maior será o custo de uma solução de recuperação de desastres.

Fonte: EMC Information Storage and Management v3

Recovery Point Objective

- **RPO (Recovery Point Objective, ou Objetivo de Ponto de Recuperação):** Este é um point-in-time em que os sistemas devem estar recuperados depois de uma paralisação. Ele define o volume de dados perdidos a que uma empresa pode resistir. Com base no RPO, as organizações planejam a frequência com que deve ser feito um backup ou réplica. Uma organização pode planejar uma solução tecnológica de continuidade de negócios apropriada com base no RPO que ela define. Por exemplo, se o RPO de um aplicativo de negócios particular for 24 horas, os backups são criados todos os dias à meia-noite. A estratégia de recuperação correspondente é restaurar os dados do conjunto do último backup.

Fonte: EMC Information Storage and Management v3

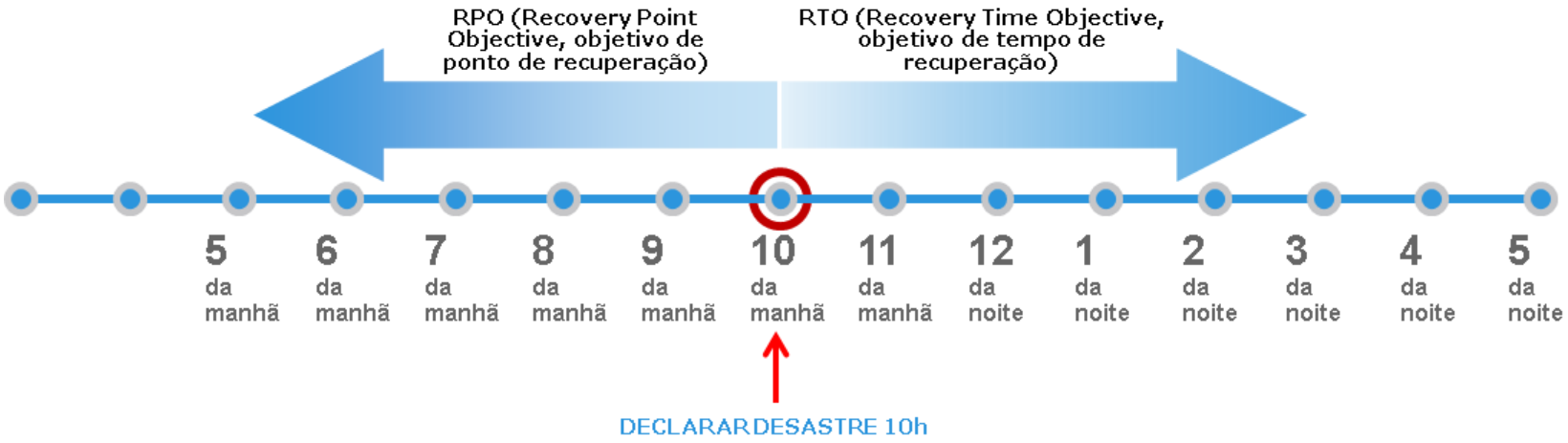
Recovery Time Objective

- **RTO (Recovery Time Objective, ou Objetivo de Tempo de Recuperação):** Esse é o tempo em que os sistemas e aplicativos devem estar recuperados depois de uma paralisação. Ele define a quantidade de tempo de inatividade que um negócio pode resistir e sobreviver. Por exemplo, se o RTO for de alguns segundos, então a implementação de clustering global ajudaria a atingir o RTO necessário. Quanto mais essencial o aplicativo, menor deve ser o RTO.

