

3 Descoberta de baixo nível (LLD)

Visão geral

O processo de LLD fornece uma forma automática de criar itens, triggers, gráficos para os diferentes objetos descobertos no dispositivo monitorado. Por exemplo, o Zabbix pode começar automaticamente a monitorar os sistemas de arquivo ou interfaces de rede de um servidor, sem precisar que sejam criados manualmente itens para cada um deles. Adicionalmente, o Zabbix também pode remove-los automaticamente também após determinado período consecutivo em que eles não sejam mais encontrados.

Nativamente no Zabbix, são suportados seis tipos de LLD:

- descoberta de sistemas de arquivo;
- descoberta de interfaces de rede;
- descoberta de CPUs seus núcleos;
- descoberta de árvores de OID SNMP;acesse
- descoberta usando consultas SQL/ODBC;
- descoberta de serviços Windows.

O usuário pode estender estas descobertas através de seus próprios scripts, contando que estes forneçam o dado em um formato em particular usando o protocolo JSON.

A arquitetura geral do processo de descoberto pode ser definido assim:

- Primeiro um usuário cria uma regra de descoberta em *Configuração → Templates* ou *Configuração → Hosts* e clica no link *Descoberta* da linha do host/template que se desejar. A configuração de um LLD pode ser separada em duas fases:
 - Definição de um item capaz de descobrir os elementos de configuração de interesse (por exemplo, sistemas de arquivo ou interfaces de rede);
 - Definição dos protótipos de itens, triggers e gráficos que poderão ser criados dinamicamente usando as informações descobertas.

Um item que descobre os elementos necessários é como qualquer outro item: O Zabbix solicita ao Zabbix Agent (ou através de qualquer outro tipo de item) um valor para o item, e o agente responde com um valor textual. A diferença aqui é que o valor contém uma lista de elementos descobertos no formato JSON. Enquanto os detalhes deste formato são importantes somente para quem for implementar uma regra customizada de descoberta, é necessário que se saiba que o valor retornado conterá uma lista de pares no padrão *macro → valor*. Por exemplo, o item `net.if.discovery` pode retornar dois pares: `"{#IFNAME}" → "lo"` e `"{#IFNAME}" → "eth0"`.

Os itens de LLD `"vfs.fs.discovery"`, `"net.if.discovery"` e a descoberta de OIDs SNMP são suportados desde o Zabbix 2.0.

O item `"system.cpu.discovery"` desde o Zabbix 2.4.

A descoberta através de `"queries SQL ODBC"` desde o Zabbix 3.0.

Os valores de retorno de um LLD são limitados a 2048 bytes no Zabbix Proxy rodando com o BD IBM DB2. Este limite não se aplica ao Zabbix Server pois os valores são processados sem precisarem de armazenamento prévio.

As macros usadas nos nomes, chaves e outros campos de protótipos serão substituídas pelos seus valores descobertos quando as entidades reais (itens, triggers, gráficos, ou até mesmo outros hosts)

forem criados. Consulte a lista completa de [opções](#) para as macros LLD.

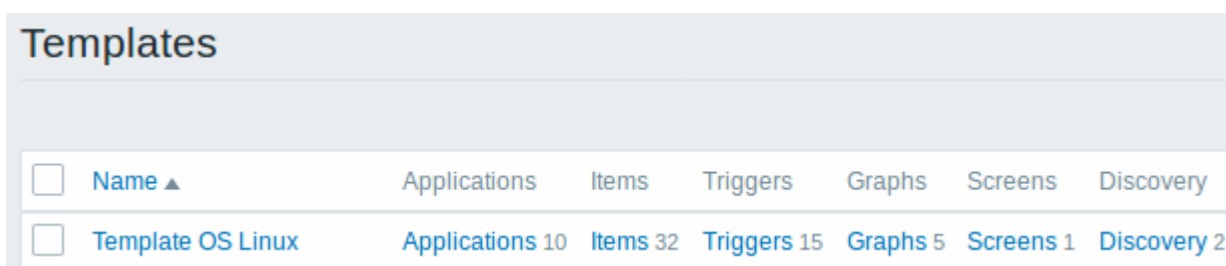
Quando o Zabbix Server recebe um valor de um item de descoberta, ele consulta os pares *macro* → *valor* para criar as entidades, conforme protótipos definidos na regra. No exemplo anterior, com o “net.if.discovery”, o Zabbix Server irá criar um conjunto de itens, triggers e graphs para a interface de 'loopback' e outro para a interface “eth0”.

As próximas seções vão demonstrar o processo em detalhes e servem como um “how-to” para configurar todos os tipos de descoberta antes citados. A última seção descreve o formato JSON para itens de descoberta e provê um exemplo de como implementar a sua própria regra de descoberta de sistema de arquivos usando um script Perl.

3.1 Descoberta de sistemas de arquivos

Para descobrir um sistema de arquivos:

- Acesse *Configuração* → *Templates*
- Clique no link *Descoberta* da linha apropriada



<input type="checkbox"/>	Name ▲	Applications	Items	Triggers	Graphs	Screens	Discovery
<input type="checkbox"/>	Template OS Linux	Applications 10	Items 32	Triggers 15	Graphs 5	Screens 1	Discovery 2

- Clique no botão *Criar regra de descoberta* situado no canto direito da barra de título
- Preencha o formulário com os detalhes necessários

A aba **Regra de descoberta** contém atributos gerais da regra de descoberta (do item de descoberta):

Discovery rule
Filters

Name

Type

Key

Update interval

Custom intervals

Type	Interval	Period
Flexible Scheduling	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>

[Add](#)

Keep lost resources period

Description

Discovery of file systems of different types as defined in global regular expression "File systems for discovery".

