

# Resolução de Problemas

Nesta capítulo, relacionaremos os principais elementos necessários para a resolução de problemas em uma rede.

- [Técnicas de Troubleshooting - Um pouco de teoria...](#)
- [Levantamento de indicadores](#)
- [Topologia](#)
- [Monitoramento](#)
- [Documentação de Rede - Atlas / Netbox](#)

# Técnicas de Troubleshooting

## - Um pouco de teoria...

### Definição

Troubleshooting é o conjunto de ações orientadas à resolução de problemas na infraestrutura de redes, computadores, sistemas ou serviços correlatos. O seu único propósito é o de sanar o problema, restaurando assim o bom funcionamento do equipamento, rede, sistema ou serviço afetado, preferencialmente em tempo hábil e sem causar distúrbios adicionais para os usuários no decorrer do processo.

O troubleshooting consiste de ações de **definição**, **análise**, **diagnóstico** e **reparo**, e fazendo isto devidamente com auxílio de processos, ferramentas e boas práticas.

### Roteiro recomendado de troubleshooting

Todo o processo é dividido em três fases primárias, denominadas **Problema**, **Diagnóstico** e **Solução**. Cada uma destas fases possui etapas, e cada uma destas etapas contém um conjunto de ações específicas para o tratamento e condução do suporte ao problema. O que será mostrado a seguir é uma expansão dos conceitos de cada fase.

- **Problema**

Nesta fase, o principal objetivo é a **definição do problema**. Como a dinâmica para surgimento de problemas envolve diversas possibilidades para cada caso, fica impraticável por muitas vezes corrigir um problema sem causar outros problemas, ou resolver o problema em tempo hábil. Uma coisa é certa: uma hora ou outra o problema será resolvido!

As questões aqui na verdade são:

**a) você conseguirá resolver o problema em tempo hábil, buscando minimizar os impactos para o negócio?**

**b) você conseguirá resolver o problema sem causar distúrbios adicionais (graves ou não) para o ambiente?**

Isto tudo pode ser evitado em grande parte através da correta definição do problema.

- **Diagnóstico**

Tão importante quanto definir o problema é saber diagnosticá-lo o mais precisamente possível. A proposta desta fase é ***conduzir diagnósticos efetivos*** alimentados pelas conclusões obtidas na fase "Problema" supracitada. Uma vez que você for capaz de compreender o problema com clareza (ou seja, defini-lo), você estará apto para iniciar o trabalho de coleta de informações e análises correspondentes com o intuito de identificar a causa-raiz e de completar o seu diagnóstico com maior clareza.

A qualidade da definição do problema impactará positiva ou negativamente o seu diagnóstico. Por onde começar o seu diagnóstico? Qual equipamento você acessará primeiro para coletar informações? Quais áreas funcionais da configuração e operação daquele equipamento deverão ser verificadas em primeira e segunda instâncias? Quais deverão ser as suas expectativas de comparação, contraste e constatação?

- **Solução**

Esta fase promoverá a correção do problema que:

**a) foi definido/compreendido corretamente,**

**b) foi analisado e diagnosticado corretamente.**

Na verdade, é mais que isso. Bem mais que isso. É resolver o problema com qualidade de ações, atitude e responsabilidade.

Esta fase constitui na correção do problema de forma mais cirúrgica, e não "*matar uma barata com bala de canhão*" como ocorre em muitos casos. Será nesta fase que você determinará o roteiro de correção do problema, as implicações e riscos associados com as manobras corretivas, ou seja, se a manobra de correção apresenta riscos de indisponibilidades parciais ou totais em caráter temporário, isto é, se haverá mais impacto ou não no ambiente para resolver aquele problema. E será nesta fase que você validará a necessidade de abertura de processo de Gestão de Mudança (GMUD) em caráter emergencial, se deverá haver um plano de comunicação com gestores e clientes, definir o plano de validação e *rollback*, dentre outras iniciativas.

## **Abordagem detalhada**

Com base nas 3 etapas iniciais, iremos detalhar estes parâmetros para uma abordagem estruturada de Troubleshooting, conforme a imagem abaixo:

[image-1608724099944.png](#)

## Etapas da fase "Problema"

A parte mais crítica do processo de resolução de problemas ("troubleshooting") é a condução de uma análise adequada com o objetivo de definição do problema. Algumas sugestões de ações cabíveis neste estágio são importantes:

### • Descrição do Problema ("título")

- Além de data e hora do surgimento do problema - quando o problema foi notado ou comunicado por usuários/clientes e/ou pela equipe de operação?