Fonte: EMC Information Storage and Management v3

Resumo

RPO (Recovery Point Objective, objetivo de ponto de recuperação)	RTO (Recovery Time Objective, objetivo de tempo de recuperação)
Point-in-time em que os sistemas devem estar recuperados depois de uma paralisação	Tempo em que os sistemas e aplicativos devem estar recuperados depois de uma paralisação
Volume de dados perdidos a que uma empresa pode resistir	Tempo de inatividade a que um negócio pode resistir e sobreviver



Fonte: EMC Information Storage and Management v3

Backup

Backup ou Cópia de Segurança é uma cópia adicional dos dados de produção, criada e retida com o objetivo exclusivo de recuperar dados perdidos ou corrompidos.

Tipicamente, tanto os dados do aplicativo quanto as configurações do servidor são incluídos em backups para restaurar dados e servidores em caso de paralisação.

As empresas também implementam soluções de backup para armazenamento de longo prazo, com o objetivo de preservar registros necessários para atender a requisitos regulamentares.

Fonte: EMC Information Storage and Management v3

Restore

A operação de recuperação de uma cópia de segurança (restore) procura atender aos seguintes objetivos:

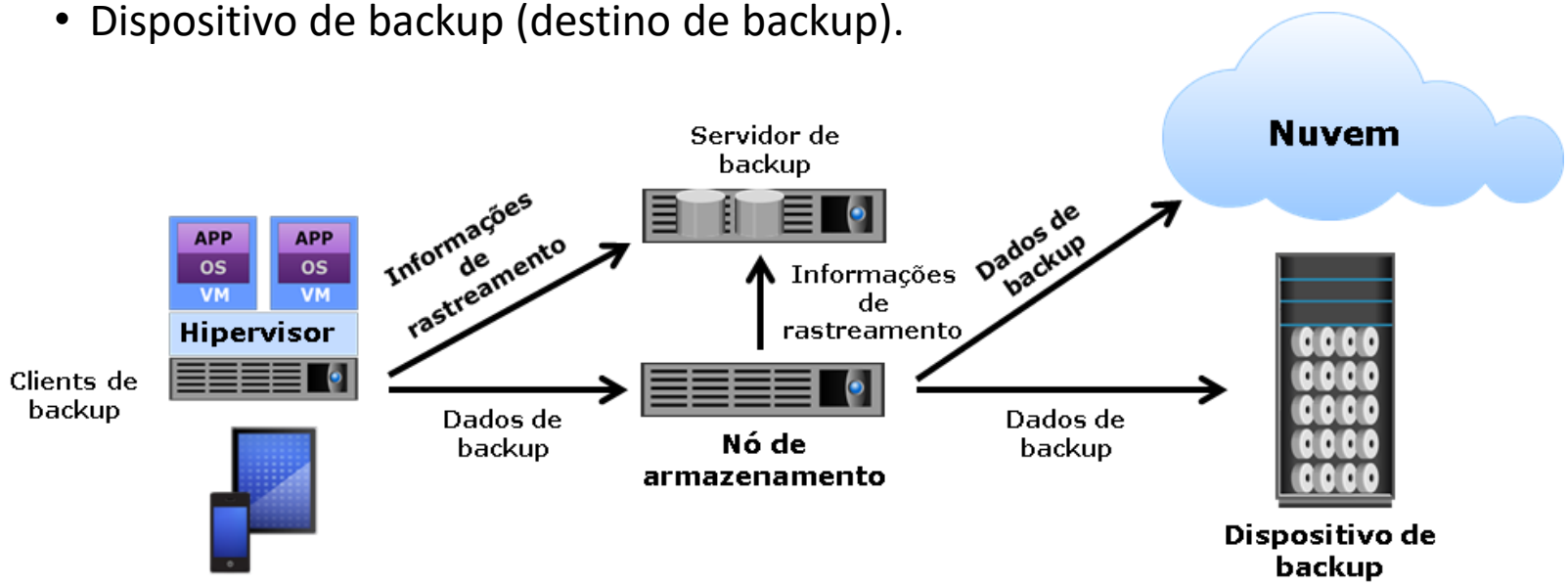
- Recuperação de desastres
  - Faz a restauração para o estado operacional após um desastre
- Restaurações operacionais
  - Permitem a recuperação em caso de perda ou corrupção lógica dos dados

Toda cópia de segurança (backup) deve ser submetida a uma operação de recuperação (restore) para verificação da mídia quanto a sua integridade.