Enabled

Add
Cancel

Parâmetro	Descrição
<i>Nome</i>	Nome da regra de descoberta.
<i>Tipo</i>	Tipo da verificação a ser executada; pode ser <i>Agente Zabbix (passivo)</i> ou <i>Agente Zabbix (ativo)</i> neste caso.
<i>Chave</i>	Um item com a chave "vfs.fs.discovery" foi desenvolvido no Zabbix Agent para permitir a descoberta de sistemas de arquivos em várias plataformas (consulte a lista de itens suportados), e retorna um JSON com a lista de sistemas de arquivos e seus tipos.
<i>Intervalo de atualização (em seg)</i>	Este campo define de quanto em quanto tempo o Zabbix irá executar a descoberta. No início, quando você está configurando a regra de descoberta, pode ser interessante definir um intervalo curto, mas uma vez que você tenha confiança que sua regra está buscando o que você precisa, modifique o tempo para, no mínimo, 30 minutos. Esta recomendação se deve ao fato que os sistemas de arquivo não mudam tanto assim. <i>Nota:</i> Se você definir o intervalo de atualização com o valor '0', a coleta do item não será agendada, entretanto, se você também definir um intervalo flexível, o item será coletado somente nos momentos definidos no intervalo flexível.
<i>Intervalo customizado</i>	Você pode criar regras customizadas de coleta para o item: Flexível - cria uma exceção ao <i>Intervalo de atualização</i> (intervalo com frequência diferenciada) Agendamento - cria um agendamento de coleta. Para maiores detalhes consulte o manual de Intervalos customizados . Agendamento é suportado desde o Zabbix 3.0.0.

Parâmetro	Descrição
<i>Manter dados de recursos perdidos por (em dias)</i>	Este campo define por quantos dias serão mantidos os recursos que foram descobertos em algum momento e deixaram de ser percebidos (máximo 3650 dias). <i>Nota:</i> Se for definido como "0" as entidades criadas com base nestes recursos serão imediatamente excluídas. O uso do valor "0" não é recomendado pois erros de edição em filtros poderão fazer com que todas as entidades criadas dinamicamente e os dados históricos coletados sejam apagados.
<i>Descrição</i>	Descrição da regra.
<i>Ativo</i>	Se marcado, a regra será processada.

A aba **Filtros** contém as definições de filtros a serem aplicados após a coleta do item de descoberta e antes da criação das entidades:

Parâmetro	Descrição
<i>Tipo do cálculo</i>	As seguintes opções podem ser utilizadas para aplicar os filtros em cada valor constante na lista descoberta: E - deve ser compatível com todos os filtros; Ou - suficiente se passar em um dos filtros; E/Ou - usa <i>E</i> com nomes de macro diferentes e <i>Ou</i> em macros com o mesmo nome; Expressão personalizada - oferece a possibilidade de definir forma customizada de cálculo dos filtros. A fórmula deverá conter todos os filtros na lista. Limitado à 255 símbolos.

Parâmetro	Descrição
<i>Filtros</i>	<p>Um filtro pode ser usado para gerar itens, triggers e gráficos apenas para determinados sistemas de arquivos. O filtro deverá seguir o padrão POSIX estendido de expressões regulares. Por exemplo, se você estiver interessado somente nos drives: C:, D:, e E:, você pode preencher o campo <i>Macro</i> com o valor <code>{#FSNAME}</code> e o campo <i>Expressão regular</i> com o valor <code>"^C ^D ^E"</code>. Também é possível filtrar usando outra macro, a <code>{#FSTYPE}</code> (ex. <code>"^ext ^reiserfs"</code>) e tipos de drives (apenas no Windows) usando a macro <code>{#FSDRIVETYPE}</code> (ex. <code>"fixed"</code>).</p> <p>Você pode informar uma expressão regular diretamente ou usar uma expressão regular global.</p> <p>Para testar a expressão uma expressão regular você pode utilizar o comando "grep -E", por exemplo:</p> <pre>for f in ext2 nfs reiserfs smbfs; do echo \$f grep -E '^ext ^reiserfs' echo "SKIP: \$f"; done</pre> <p>A macro <code>{#FSDRIVETYPE}</code> no Windows é suportada desde o Zabbix 3.0.0. A definição de vários filtros é suportada desde o Zabbix 2.4.0.</p> <p>Observe que se alguma macro definida no filtro estiver ausente, o recurso em questão será ignorado.</p>

O BD do Zabbix em MySQL precisa ser criado de forma sensível ao caso se os nomes de sistemas de arquivo puderem ser diferenciados apenas pelo caso, senão a regra de descoberta poderá não funcionar.

O histórico das coletas da regra de descoberta não é preservada.

Uma vez que uma regra tenha sido criada, vá para use o link *Protótipos de item*, disponível na lista de regras de descoberta do host/template, e clique no botão *Criar protótipo de item*. Observe que a macro `{#FSNAME}` será utilizada aqui, seu uso neste é obrigatório, pois cada item a ser criado deverá ser diferente do item criado anteriormente.

Item prototype [Preprocessing](#)

Name

Type

Key

Type of information

Units

Update interval

Custom intervals

Type	Interval	Period
<input checked="" type="checkbox"/> Flexible	<input type="text" value="Scheduling"/>	<input type="text" value="50s"/>
		<input type="text" value="1-7,00:00-24:00"/>

[Add](#)

History storage period

Trend storage period

Show value [show value mappings](#)

New application

Applications

- None-
- CPU
- Filesystems
- General
- Memory
- Network interfaces
- OS
- Performance
- Processes
- Security