### • Escopo do Problema

- Quais serviços da rede estão sendo afetados? Por exemplo:
  - Wireless corporativo ou de convidados, acesso à Internet de usuários banda larga, acesso à Internet de usuários corporativos, acesso a websites ou serviços específicos, etc.
- Fator de indisponibilidade associado ao problema:
  - 100% indisponível?
  - Parcialmente indisponível?
  - Problema de natureza intermitente?
  - Lentidão apenas?
- Locais afetados pelo problema:
  - Prédios/sites, andares, departamentos/setores, sites, pops, e os usuários ou clientes espalhados nestes
  - Segmentos lógicos afetados, do conceito lógico do projeto
    - VLANs específicas? Subredes específicas? Servidores específicos? Aplicações específicas?
    - Perímetros específicos, tais como usuários autenticados em um BNG/BRAS específico, usuários de um anel Metro, usuários atendidos por um roteador PE específico, etc.

### • Análise temporal do problema

- Quando o problema surgiu pela primeira vez, isto é, quando a equipe de TI foi acionada?
- Algum analista estava realizando alguma configuração ou modificação em algum equipamento da rede?

- Há registros de mudanças recentes que coincidam com o surgimento do problema? (ex: revisão dos logs de TACACS+ ou registros internos de GMUD)
  - Caso afirmativo, qual é a probabilidade de relevância das alterações que foram realizadas com o problema reportado?
    - É factível considerar *rollback*, caso esta análise indique alta probabilidade.
- É um problema recorrente, ou seja, ocorre com alguma frequência em sua rede?
- Dentre outras iniciativas e questionamentos desta natureza.

Este pequeno roteiro embarca fatores tais como escopo *temporal + perímetro + qualitativo + quantitativo*, fomentando toda a lógica de análise preliminar e a devida compreensão do problema, ou seja, trazendo à tona todas as informações que você precisa saber para definir o problema! A qualidade das confirmações das situações e contextos acima ditará o seu grau de sucesso no troubleshooting nas etapas posteriores.

Isto é o que chamamos de **Abordagem de Troubleshooting Estruturado**.

## Etapas da fase "Diagnóstico"

Verifiquemos o roteiro esmiuçado e recomendado da fase Diagnóstico.

### Colete informações

Com a definição do problema realizada com êxito, aqui você buscará coletar as informações necessárias para promover um diagnóstico efetivo do problema. Os equipamentos que você deverá acessar e as respectivas áreas funcionais a serem inspecionadas, enfim, tudo isto dependerá das informações obtidas durante a definição do problema. Já neste estágio, você deverá saber quais tecnologias (protocolos, serviços) deverão ser verificadas e em quais equipamentos você deverá conduzir estas verificações inicialmente.

Aqui você analisará logs, processos, CPU, memória, filas, buffers, interfaces, VLANs, tabelas MAC, ARP cache, vizinhanças/adjacências de protocolos de roteamento, estruturas de dados dos protocolos de roteamento, tabela de roteamento, ACLs, policieis de BGP ou IGP, NAT, e tantos outros, mas tudo aquilo e **somente** os componentes que tiverem relação ou conexão parcial ou total com a definição do problema.

### Análise as informações coletadas

Na medida em que a coleta de informações vai desenrolando-se, você deverá traçar uma estratégia de análise para cada componente inspecionado. Em outras palavras, saber exatamente o que olhar e o que verificar em cada situação coletada. Isto inclui estado das interfaces, erros nas interfaces, configuração das interfaces (endereços IP, MTU, etc.), configurações e estados VLAN/802.1Q/STP/etc., configurações e estados de protocolos de roteamento (métricas, áreas, autenticações, políticas, filtros, adjacências, etc.), rotas na tabela de roteamento, serviços diversos e que por ventura se façam presentes (ex: port security, DHCP Snooping, DAI, IPSG, IP SLA, PBR, PPPoE, NAT, QoS/policy, o que for.. etc.), e assim por diante.

Obviamente isto exigirá bons conhecimentos sobre cada uma das tecnologias mantidas nas coletas que você realizou, como elas funcionam, como interagem, e quais são os requisitos de integração de cada uma destas tecnologias.

## Elimine hipóteses

Das informações que você coletou, e após efetuar as análises preliminares, você deverá saber identificar o que certamente não contribui para o problema, ou o que não promoveu participação para o surgimento do problema.

O foco é o seguinte: tudo o que não for relacionado ao problema deverá ser desconsiderado.