Fonte: EMC Information Storage and Management v3

Arquitetura de backup

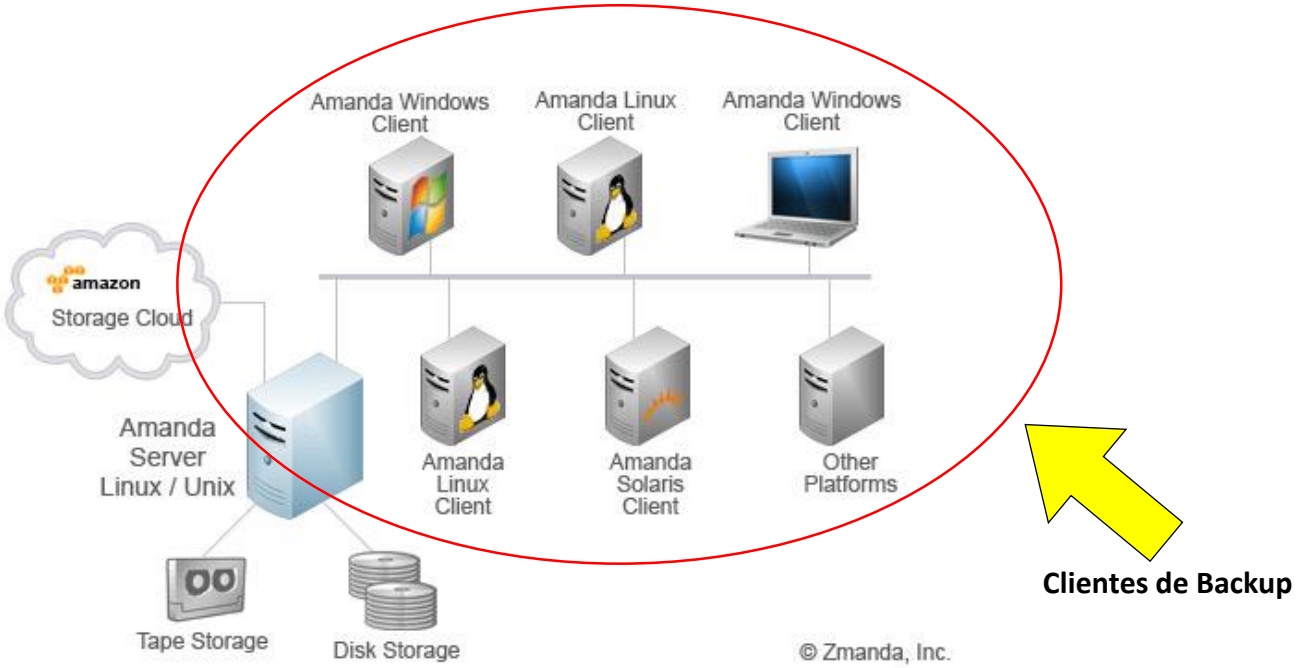
- Componentes principais do backup
  - Cliente de backup;
  - Servidor de backup;
  - Nó de armazenamento;
  - Dispositivo de backup (destino de backup).



Fonte: EMC Information Storage and Management v3

Arquitetura de backup

A função de um cliente de backup é coletar os dados a serem incluídos no backup e enviá-los ao nó de armazenamento. O cliente de backup pode ser instalado nos servidores de aplicativos, clientes móveis e desktops. Ele também envia informações de monitoramento para o servidor de backup.



Fonte: EMC Information Storage and Management v3

Arquitetura de backup

O servidor de backup gerencia as operações de backup e mantém o catálogo de backup, que contém informações sobre a configuração e os metadados do backup. A configuração do backup contém informações sobre quando os backups devem ser feitos, quais dados do cliente devem ser incluídos e assim por diante. Os metadados do backup contêm informações sobre os dados incluídos no backup.