New application prototype

Application prototypes

- None-

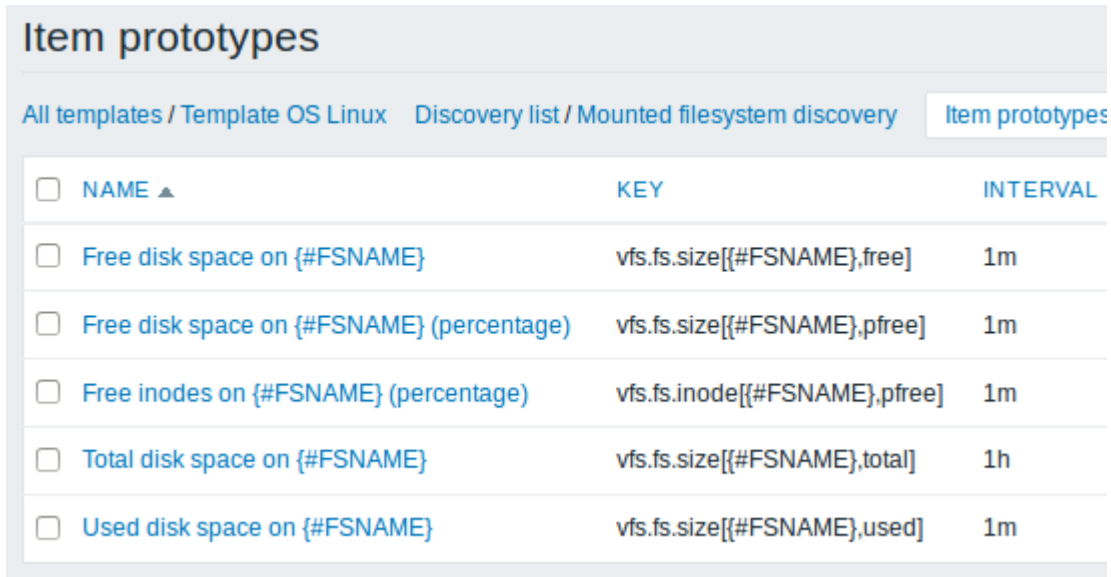
Description

Create enabled

Se um protótipo de item for criado com o status *Inativo*, os itens continuarão a ser criados a partir dele mas estarão com o status *Inativo* também.

O campo *Protótipo de aplicação* é uma opção disponível especificamente nos protótipos de itens. Um protótipo de aplicação permite que você crie dinamicamente as aplicações e as associe aos itens. Consulte mais nas [notas sobre descoberta de aplicações](#).

Nós podemos criar vários protótipos de item para cada métrica de sistema de arquivo que nos interesse:



The screenshot shows the 'Item prototypes' section in Zabbix. It features a breadcrumb trail: 'All templates / Template OS Linux / Discovery list / Mounted filesystem discovery / Item prototypes'. Below this is a table with three columns: 'NAME', 'KEY', and 'INTERVAL'. Each row represents a different item prototype for disk space metrics, with a checkbox in the 'NAME' column.

<input type="checkbox"/> NAME ▲	KEY	INTERVAL
<input type="checkbox"/> Free disk space on {#FSNAME}	vfs.fs.size[{#FSNAME},free]	1m
<input type="checkbox"/> Free disk space on {#FSNAME} (percentage)	vfs.fs.size[{#FSNAME},pfree]	1m
<input type="checkbox"/> Free inodes on {#FSNAME} (percentage)	vfs.fs.inode[{#FSNAME},pfree]	1m
<input type="checkbox"/> Total disk space on {#FSNAME}	vfs.fs.size[{#FSNAME},total]	1h
<input type="checkbox"/> Used disk space on {#FSNAME}	vfs.fs.size[{#FSNAME},used]	1m

Então, criamos protótipos de trigger de forma similar:

Trigger prototype [Dependencies](#)

Name

Severity Not classified Information Warning Average High Critical

Expression

[Expression constructor](#)

OK event generation Expression Recovery expression None

PROBLEM event generation mode Single Multiple

OK event closes All problems All problems if tag values match

Tags

tag	value
<input type="text"/>	<input type="text"/>

[Add](#)

Allow manual close

URL

Description

Create enabled

Você pode definir [dependências](#) entre protótipos de trigger também (suportado desde o Zabbix 3.0). Para fazer isso, acesse a **Dependências**. Um protótipo de trigger poderá depender de outro protótipo de trigger da mesma regra de descoberta ou de outra trigger normal. Não é possível criar relações de dependência entre protótipos de trigger de diferentes regras de descoberta. Um protótipo de trigger em nível de host não poderá depender de uma trigger em nível de template.

Trigger prototypes

[All templates / Template OS Linux](#) [Discovery list / Mounted filesystem discovery](#) [Item prototypes 5](#)

<input type="checkbox"/>	SEVERITY	NAME ▲	EXPRESSION
<input type="checkbox"/>	Warning	Free disk space is less than 20% on volume {#FSNAME}	{Template OS
<input type="checkbox"/>	Warning	Free inodes is less than 20% on volume {#FSNAME}	{Template OS

Nós podemos criar protótipos de gráfico também:

Graph prototype

[Preview](#)

Name

Width

Height

Graph type

Show legend

3D view

Items	Name	Type
⋮	1: Template OS Linux: Total disk space on {#FSNAME}	Graph
⋮	2: Template OS Linux: Free disk space on {#FSNAME}	Simple

[Add](#) [Add prototype](#)

Graph prototypes

[All templates / Template OS Linux](#) [Discovery list / Mounted filesystem discovery](#) [Item prototypes 5](#)

<input type="checkbox"/>	NAME ▲	WIDTH
<input type="checkbox"/>	Disk space usage {#FSNAME}	600

Finalmente, nós criamos a regra de descoberta e tudo parece que irá funcionar. Temos cinco protótipos de itens, dois protótipos de trigger e um protótipo de gráfico.