A ideia aqui é fazer você ir ao campo de batalha com as armas necessárias apenas e com, no máximo, 3 possibilidades de ações visando a correção do problema. Além de levar muito mais tempo, é pouco efetivo, confunde, e pode causar outros e indesejáveis problemas, além de estresse emocional. Procure ser cirúrgico na hora de eliminar possibilidades, pois não adianta você encaminhar "10 possibilidades" para a fase de solução!

## Etapas da fase "Solução"

Verifiquemos o roteiro esmiuçado e recomendado da fase Solução.

### Proponha hipóteses

Em muitos casos você pode ter sido muito eficiente ou ter tido sorte, pois o problema foi fácil de diagnosticar! Isto é, você definiu bem o problema, fez as análises devidas, e, num piscar de olhos, conseguiu identificar a causa-raiz do problema!

No entanto, em muitos casos, poderão restar dúvidas, pois o diagnóstico do problema em questão talvez possa ser mais complexo e exigir mais conhecimentos por parte do analista, mas que, mesmo assim, você acredita que o problema esteja relacionado a duas ou três possibilidades, cujas interpretações são decorrentes da análise de informações e eliminação de hipóteses. Neste caso, a sugestão aqui é a de propor as hipóteses restantes devidamente classificadas por fidelidade (com o problema) versus o risco e esforço de implementação da correção.

Por exemplo, você tem duas hipóteses para resolver um determinado problema: uma delas, aparentemente a mais óbvia de ser o problema, mas que você não tem muita certeza ainda, exige uma manobra que provocará algum distúrbio na rede, tipo uma indisponibilidade. Já a segunda hipótese, menos provável de ser o problema, exige uma manobra corretiva mais rápida e que ainda apresenta zero risco para o negócio. Em razão disto, você poderá optar por aplicar a hipótese #2 e, caso não dê certo, fazer o *rollback*, e agendar a manobra necessária para a execução da hipótese #1, seja em caráter emergencial ou em horário apropriado, dependendo da urgência para o saneamento do problema no seu caso.

### Testar hipóteses

É exatamente aqui que você conduzirá as ações especificamente corretivas. Não saia mexendo em vários componentes de uma vez só! Seja organizado e tenha o controle absoluto da situação. Isto significa que você deverá implementar uma única ação corretiva (hipótese) por vez, sabendo que, em muitos casos, uma única hipótese poderá exigir a intervenção de uma ou mais tecnologias e em um ou mais equipamentos. Execute o procedimento com cautela, e faça as validações devidas para confirmar a correção do problema. Certifique-se que a manobra não tenha causado outros problemas (as vezes resolve “aquele” problema, mas pode afetar outras coisas na rede).

Não funcionou? Desfaça a alteração e implemente a próxima hipótese, ou, caso o problema não tenha sido corrigido, mas a correção (que não deu certo) é necessária mesmo assim, talvez esteja faltando conhecimentos para resolver o problema ou que talvez algum componente adicional tenha ficado de fora. Ou você (talvez) não tenha sido eficiente durante a coleta e análise de informações.

É a parte mais difícil de todo o processo de suporte, por isto que insisto que você seja bem efetivo nos estágios anteriores, justamente para atenuar a complexidade de compreensão, diagnóstico e correção do problema aqui, neste estágio.

## Problema Resolvido

Aqui você celebrará a resolução do problema! Aliás, não somente isto, aproveite a oportunidade para **documentar o problema e a solução empregada**, e fazendo isto em uma base de conhecimentos que poderá servir para capacitar os times de suporte para que o problema em questão possa ser evitado futuramente, ou, caso haja nova ocorrência, ter a solução ou correção implementada em menor prazo e esforço.

## Referência:

[Abordagens para o Troubleshooting Eficaz de Problemas Típicos na Rede do ISP](#)

# Levantamento de indicadores

Durante a tratativa de um problema, o primeiro e mais importante passo é o levantamento de indícios que permitam a identificação do problema.

Esses indicadores podem ser métricas ou registros de eventos (logs).

## Métricas

As métricas são valores de referência em um determinado sistema (Ex.: Uso de CPU, número de acessos a página, etc). Estes valores podem ser registrados através de sistemas de monitoramento de rede (NMS), como Zabbix, LibreNMS, Cacti, etc.

## Registro de Eventos (Logs)

Os Logs são registros de eventos ocorridos em uma determinada aplicação ou sistema operacional. Estes logs podem ser encontrados em um local padrão (Ex.: /var/log, no caso do Linux) ou em locais especificados na configuração da aplicação.