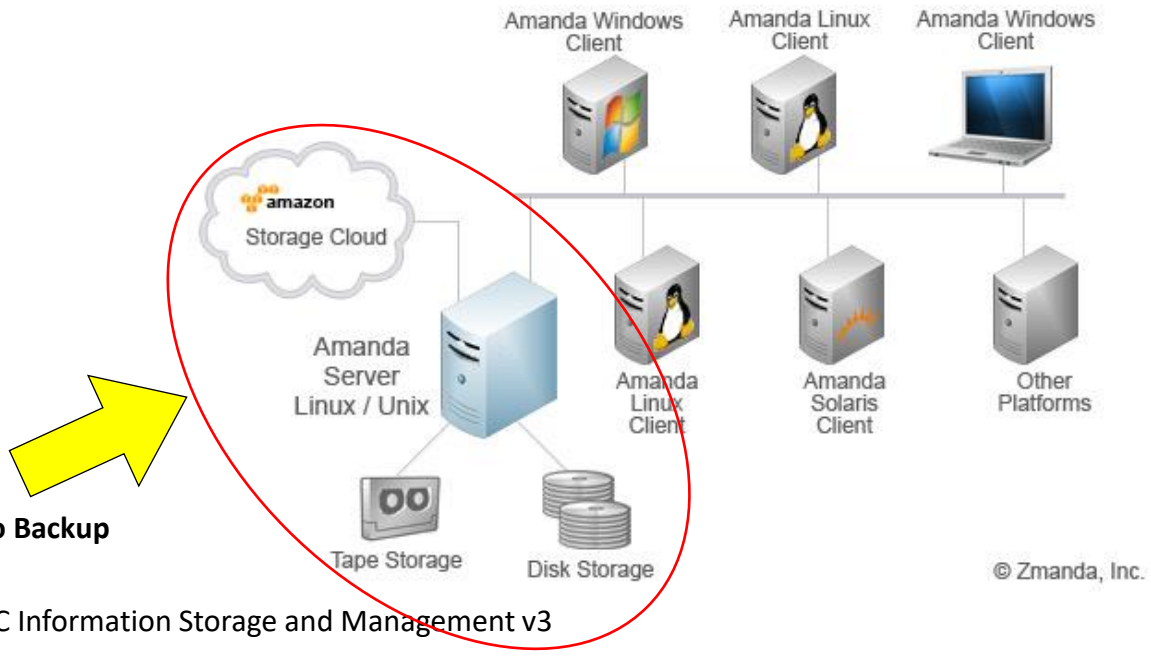
O nó de armazenamento é responsável por organizar os dados do cliente e gravá-los em um dispositivo de backup. O nó de armazenamento controla um ou mais dispositivos de backup. Os dispositivos de backup podem ser conectados diretamente ao nó de armazenamento ou através de uma rede. O nó de armazenamento envia ao servidor de backup as informações de monitoramento sobre os dados gravados no dispositivo de backup. Tipicamente, essas informações são usadas em recuperações.

Na maioria das implementações, o nó de armazenamento e o servidor de backup são executados no mesmo sistema.