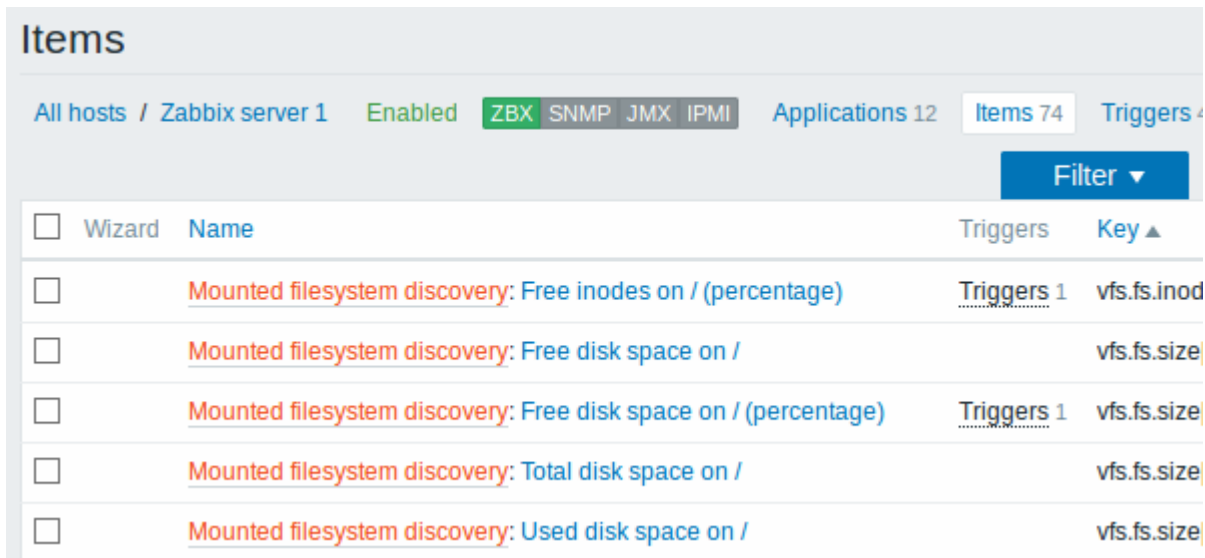
Discovery rules

[All templates / Template OS Linux](#) [Applications 10](#) [Items 32](#) [Triggers 15](#) [Graphs 5](#) [Screens 1](#)

<input type="checkbox"/>	NAME ▲	ITEMS	TRIGGERS	GRAPHS	H
<input type="checkbox"/>	Mounted filesystem discovery	Item prototypes 5	Trigger prototypes 2	Graph prototypes 1	H

Nota: Para configurar um protótipo de host consulte o manual de [protótipos de host](#) na área de monitoração de máquinas virtuais.

As telas a seguir ilustram como itens, triggers e gráficos que foram criados pelo processo de descoberta irão se parecer na tela de configuração de um host. As entidades descobertas serão prefixadas por um link laranja com o nome de sua regra de descoberta de origem.

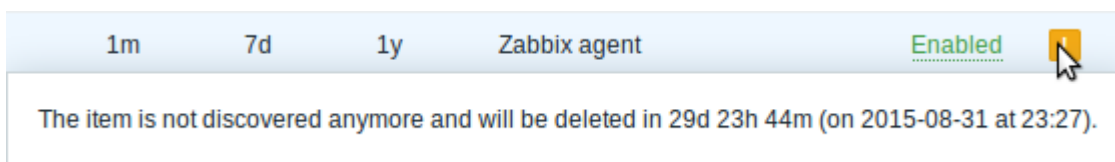


<input type="checkbox"/>	Wizard	Name	Triggers	Key ▲
<input type="checkbox"/>		Mounted filesystem discovery: Free inodes on / (percentage)	Triggers 1	vfs.fs.inod
<input type="checkbox"/>		Mounted filesystem discovery: Free disk space on /		vfs.fs.size
<input type="checkbox"/>		Mounted filesystem discovery: Free disk space on / (percentage)	Triggers 1	vfs.fs.size
<input type="checkbox"/>		Mounted filesystem discovery: Total disk space on /		vfs.fs.size
<input type="checkbox"/>		Mounted filesystem discovery: Used disk space on /		vfs.fs.size

Observe que não serão criadas entidades para recursos caso já exista outra entidade com o mesmo critério de unicidade (por exemplo outro item com a mesma chave, ou gráfico com o mesmo nome).

Os itens (de forma similar às triggers e gráficos) criados por um LLD não poderão ser excluídos manualmente. Entretanto, poderão ser excluídos automaticamente se a regra de descoberta não conseguir mais localizar o recurso, ou se seu filtro excluir o recurso da lista. Neste caso os itens, triggers e gráficos serão apagados após o período definido no campo *Manter dados de recursos perdidos por (em dias)*.

Quando as entidades passam para o estado 'Não foi mais descoberto', um indicador do tempo restante de vida será apresentado para o item na lista. Ao posicionar o mouse sobre o ícone de alerta será apresentada uma mensagem indicando quanto tempo falta para o item e seu histórico serem excluídos.



1m 7d 1y Zabbix agent Enabled

The item is not discovered anymore and will be deleted in 29d 23h 44m (on 2015-08-31 at 23:27).

Se as entidades forem marcadas para exclusão, mas não forem excluídas no momento previsto (por exemplo por causa da regra de descoberta ter sido inativada), eles serão excluídos no próximo momento que a regra for processada.

The screenshot shows the Zabbix Triggers interface. At the top, there are navigation links: "All hosts / Zabbix server 1", status "Enabled", and filter tabs for "ZBX", "SNMP", "JMX", and "IPMI". On the right, it shows "Applications 12", "Items 74", and "Triggers 4". A "Filter" button is visible. Below this is a table with columns for "Severity", "Name", and "Expression". Two triggers are listed, both with a "Warning" severity:

Severity	Name	Expression
Warning	Mounted filesystem discovery: Free disk space is less than 20% on volume /	{Zabbix serv
Warning	Mounted filesystem discovery: Free inodes is less than 20% on volume /	{Zabbix serv

The screenshot shows the Zabbix Graphs interface. At the top, there are navigation links: "All hosts / Zabbix server 1", status "Enabled", and filter tabs for "ZBX", "SNMP", "JMX", and "IPMI". On the right, it shows "Applications 12", "Items 74", and "Triggers 4". A "Group" dropdown menu is set to "all". Below this is a table with columns for "Name" and "Expression". Several items are listed, including templates and triggers:

Name	Expression
Template OS Linux_b: CPU jumps	
Template OS Linux_b: CPU load	
Template OS Linux_b: CPU utilization	
Mounted filesystem discovery: Disk space usage /	

3.2 Descoberta de interfaces de rede

A descoberta de interfaces de rede é feita exatamente da mesma forma que a descoberta de sistemas de arquivos. O que muda é o nome da chave buscada (“net.if.discovery” ao invés de “vfs.fs.discovery”) e o nome das macros retornadas ({#IFNAME} ao invés de {#FSNAME}).

Exemplos de protótipos de item que você definir usando a chave “net.if.discovery”:
“net.if.in[{#IFNAME},bytes]”, “net.if.out[{#IFNAME},bytes]”. [Clique aqui](#) para maiores detalhes.