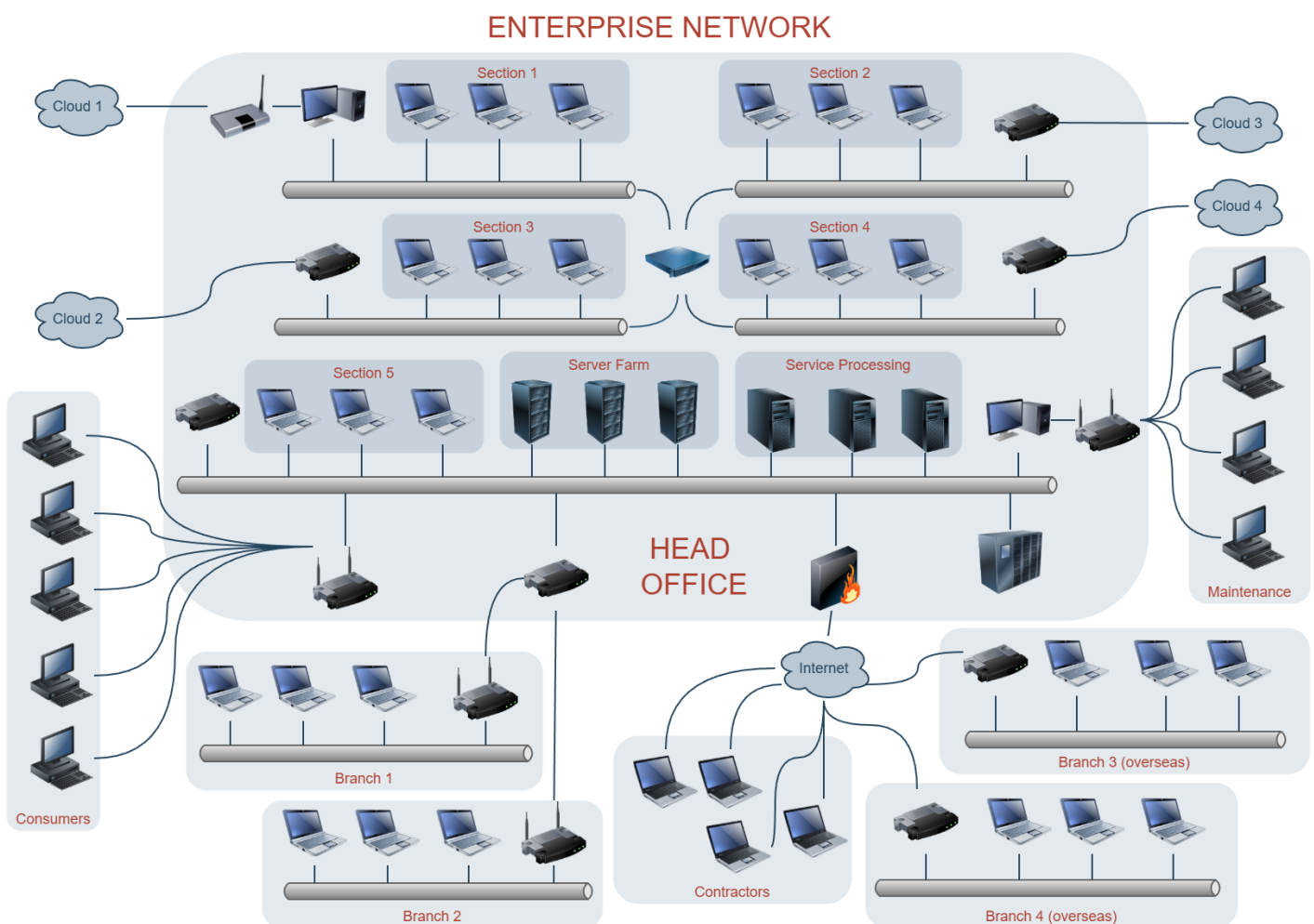
# Topologia

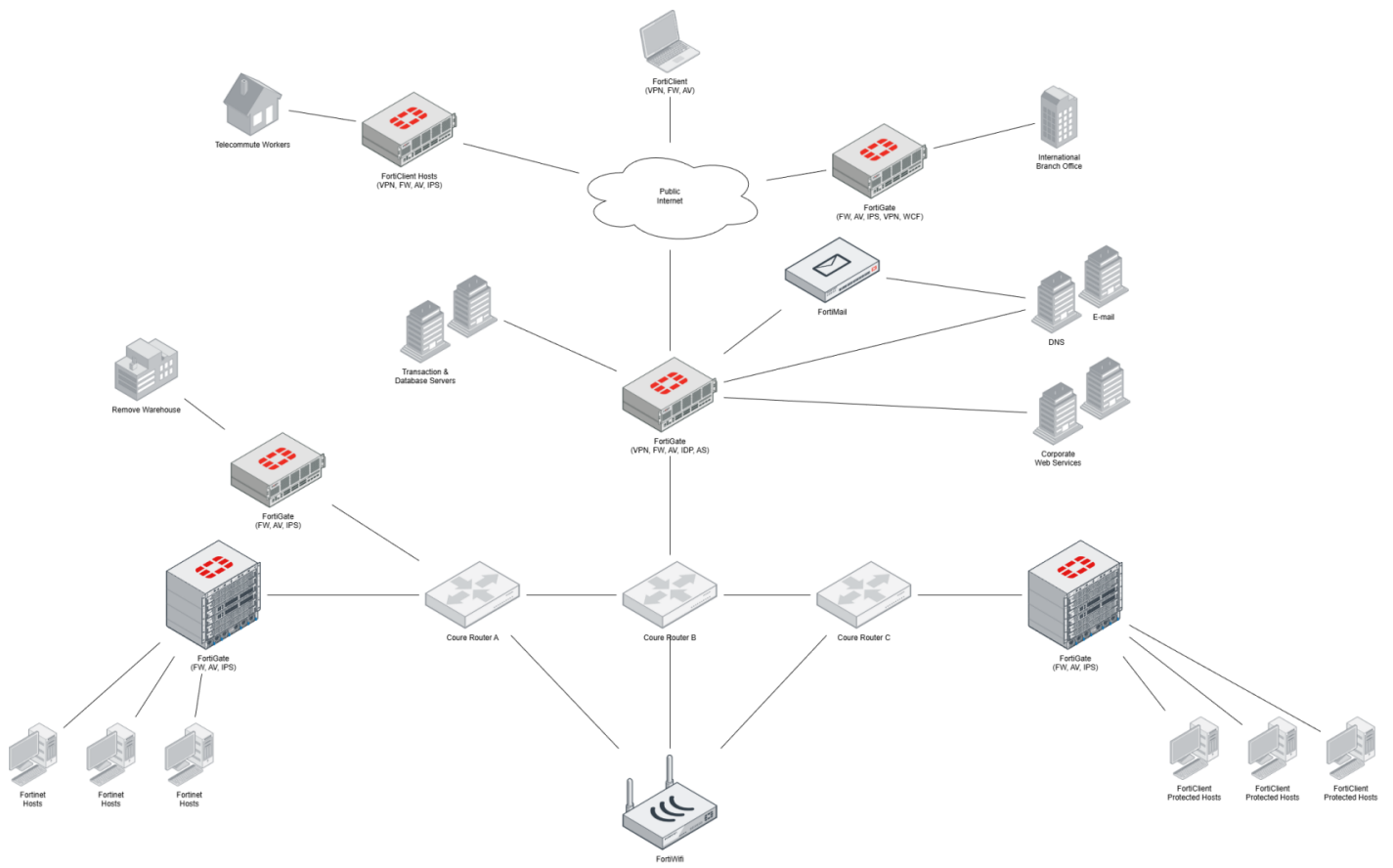
O desenho da topologia de uma rede tem por objetivo criar um modelo visual da rede lógica da instituição.

Esta topologia permite as envolvidos em uma tratativa o alinhamento claro das ideias discutidas, e identificação de possíveis pontos de falha em uma rede.

Estes desenhos pode ser realizados em aplicações diversas, como: DIA UML, DrawIO, etc.

Abaixo colocamos o exemplo de 2 modelos presentes no DrawIO.





# Monitoramento

# Documentação de Rede - Atlas / Netbox

## Sumário

1. [Por quê documentar?](#)
  2. [O que é o NetBox](#)
  3. [Acesso ao Sistema](#)
  4. [Navegação Básica](#)
  5. [Conceitos Importantes](#)
  6. [O Tenant e as Permissões](#)
  7. [Cadastro de Objetos por Módulo](#)
  8. [Boas Práticas para os Campi](#)
  9. [Consultas e Filtros](#)
  10. [Erros Comuns](#)
- 

## 1. Por quê documentar?

A documentação da rede é uma etapa fundamental para a perenidade de sua rede, uma vez que esta documentação favorece a análise e resolução de problemas.

Durante os anos a documentação da rede do IFSP passou por estágios de maturação, saindo da documentação da rede em planilhas e posteriormente em aplicações web específicas para este fim (Ex.: Racktables, Hub e Netbox).

Atualmente a aplicação responsável por manter a uma documentação fidedigna da rede do IFSP é o Netbox, disponível na URL <https://atlas.ifsp.edu.br>.