Fonte: EMC Information Storage and Management v3

Arquitetura de backup

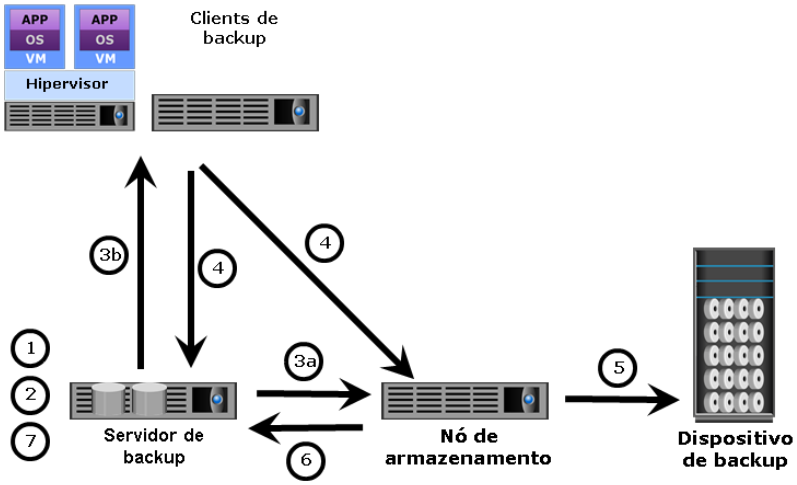
Uma ampla variedade de destinos de backup está disponível atualmente, como fita, disco e biblioteca de fitas virtuais (Virtual Tape Library ou VTL). Agora, a organização também pode fazer backup de seus dados no armazenamento em nuvem. Muitos prestadores de serviços oferecem backup como serviço, o que permite às organizações reduzir a sobrecarga de gerenciamento de backups.



Destino do Backup

Fonte: EMC Information Storage and Management v3

Operação de backup



1 - O servidor de backup inicia o processo de backup agendado.

2 - O servidor de backup obtém informações relacionadas ao backup do catálogo de backup.

3a - O servidor de backup instrui o nó de armazenamento para carregar a mídia de backup no dispositivo de backup.

3b - O servidor de backup instrui os clientes de backup a enviar dados ao nó de armazenamento incluído no backup.

4 - Os clientes de backup enviam dados ao nó de armazenamento e atualizam o catálogo de backup no servidor de backup.

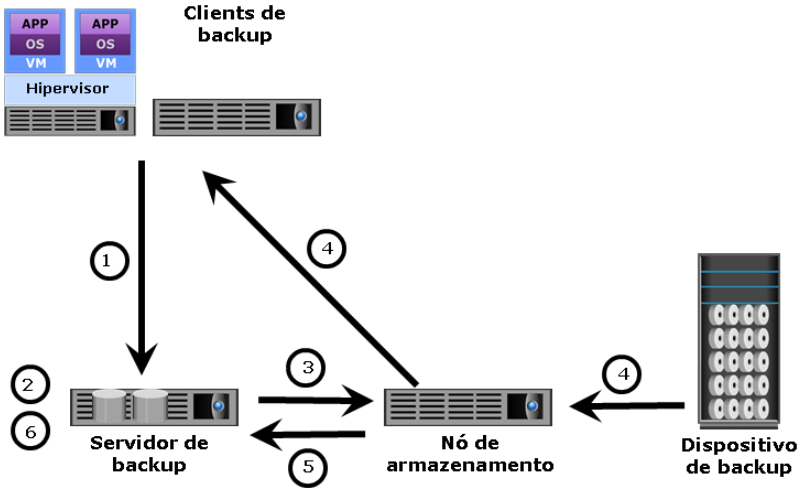
5 - O nó de armazenamento envia dados ao dispositivo de backup.

6 - O nó de armazenamento envia metadados e informações de mídia ao servidor de backup.

7 - O servidor de backup atualiza o catálogo de backup.

Fonte: EMC Information Storage and Management v3

Operação de restore



1 - O cliente de backup solicita a restauração de dados ao servidor de backup.

2 - O servidor de backup examina o catálogo de backup para identificar dados a serem restaurados e o cliente que receberá os dados.

3 - O servidor de backup instrui o nó de armazenamento a carregar a mídia de backup no dispositivo de backup.

4 - Os dados são lidos e enviados ao cliente de backup.