3.3 Descoberta de CPUs e núcleos de CPU

A descoberta de CPUs e núcleos de CPU da mesma forma que as anteriores, mudando novamente a chave de descoberta: “system.cpu.discovery”. Ela também retorna duas macros: {#CPU.NUMBER} e {#CPU.STATUS}, respectivamente o número de sequencia da CPU e seu status. Pode não ser possível uma distinção clara entre processadores físicos, núcleos e 'hyperthreads'. Em ambientes Linux, UNIX e BSD a macro {#CPU.STATUS} retorna o status do processador, que poderá ser “online” ou “offline”. Em ambientes Windows, esta macro poderá conter um terceiro valor - “unknown” - que indicará que o processador foi detectado mas nenhuma informação foi coletada ainda sobre ele.

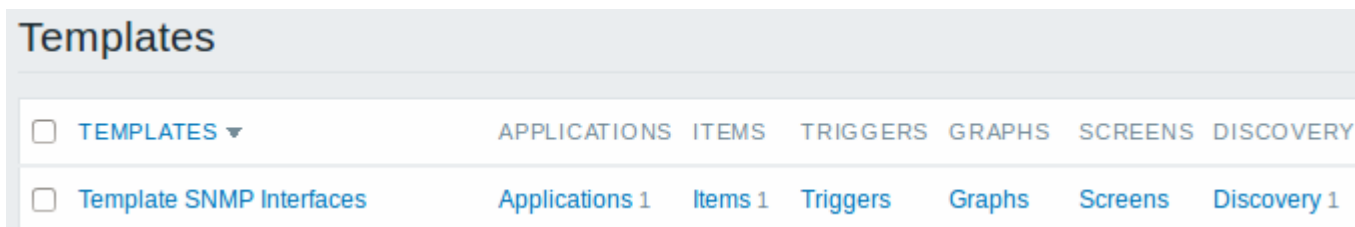
A descoberta de CPU utiliza estatísticas dos processos de coleta do agente para manter a consistência dos dados providos e economizar recursos ao obter os dados. Isso afeta a coleta desta chave quando se tenta utilizar a opção '-t' na linha de comando com o binário do agente diretamente, esta chave será devolvida com o status de NOT_SUPPORTED, acompanhada da mensagem que o coletor não foi iniciado.

Os protótipos de item que podem ser criados com esta descoberta incluem

“system.cpu.load[{#CPU.NUMBER}, <mode>]”, “system.cpu.util[{#CPU.NUMBER}, <type>, <mode>]”, dentre outros.

3.4 Descoberta de OIDs SNMP

Neste exemplo, nós vamos executar a descoberta SNMP em um switch. Acesse *Configuração* → *Templates*.



Para editar as regras de descoberta do template desejado, clique no link *Descoberta* de sua linha.

Para criar uma nova regra de descoberta, use o botão *Criar regra de descoberta* localizado no canto direito da barra de título.

Diferentemente das descobertas de sistemas de arquivos e de interfaces de rede, esta regra não necessita de uma chave “snmp.discovery”, o uso do tipo SNMP agent é suficiente.

Os OIDs serão descobertos no seguinte formato: `discovery[{#MACRO1}, oid1, {#MACRO2}, oid2, ...,]`

Onde `{#MACRO1}`, `{#MACRO2}` ... são nomes válidos de macro e `oid1`, `oid2`... são identificadores OIDs capazes de gerar valores para estas macros. Uma macro pré-definida `{#SNMPINDEX}` conterá o índice do OID descoberto que poderá ser aplicado aos recursos descobertos. Os recursos estarão agrupados através da macro `{#SNMPINDEX}`.

Para entender o que isso significa, vamos executar alguns `snmpwalks` em nosso switch:

```
$ snmpwalk -v 2c -c public 192.168.1.1 IF-MIB::ifDescr
IF-MIB::ifDescr.1 = STRING: WAN
IF-MIB::ifDescr.2 = STRING: LAN1
IF-MIB::ifDescr.3 = STRING: LAN2

$ snmpwalk -v 2c -c public 192.168.1.1 IF-MIB::ifPhysAddress
IF-MIB::ifPhysAddress.1 = STRING: 8:0:27:90:7a:75
IF-MIB::ifPhysAddress.2 = STRING: 8:0:27:90:7a:76
IF-MIB::ifPhysAddress.3 = STRING: 8:0:27:2b:af:9e
```

E definir o OID SNMP para: `discovery[{#IFDESCR}, ifDescr, {#IFPHYSADDRESS}, ifPhysAddress]`

Agora esta regra irá descobrir os recursos com as macros `{#IFDESCR}` definidas como **WAN**, **LAN1** e **LAN2**, as macros `{#IFPHYSADDRESS}` terá os valores **8:0:27:90:7a:75**, **8:0:27:90:7a:76**, e **8:0:27:2b:af:9e**, e as macros `{#SNMPINDEX}` com os índices **1**, **2** e **3**:

```
{
  "data": [
    {
      "#{SNMPINDEX}": "1",
      "#{IFDESCR}": "WAN",
      "#{IFPHYSADDRESS}": "8:0:27:90:7a:75"
    },
    {
      "#{SNMPINDEX}": "2",
      "#{IFDESCR}": "LAN1",
      "#{IFPHYSADDRESS}": "8:0:27:90:7a:75"
    },
    {
      "#{SNMPINDEX}": "3",
      "#{IFDESCR}": "LAN2",
      "#{IFPHYSADDRESS}": "8:0:27:2b:af:9e"
    }
  ]
}
```

Se um recurso não existir no OID especificado então a macro correspondente para ele será omitida, por exemplo:

```
ifDescr.1 "Interface #1"
ifDescr.2 "Interface #2"
ifDescr.4 "Interface #4"

ifAlias.1 "eth0"
ifAlias.2 "eth1"
ifAlias.3 "eth2"
ifAlias.5 "eth4"
```

Então, neste caso, a descoberta SNMP `discovery[#{IFDESCR}, ifDescr, {#IFALIAS}, ifAlias]` retornará a seguinte estrutura JSON:

```
{
  "data": [
    {
      "#{SNMPINDEX}": 1,
      "#{IFDESCR}": "Interface #1",
      "#{IFALIAS}": "eth0"
    },
    {
      "#{SNMPINDEX}": 2,
      "#{IFDESCR}": "Interface #2",
      "#{IFALIAS}": "eth1"
    },
    {
      "#{SNMPINDEX}": 3,
      "#{IFALIAS}": "eth2"
    }
  ]
}
```

```
},
{
  "#{SNMPINDEX}": 4,
  "#{IFDESCR}": "Interface #4"
},
{
  "#{SNMPINDEX}": 5,
  "#{IFALIAS}": "eth4"
}
]
}
```