## 2. O que é o NetBox

O NetBox é uma [aplicação web](#) desenvolvida com o objetivo de funcionar como a **fonte de verdade** (Source of Truth) para:

- Endereçamento IP (prefixos, IPs, VRFs)
- Dispositivos de rede (switches, firewalls, APs, servidores)
- Racks e localização física
- Circuitos e provedores de internet
- VLANs
- Máquinas virtuais

Uma boa referencia, mostrando o Netbox desde a instalação até o seu uso foi apresentada na [Semana de Capacitação do Nic.br](#).

“ **Regra de ouro:** Se está na rede, deve estar documentado no NetBox.

## 3. Acesso ao Sistema

### URL

<https://atlas.ifsp.edu.br>

The screenshot displays the NetBox web interface. On the left is a dark sidebar with a navigation menu including 'Organização', 'SITES', 'Regiões', 'Grupos de Sites', 'Locais', 'LOCAÇÃO', 'Inquilinos', 'Grupos de Inquilinos', 'CONTATOS', 'Contatos', 'Grupos de Contatos', 'Funções dos Contatos', 'Atribuições dos Contatos', 'Racks', 'Dispositivos', 'Conexões', 'Wireless', 'IPAM', 'VPN', 'Virtualização', 'Circuitos', and 'Alimentação Elétrica'. The main content area shows the configuration for a site named 'Reitoria' under the 'São Paulo' region. The site is active and located at 'R. Pedro Vicente, 625'. It has 23 devices, 1 group of VLANs, 3 localities, 1 virtual machine, 23 prefixes, 2 racks, and 1 circuit termination. A table at the bottom shows storage usage: 0 installed, 0 stored, and 0 total assets. The user 'geraldojunior' is logged in as Administrator.

# Login

- Utilize seu **e-mail institucional** através do OAuth do Google.
- Cada usuário é associado à **CTI** do seu campus, a qual possui permissões restritas ao seu escopo.

## Permissões

O usuário só pode **criar, visualizar e alterar** objetos que estejam associados ao **Tenant do seu campus**. Por isso, ao cadastrar qualquer objeto no NetBox, é **obrigatório** selecionar o Tenant correto.

“ **Exemplo:** Usuários da CTI do campus "Reitoria" só podem editar objetos cujo Tenant seja "Reitoria" (slug `ret` ).

## 4. Navegação Básica

### Menu Principal

Menu	O que contém
<b>Organization</b>	Sites, Tenants, Contacts
<b>Devices</b>	Devices, Racks, Device Types, Manufacturers
<b>Connections</b>	Cables, Interfaces
<b>IPAM</b>	Prefixes, IPs, VLANs, VRFs, ASNs
<b>Circuits</b>	Providers, Circuits
<b>Virtualization</b>	VMs, Clusters

### Barra de Pesquisa

Use a barra de pesquisa global (topo da tela) para encontrar qualquer objeto por nome, IP ou identificador.

# Filtros

Cada listagem possui filtros laterais. Use-os para localizar objetos do seu campus (filtre por **Site**, **Tenant** ou **Tag**).

---

## 5. Conceitos Importantes

### Hierarquia Física

Region → Site → Location → Rack → Device

Conceito	No IFSP
<b>Region</b>	Estado de São Paulo
<b>Site</b>	Campus (ex: Campus Reitoria)
<b>Location</b>	Sala/Andar (ex: Sala de Telecom Bloco A)
<b>Rack</b>	Rack físico (ex: Rack-01)
<b>Device</b>	Equipamento (ex: SW-CORE-RET-01)

### Hierarquia Lógica (IPAM)

VRF → Prefix → IP Address

VLAN Group → VLAN

### Tenant (Inquilino)

Identifica **quem é responsável** por um recurso. No nosso caso, cada campus é um tenant.

### Tag

Etiqueta para classificação adicional. Usamos tags com a sigla do campus (ex: **ARQ**, **BRT**, **CMP**).

---

# 6. O Tenant e as Permissões

## Como funciona o controle de acesso

No Atlas (NetBox do IFSP), as permissões de cada equipe são controladas pelo **Tenant** (inquilino). Cada campus possui um Tenant próprio, e o sistema utiliza o filtro `tenant__slug` nas regras de permissão para determinar o que cada usuário pode ver e editar.

```
Constraint de permissão: { "tenant__slug": "ret" }
```

Isso significa que o usuário do campus RET só consegue visualizar e modificar objetos cujo Tenant tenha o slug `ret`.

“ **Resumindo:** Se um objeto não estiver associado ao Tenant do seu campus, você **não terá acesso** a ele.