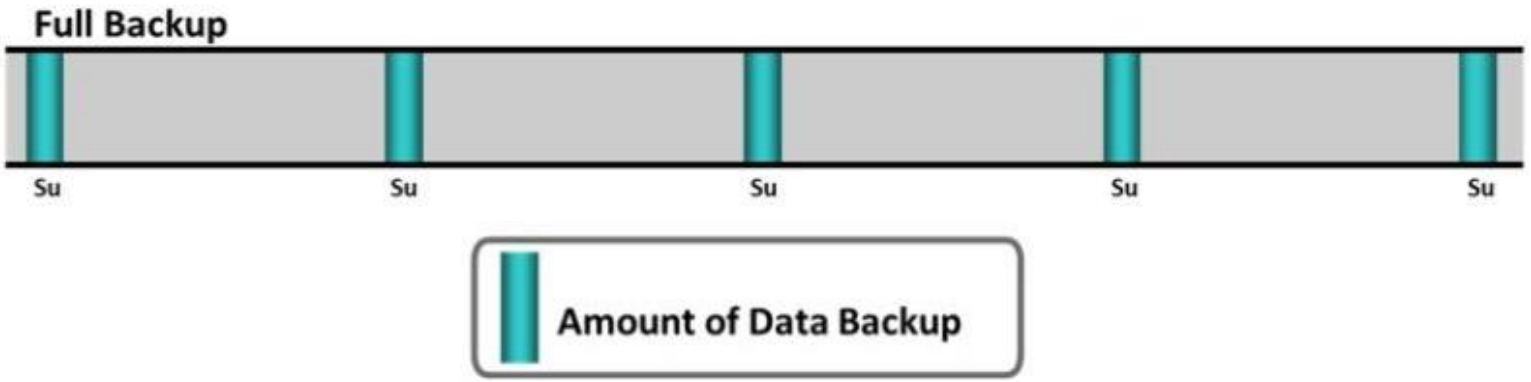
5 - O nó de armazenamento envia metadados de restauração ao servidor de backup.

6 - O servidor de backup atualiza o catálogo de backup.

Fonte: EMC Information Storage and Management v3

Granularidade

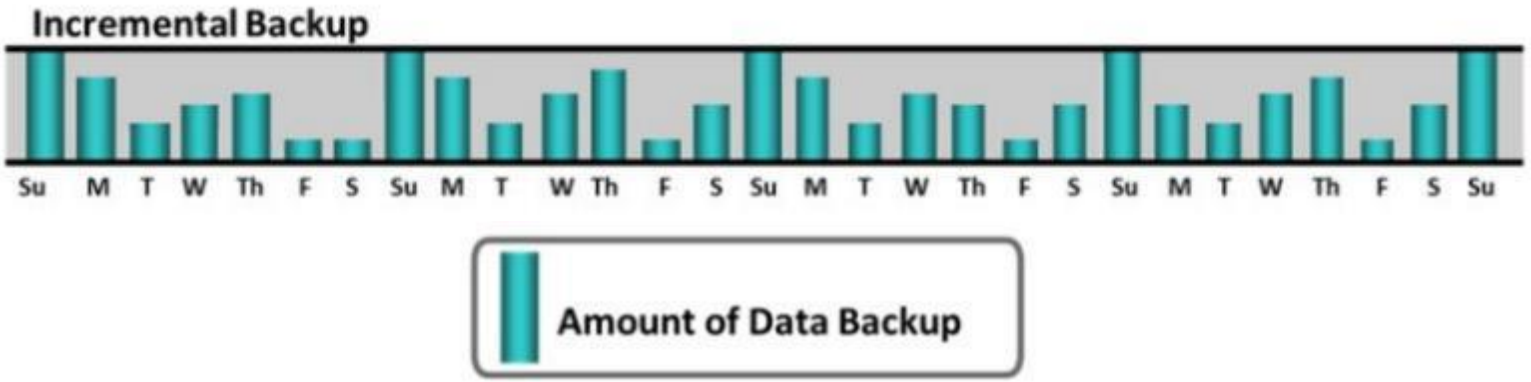
- **Backup completo:** como o nome indica, trata-se de uma cópia completa de todo o conjunto de dados. Tipicamente, as organizações usam o backup completo periodicamente, pois ele exige mais espaço de armazenamento e também demora mais para ser concluído. O backup completo oferece recuperação rápida dos dados.