Discovery rule **Filters**

Name

Type

Key

SNMP OID

SNMP community

Port

Update interval

Custom intervals

Type	Interval	Period
<input checked="" type="checkbox"/> Flexible <input type="checkbox"/> Scheduling	<input type="text" value="50s"/>	<input type="text" value="1-7,00:00-24:00"/>

[Add](#)

Keep lost resources period

Description

Enabled

Estas telas ilustram como as macros podem ser utilizadas em protótipos de item:

Item prototype **Preprocessing**

Name Incoming traffic on interface \$1

Type SNMPv2 agent

Key ifInOctets[#{IFDESCR}]

SNMP OID IF-MIB::ifInOctets.#{SNMPINDEX}

SNMP community {\$SNMP_COMMUNITY}

Port

Type of information Numeric (unsigned)

Units bps

Update interval 1m

Custom intervals

Type	Interval	Period
Flexible Scheduling	50s	1-7,00:00-24:00

[Add](#)

History storage period 1w

Trend storage period 365d

Show value As is [show value mappings](#)

New application

Da mesma forma, criando quantos itens quanto o necessário:

Item prototypes

[All templates / Template SNMP Interfaces](#) [Discovery list / Network interfaces](#) **Item prototypes 8**

<input type="checkbox"/> NAME ▲	KEY	INTERVAL	HI
<input type="checkbox"/> Admin status of interface {#IFDESCR}	ifAdminStatus[{#IFDESCR}]	1m	7d
<input type="checkbox"/> Alias of interface {#IFDESCR}	ifAlias[{#IFDESCR}]	1h	7d
<input type="checkbox"/> Description of interface {#IFDESCR}	ifDescr[{#IFDESCR}]	1h	7d
<input type="checkbox"/> Inbound errors on interface {#IFDESCR}	ifInErrors[{#IFDESCR}]	1m	7d
<input type="checkbox"/> Incoming traffic on interface {#IFDESCR}	ifInOctets[{#IFDESCR}]	1m	7d
<input type="checkbox"/> Operational status of interface {#IFDESCR}	ifOperStatus[{#IFDESCR}]	1m	7d
<input type="checkbox"/> Outbound errors on interface {#IFDESCR}	ifOutErrors[{#IFDESCR}]	1m	7d
<input type="checkbox"/> Outgoing traffic on interface {#IFDESCR}	ifOutOctets[{#IFDESCR}]	1m	7d

Protótipos de trigger:

Trigger prototype [Dependencies](#)

Name

Severity Not classified Information Warning Average High Critical

Expression

[Expression constructor](#)

OK event generation Expression Recovery expression None

PROBLEM event generation mode Single Multiple

OK event closes All problems All problems if tag values match

Tags

<input type="text" value="tag"/>	<input type="text" value="value"/>	<input type="button" value="Remove"/>
----------------------------------	------------------------------------	---------------------------------------

[Add](#)

Allow manual close

URL

Description

Create enabled

Trigger prototypes

[All templates / Template SNMP Interfaces](#) [Discovery list / Network interfaces](#) [Item prototypes 8](#)

<input type="checkbox"/>	SEVERITY	NAME ▲	EXPR
<input type="checkbox"/>	Information	Operational status was changed on {HOST.NAME} interface {#IFDESCR}	{Temp

Protótipos de gráfico:

Graph prototype
Preview

Name

Width

Height

Graph type Normal

Show legend

Show working time

Show triggers

Percentile line (left)

Percentile line (right)

Y axis MIN value Calculated

Y axis MAX value Calculated

	Name	Function	Draw style
⋮	1: Template SNMP Interfaces: Incoming traffic on interface {#IFDESCR}	avg	Gradient
⋮	2: Template SNMP Interfaces: Outgoing traffic on interface {#IFDESCR}	avg	Gradient

[Add](#) [Add prototype](#)

Graph prototypes

[All templates / Template SNMP Interfaces](#)
[Discovery list / Network interfaces](#)
[Item prototypes 8](#)

	NAME ▲	WIDTH
<input type="checkbox"/>	Traffic on interface {#SNMPVALUE}	900

Um sumário de nossa regra de descoberta:

Discovery rules

[All templates / Template SNMP Interfaces](#)
[Applications 1](#)
[Items 1](#)
[Triggers](#)
[Graphs](#)
[Screens](#)

	NAME ▲	ITEMS	TRIGGERS	GRAPHS	HO
<input type="checkbox"/>	Network interfaces	Item prototypes 8	Trigger prototypes 1	Graph prototypes 1	Ho

Quando o servidor executa, ele cria itens, triggers e gráficos reais a partir dos valores retornados pela descoberta SNMP. Na configuração do host eles estarão prefixados com o nome da regra de descoberta que os originou e na cor laranja.

Items

All hosts / Switch1 Enabled ZBX SNMP JMX IPMI Applications 1 Items 241 Triggers 30 Gr

Filter

<input type="checkbox"/>	Wizard	Name	Triggers	Key
<input type="checkbox"/>		Network interfaces: Admin status of interface 1		ifAdminStatus[1]
<input type="checkbox"/>		Network interfaces: Admin status of interface 2		ifAdminStatus[2]
<input type="checkbox"/>		Network interfaces: Admin status of interface 3		ifAdminStatus[3]
<input type="checkbox"/>		Network interfaces: Admin status of interface 4		ifAdminStatus[4]

Triggers

All hosts / Switch1 Enabled ZBX SNMP JMX IPMI Applications 1 Items 241 Triggers 30 Gr

Filter

<input type="checkbox"/>	Severity	Name	Exp
<input type="checkbox"/>	Information	Network interfaces: Operational status was changed on {HOST.NAME} interface 1	{pr
<input type="checkbox"/>	Information	Network interfaces: Operational status was changed on {HOST.NAME} interface 2	{pr
<input type="checkbox"/>	Information	Network interfaces: Operational status was changed on {HOST.NAME} interface 3	{pr
<input type="checkbox"/>	Information	Network interfaces: Operational status was changed on {HOST.NAME} interface 4	{pr