Ao cadastrar **qualquer objeto** no NetBox (device, rack, prefix, IP, VLAN, etc.), **obrigatoriamente selecione o Tenant do seu campus**. Se o campo Tenant ficar vazio ou com valor incorreto:

- Você poderá perder acesso ao objeto após salvar
- Outros membros da sua equipe não conseguirão visualizá-lo
- A equipe central (CAOTI) precisará intervir para corrigir

**REGRA FUNDAMENTAL:** Sempre preencha o Tenant

## O que é o Slug do Tenant?

O **slug** é o identificador interno do Tenant. Ele é definido em letras minúsculas, sem espaços ou acentos. Os slugs já estão configurados para cada campus — você **não precisa criá-los**, apenas **selecionar o Tenant correto** na lista suspensa ao cadastrar objetos.

### Exemplo:

Tenant (nome exibido)	Slug (usado nas permissões)
Araraquara	`arq`
Barretos	`brt`

Tenant (nome exibido)	Slug (usado nas permissões)
Campinas	`cmp`

## Regras do Slug (para referência)

Regra	Exemplo Correto	Exemplo Errado
Somente letras minúsculas	`arq`	`ARQ`
Sem espaços (use hífen)	`brt-a`	`brt a`
Sem acentos	`hortolandia`	`hortolândia`
Sem caracteres especiais	`brt-a`	`brt/a`

## Na prática: como garantir que o Tenant está correto

1. Ao criar ou editar qualquer objeto, localize o campo **Tenant**
2. Selecione o nome do seu campus na lista suspensa
3. Se o campo já estiver preenchido com o Tenant correto, não altere
4. **Nunca** selecione o Tenant de outro campus

## Onde o Tenant deve ser preenchido

O campo Tenant está presente nos seguintes objetos:

- **Devices** (equipamentos)
  - **Racks**
  - **Sites**
  - **Prefixes** (redes IP)
  - **IP Addresses**
  - **VLANS**
  - **VLAN Groups**
  - **Circuits**
  - **Virtual Machines**
  - **Clusters**
-

# 7. Cadastro de Objetos por Módulo

## 7.1 Devices (Equipamentos)

**Caminho:** Devices → Devices → + Add

Campo	Descrição	Exemplo
Name	Nome do equipamento (padrão de nomenclatura)	`SW-CORE-RET-01`
Device Role	Função do equipamento	Switch
Device Type	Modelo exato	Extreme X460-G2-48p
Site	Seu campus	Campus Reitoria (RET)
Location	Sala onde está	Telecom Bloco A
Rack	Rack onde está montado	Rack-01
Position	Posição U no rack (de baixo para cima)	20
Tenant	Seu campus	Reitoria
Tags	Adicione a tag do campus	RET

## 7.2 Racks

**Caminho:** Devices → Racks → + Add

Campo	Descrição	Exemplo
Name	Identificação do rack	Rack-01
Site	Seu campus	Campus Reitoria (RET)
Location	Sala	Telecom Bloco A
Height	Altura em U	42
Tenant	Seu campus	Reitoria
Tags	Sigla do campus	RET

## 7.3 Prefixes (Redes IP)

**Caminho:** IPAM → Prefixes → + Add

Campo	Descrição	Exemplo
Prefix	Rede no formato CIDR	10.100.10.0/24
VRF	Virtual Routing (veja tabela abaixo)	Rede Intracampus
Tenant	Seu campus	Reitoria
Site	Seu campus	Reitoria (RET)
Status	Estado atual	Active
Description	Descrição da rede	VLAN 10 - Administrativo
Tags	Sigla do campus	RET

**VRFs disponíveis:**

VRF	Quando usar
Rede Intracampus	Redes internas do campus (10.x.x.x)
RNP	IPs fornecidos pela RNP (200.133.x.x)
WAN-[Provedor]	IPs de link do provedor
ASN-BGP	Blocos BGP do IFSP (não editar sem autorização)
AWS	VPCs na AWS (não editar sem autorização)

## 7.4 IP Addresses

**Caminho:** IPAM → IP Addresses → + Add

Campo	Descrição	Exemplo
Address	IP com máscara CIDR	10.100.50.1/24
VRF	Mesmo VRF do prefix pai	Rede Intracampus
Status	Active, Reserved, Deprecated	Active
DNS Name	FQDN se houver	fw-ret.ifsp.edu.br
Description	O que usa esse IP	Gateway VLAN Servidores

Campo	Descrição	Exemplo
Tenant	Seu campus	Reitoria
Tags	Sigla	RET
Assigned to	Interface do device (se aplicável)	—