Fonte: EMC Information Storage and Management v3

Granularidade

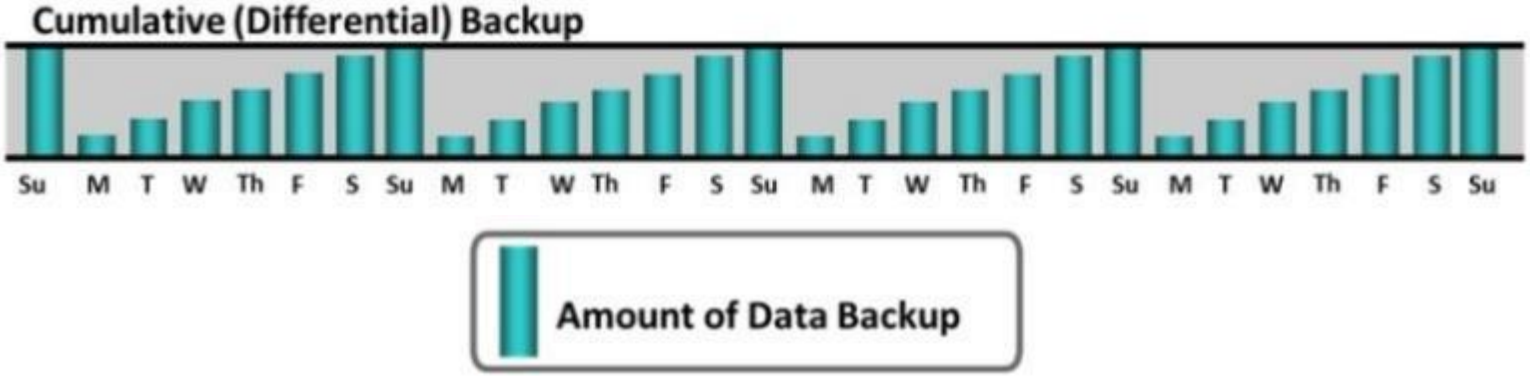
- **Backup incremental:** ele copia os dados que foram alterados desde o último backup. Por exemplo, um backup completo é criado para a segunda-feira, e backups incrementais são criados para o restante da semana. O backup de terça-feira conterá apenas os dados alterados desde segunda-feira. O backup de quarta-feira conterá apenas os dados alterados desde terça-feira. A desvantagem principal dos backups incrementais é o fato de que a restauração deles pode ser demorada. Imagine que um administrador queira restaurar o backup de quarta-feira. Para isso, ele deve primeiro restaurar o backup completo de segunda-feira. Depois, o administrador deve restaurar a cópia de terça-feira, seguida pela de quarta-feira.