Graphs

Group all

All hosts / Switch1 Enabled ZBX SNMP JMX IPMI Applications 1 Items 241 Triggers 30 Gr

<input type="checkbox"/>	Name
<input type="checkbox"/>	Network interfaces: Traffic on interface 1
<input type="checkbox"/>	Network interfaces: Traffic on interface 2
<input type="checkbox"/>	Network interfaces: Traffic on interface 3
<input type="checkbox"/>	Network interfaces: Traffic on interface 4

3.5 Descoberta usando consultas SQL/ODBC

Este tipo de descoberta é feito através de consultas SQL, cujos resultados são transformados

automaticamente em um objeto JSON aceitável pelo LLD. As consultas SQL são executadas com itens do tipo “Monitoração de banco de dados”. Consulte o manual sobre [monitoração ODBC](#) para maiores detalhes de como trabalhar com este tipo de item, a única diferença é que a chave a ser utilizada será “db.odbc.discovery[<description>,<dsn>]” ao invés de “db.odbc.select[<description>,<dsn>]”.

Um exemplo prático de como as consultas SQL são transformadas em um JSON pode ser a descoberta através de um proxy com consultas ODBC no banco do Zabbix. Isso pode ser útil para a criação automática de itens [internos](#) para monitorar os proxies “zabbix[proxy,<name>,lastaccess]”, verificando se estão ativos.

Vamos começar com a configuração da regra de descoberta:

The screenshot shows the configuration page for a discovery rule named "Proxy discovery". The "Discovery rule" tab is active, and the "Filters" tab is also visible. The configuration includes:

- Name:** Proxy discovery
- Type:** Database monitor
- Key:** db.odbc.discovery[proxies,{\$DSN}]
- User name:** (empty field)
- Password:** (empty field)
- SQL query:** SELECT h1.host, COUNT (h2.host) AS count FROM hosts h1 LEFT JOIN hosts h2 ON h1.hostid = h2.proxy_hostid WHERE h1.status IN (5, 6) GROUP BY h1.host;
- Update interval:** 1h
- Custom intervals:** A table with columns Type, Interval, and Period. One interval is defined with Type "Flexible Scheduling", Interval "50s", and Period "1-7,00:00-24:00". An "Add" link is present below the table.
- Keep lost resources period:** 30d
- Description:** (empty text area)
- Enabled:**
- Buttons:** "Add" and "Cancel"

Aqui vamos usar conexão direta com o BD do Zabbix para localizar todos os proxies, junto com a quantidade de hosts que eles monitoram. A quantidade de hosts pode ser utilizada, por exemplo, para filtrar proxies que não tem carga de monitoração sobre sí:

```
mysql> SELECT h1.host, COUNT(h2.host) AS count FROM hosts h1 LEFT JOIN hosts
h2 ON h1.hostid = h2.proxy_hostid WHERE h1.status IN (5, 6) GROUP BY
h1.host;
+-----+-----+
| host    | count |
+-----+-----+
| Japan 1 |     5 |
| Japan 2 |    12 |
| Latvia  |     3 |
+-----+-----+
3 rows in set (0.01 sec)
```

Internamente a chave “db.odbc.discovery[]” irá receber este valor e transformar em um código JSON:

```
{
  "data": [
    {
      "#{HOST}": "Japan 1",
      "#{COUNT}": "5"
    },
    {
      "#{HOST}": "Japan 2",
      "#{COUNT}": "12"
    },
    {
      "#{HOST}": "Latvia",
      "#{COUNT}": "3"
    }
  ]
}
```

Os nomes das colunas da consulta foram automaticamente definidos como sendo os nomes de macro, seguidos de seus valores.

Se não estiver muito claro como um nome de coluna foi transformado em um nome de macro, sugerimos utilizar apelidos de colunas no exemplo acima (ex. “COUNT(h2.host) AS count”).

Caso o nome de alguma coluna não possa ser transformado em um nome válido de macro, a regra irá para o estado 'Não suportado' com mensagem de erro detalhando o problema com a coluna de número X. Se informações adicionais forem necessárias, poderão ser obtidas ao ativar o modo de debug 4 (**DebugLevel=4**) e consultar o log do Zabbix Server:

```
$ grep db.odbc.discovery /tmp/zabbix_server.log
...
23876:20150114:153410.856 In db_odbc_discovery() query:'SELECT h1.host,
COUNT(h2.host) FROM hosts h1 LEFT JOIN hosts h2 ON h1.hostid =
h2.proxy_hostid WHERE h1.status IN (5, 6) GROUP BY h1.host;'
23876:20150114:153410.860 db_odbc_discovery() column[1]:'host'
```

```
23876:20150114:153410.860 db_odbc_discovery() column[2]:'COUNT(h2.host)'  
23876:20150114:153410.860 End of db_odbc_discovery():NOTSUPPORTED  
23876:20150114:153410.860 Item [Zabbix  
server:db.odbc.discovery[proxies,{ $DSN}]] error: Cannot convert column #2  
name to macro.
```

Agora conseguimos entender como uma consulta SQL é transformada em um objeto JSON e podemos utilizar a macro {#HOST} para criar os protótipos de itens:

The screenshot shows the 'Item prototype' configuration page for 'Preprocessing'. The fields are as follows:

- Name: Last acces time of proxy {#HOST}
- Type: Zabbix internal
- Key: zabbix[proxy,{#HOST},lastaccess]
- Type of information: Numeric (unsigned)
- Units: unixtime
- Update interval: 60s
- Custom intervals: A table with columns Type, Interval, and Period. It contains one entry: Type: Flexible Scheduling, Interval: 50s, Period: 1-7,00:00-24:00. There is an 'Add' link below.
- History storage period: 90d
- Trend storage period: 365d
- Show value: As is (with a 'show value mappings' link)

Uma vez que a descoberta seja executada, um item será criado para cada proxy:

The screenshot shows the 'Items' page in Zabbix. At the top, there are navigation links: 'All hosts / Zabbix server 1', status 'Enabled', and discovery methods 'ZBX', 'SNMP', 'JMX', 'IPMI'. It also shows 'Applications 12', 'Items 70', and 'Triggers'. A 'Filter' button is present. The table below lists the discovered items:

<input type="checkbox"/>	Wizard	Name	Triggers	Key ▲
<input type="checkbox"/>		Proxy discovery: Last access time of proxy Japan1		zabbix[proxy,Japan1,lastacce
<input type="checkbox"/>		Proxy discovery: Last access time of proxy Japan2		zabbix[proxy,Japan2,lastacce
<input type="checkbox"/>		Proxy discovery: Last access time of proxy Latvia		zabbix[proxy,Latvia,lastaccess

3.6 Descobertas de serviços no Windows

A descoberta de serviços no Windows é feita da mesma forma que a descoberta de sistemas de arquivos. A chave utilizada é a “service.discovery” as seguintes macros estarão disponíveis para uso nos [filtros](#) e protótipos de item/trigger/graph:

```
{#SERVICE.NAME}  
{#SERVICE.DISPLAYNAME}  
{#SERVICE.DESCRPTION}  
{#SERVICE.STATE}  
{#SERVICE.STATENAME}  
{#SERVICE.PATH}  
{#SERVICE.USER}  
{#SERVICE.STARTUP}  
{#SERVICE.STARTUPNAME}
```

Através da descoberta de serviços do Windows você poderá criar protótipos de itens como “service.info[`{#SERVICE.NAME},<param>`]”, onde *param* aceita os seguintes valores: *state*, *displayname*, *path*, *user*, *startup* ou *description*. Por exemplo, para obter o nome de exibição de um serviço você pode criar um item com a chave “service.info[`{#SERVICE.NAME},displayname`]”. Se o parâmetro *param* não for definido (“service.info[`{#SERVICE.NAME}`]”), o valor padrão *state* será utilizado.

As macros `{#SERVICE.STATE}` e `{#SERVICE.STATENAME}` retornarão o mesmo conteúdo, entretanto, `{#SERVICE.STATE}` retornará a representação numérica (0-7), e `{#SERVICE.STATENAME}` a representação textual (*running*, *paused*, *start pending*, *pause pending*, *continue pending*, *stop pending*, *stopped* ou *unknown*). O mesmo se aplica às macros `{#SERVICE.STARTUP}` e `{#SERVICE.STARTUPNAME}`, onde uma retorna a representação numérica (0-4) e a outra textual (*automatic*, *automatic delayed*, *manual*, *disabled*, *unknown*).

3.7 Criando LLD customizado

Além de todos os tipos nativos de regra de descoberta, você também poderá criar suas próprias regras de descoberta para retornar qualquer tipo de recurso - por exemplo, descobrir as bases de dados em um servidor de banco.

Para fazer isso precisamos de um item que retorne um JSON, definindo objetos e, opcionalmente, propriedades deles. A quantidade de macros por entidade não é limitada. Nas descobertas nativas normalmente são retornadas uma ou duas macros mas é possível retornar muito mais..

O formato JSON requerido é ilustrado neste exemplo, suponhamos que você esteja usando um Zabbix Agent 1.8 (bem antigo), ele não irá ter suporte nativo para a chave “vfs.fs.discovery”, mas ainda assim ele será capaz de executar a descoberta de sistemas de arquivo. Um simples script em Perl no Linux poderá descobrir os sistemas de arquivo montados e apresentar o resultado no formato JSON, indexando tanto os nomes quanto os seus tipos. Poderíamos criar, por exemplo, um **UserParameter** chamado “vfs.fs.discovery_perl”:

```
#!/usr/bin/perl

$first = 1;

print "{\n";
print "\t\data\":[\n\n";

for (`cat /proc/mounts`)
{
    ($fsname, $fstype) = m/\S+ (\S+) (\S+)/;
    $fsname =~ s/!\//!g;

    print "\t,\n" if not $first;
    $first = 0;

    print "\t{\n";
    print "\t\t\"{#FSNAME}\" : \"$fsname\", \n";
    print "\t\t\"{#FSTYPE}\" : \"$fstype\" \n";
    print "\t}\n";
}

print "\n\t]\n";
print "}\n";
```

Os caracteres permitidos em um nome de macro LLD são **0-9** , **A-Z** , **_** , **.**

Não são suportadas letras minúsculas em seus nomes.

Um exemplo de saída deste script (reformatado para melhor legibilidade) poderia ser algo como isso:

```
{
  "data": [
    { "{#FSNAME}": "\/", "{#FSTYPE}": "rootfs" },
    { "{#FSNAME}": "\/sys", "{#FSTYPE}": "sysfs" },
    { "{#FSNAME}": "\/proc", "{#FSTYPE}": "proc" },
    { "{#FSNAME}": "\/dev", "{#FSTYPE}": "devtmpfs" },
    { "{#FSNAME}": "\/dev/pts", "{#FSTYPE}": "devpts" },
    { "{#FSNAME}": "\/", "{#FSTYPE}": "ext3" },
    { "{#FSNAME}": "\/lib/init/rw", "{#FSTYPE}": "tmpfs" },
    { "{#FSNAME}": "\/dev/shm", "{#FSTYPE}": "tmpfs" },
    { "{#FSNAME}": "\/home", "{#FSTYPE}": "ext3" },
    { "{#FSNAME}": "\/tmp", "{#FSTYPE}": "ext3" },
    { "{#FSNAME}": "\/usr", "{#FSTYPE}": "ext3" },
    { "{#FSNAME}": "\/var", "{#FSTYPE}": "ext3" },
    { "{#FSNAME}": "\/sys/fs/fuse/connections", "{#FSTYPE}": "fusectl" }
  ]
}
```

Assim, no *Filtro* da regra de descoberta você poderá, por exemplo, validar o conteúdo da macro "{#FSTYPE}" com uma expressão regular ("rootfs|ext3").

Você não precisa nomear as macros como FSNAME/FSTYPE em regras customizadas, use o nome que quiser contando que se adeque aos caracteres permitidos.

From:

<https://www.zabbix.com/documentation/3.4/> - **Zabbix Documentation 3.4**

Permanent link:

https://www.zabbix.com/documentation/3.4/pt/manual/discovery/low_level_discovery

Last update: **2019/01/28 14:50**