## 7.5 VLANs

**Caminho:** IPAM → VLANs → + Add

Campo	Descrição	Exemplo
VLAN ID	Número da VLAN	10
Name	Nome descritivo	Administrativo
VLAN Group	Grupo do campus	RET
Site	Seu campus	Campus Reitoria (RET)
Tenant	Seu campus	Reitoria
Status	Active	Active
Tags	Sigla	RET

## 7.6 Cables (Cabeamento)

**Caminho:** Vá até a interface do device → clique em "Connect"

Campo	Descrição	Exemplo
Type	Tipo do cabo	CAT6a, SMF (fibra monomodo)
A Side	Interface de origem	SW-CORE-RET-01 → GigE 0/1
B Side	Interface de destino	FW-RET-01 → Port1
Status	Connected	Connected
Length	Comprimento (opcional)	3m

## 8. Boas Práticas para os Campi

# Nomenclatura de Devices

Use o padrão:

[TIPO] - [FUNÇÃO] - [CAMPUS] - [NÚMERO]

Tipo	Exemplos
SW	SW-CORE-PEP-01, SW-ACESSO-PEP-02
FW	FW-RET-01
AP	AP-RET-BLOCO-A-01
SRV	SRV-RET-01

## Checklist ao Cadastrar um Novo Equipamento

- Verificar se o Device Type já existe (não criar duplicado)
- Preencher Site, Location, Rack e Position
- Atribuir Tenant do campus
- Adicionar Tag com a sigla do campus
- Cadastrar as interfaces (se não vieram com o device type)
- Documentar IPs de gerência
- Conectar cabos entre interfaces

## Checklist ao Documentar uma Nova Rede

- Criar o Prefix no VRF correto
- Associar ao Tenant/Site do campus
- Criar a VLAN correspondente no VLAN Group do campus
- Cadastrar IPs relevantes (gateways, servidores)
- Adicionar Tag do campus

## O que NÃO fazer

- Não editar objetos de outros campi

- Não criar Device Types duplicados (pesquise antes)
  - Não alterar VRFs, ASNs ou Aggregates (solicite ao CAOTI/NTI)
  - Não deixar campos obrigatórios em branco
  - Não usar slugs com letras maiúsculas ou caracteres especiais
- 

## 9. Consultas e Filtros

### Encontrar todos os dispositivos do meu campus

1. Vá em **Devices** → **Devices**
2. No filtro lateral, selecione **Site** = seu campus
3. Ou filtre por **Tag** = sigla do campus

### Encontrar IPs disponíveis numa rede

1. Vá em **IPAM** → **Prefixes**
2. Clique no prefix desejado
3. Clique na aba **IP Addresses**
4. Os IPs livres serão mostrados com status "Available"

## Exportar dados

1. Em qualquer listagem, clique no botão **Export** (canto superior direito)
2. Escolha o formato: CSV, JSON ou YAML

## Usar a API

O NetBox possui uma API REST completa:

```
https://atlas.ifsp.edu.br/api/
```

Documentação interativa (Swagger):

```
https://atlas.ifsp.edu.br/api/docs/
```

---

# 10. Erros Comuns

Erro	Causa	Solução
"A device with this name already exists"	Nome duplicado no mesmo site	Verifique se o device já foi cadastrado
"Duplicate IP address"	IP já cadastrado naquele VRF	Consulte quem está usando o IP
"This field is required"	Campo obrigatório vazio	Preencha todos os campos marcados com \*
"Invalid slug"	Slug com caracteres inválidos	Use apenas letras minúsculas, números e hífens
"Object not found" / Sem permissão	Tenant incorreto ou ausente no objeto	Edite o objeto e selecione o Tenant correto do seu campus
Não consigo ver meus objetos	Faltou o Tenant correto	Peça ao CAOTI/NTI para associar o Tenant ao objeto
Objeto sumiu após salvar	Salvou sem Tenant ou com Tenant errado	Contate o CAOTI/NTI para corrigir

---

## Suporte

Em caso de dúvidas ou problemas de acesso:

- **E-mail:** Contate a equipe CAOTI
- **Documentação oficial:** <https://netboxlabs.com/docs/netbox/>
- **API Docs:** <https://atlas.ifsp.edu.br/api/docs/>
- **Referencia:** [Semana de Capacitação Nic.br - Curso - Gerenciando a infraestrutura de maneira organizada com Netbox](#)

---

*Documento elaborado pela equipe da CAOTI / DTI - IFSP com apoio de IA (Sonet 4.5)*