Fonte: EMC Information Storage and Management v3

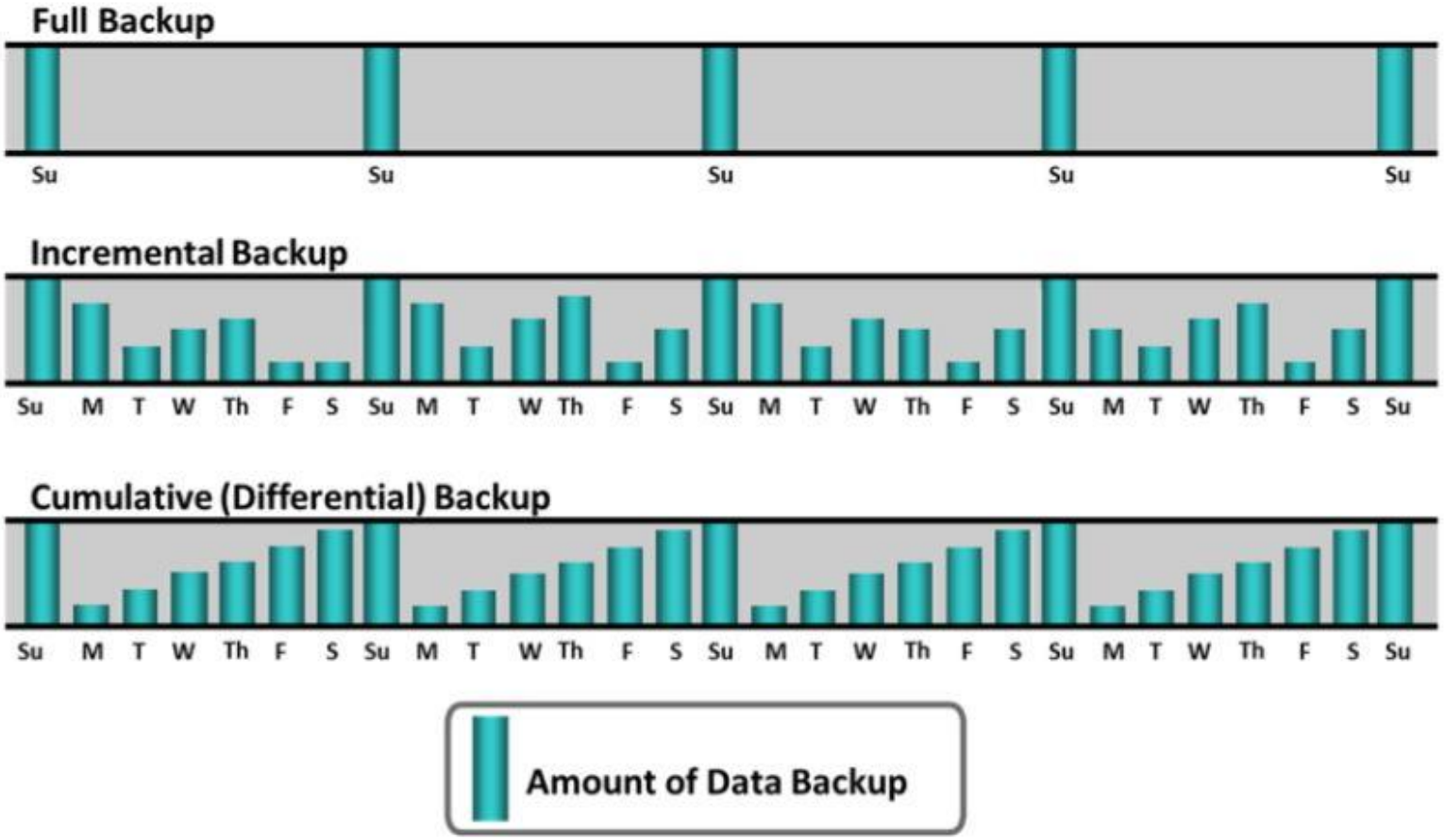
Granularidade

- **Backup cumulativo (diferencial):** ele copia os dados que foram alterados desde o último backup completo. Imagine, por exemplo, que o administrador queira criar um backup completo na segunda-feira e backups diferenciais para o restante da semana. O backup de terça-feira conterá todos os dados alterados desde segunda-feira. Neste ponto, ele seria idêntico a um backup incremental. No entanto, na quarta-feira, o backup diferencial incluirá todos os dados que foram alterados desde segunda-feira (backup completo). A vantagem dos backups diferenciais sobre os incrementais consiste nos tempos de restauração mais curtos. A restauração de um backup diferencial nunca exige mais do que duas cópias. Obviamente, a desvantagem é que, ao longo do tempo, o backup diferencial pode crescer e conter muito mais dados que o backup incremental.



Fonte: EMC Information Storage and Management v3

Granularidade - resumo



Fonte: EMC Information Storage and Management v3

Para saber mais...

… consulte o livro Armazenamento e Gerenciamento de Informações - Como Armazenar, Gerenciar e Proteger Informações, da EMC Education Services.

FIM