

# Totvs RM

## Serviço de Cache Centralizado

### Guia de Instalação e Configuração



21/03/2018



## Sumário

1	Introdução .....	3
1.1.	Organização do documento .....	3
1.2.	Entendendo os benefícios .....	3
2	Instalando o Redis .....	3
2.1.	Instalando o Redis no Linux .....	3
2.2.	Instalando o Redis via Docker .....	5
2.3.	Instalando o Redis no Windows .....	5
3	Configurando SSL .....	7
3.1.	Configurando SSL no Linux .....	7
3.2.	Instalando certificado no servidor Windows .....	9
4	Configurando o Totvs RM .....	10
4.1.	Configurando o Redis .....	10

Versão do documento	Modificação	Autor / Revisor
1.0 - 21/03/2018	Criação do documento	Carlos Garcia / Carlos Garcia
1.1 - 26/03/2018	Alteração do documento	Carlos Garcia / Diogo Damiani
1.2 - 26/03/2018	Alteração do documento	Carlos Garcia / Carlos Farias



## 1 Introdução

Este documento é um guia de instalação e configuração do serviço de cache centralizado para os produtos da linha TOTVS RM. Dentre os benefício que o cache centralizado traz estão: racionalização de recursos de memória e eliminação de chaves duplicadas em instancias distintas de servidores de aplicação.

### 1. 1. Organização do documento

Para instalar o serviço de cache centralizado será necessário realizar as operações dos seguintes tópicos deste documento:

- Instalação do Redis, tópico 2. (requerido)
- Caso opte por utilizar a criptografia SSL, tópico 3. (opcional)
- Configuração dos serviços de host do Totvs RM, tópico 4. (requerido)

### 1. 2. Entendendo os benefícios

Os benefícios de utilização do cache centralizado está relacionado com o tamanho do ambiente. Quanto maior o ambiente, ou seja, quanto maior o número de instancias de servidores de aplicação (Host) e servidores de job (Job Server) maiores serão os ganhos na utilização deste serviço.

## 2 Instalando o Redis

Dentre as opções de instalação do Redis estão: Instalação nativa nos sistemas operacionais Linux, Windows e instalação via Docker em ambos os sistemas operacionais.

A versão corrente para Windows é a 3.2.1 e atualmente não recebe atualizações, apesar de suportar o uso do serviço de cache do Totvs RM.

O Docker Container oficial disponível no Docker Hub é para Linux. Desta forma se você pretende utiliza-lo em ambiente Windows terá que realizar as configurações mencionadas no tópico 2.2 deste documento.

### 2. 1. Instalando o Redis no Linux

Para instalar o Redis no Linux utilizando o gerenciador de pacotes apt-get, abra uma sessão ssh e entre com os comandos abaixo:

Sincronizando os índices dos pacotes

```
sudo apt-get update  
sudo apt-get upgrade
```

Instalando o Redis

```
sudo apt-get install redis-server
```

Configurando o Redis – Abra o arquivo de configuração



```
sudo vi /etc/redis/redis.conf
```

Procure pela chave **bind**, descomente-a e altere-a para o IP o qual será visto pelos servidores RM. **NÃO** utilize um IP que seja expoto à internet.

```
bind 10.1.21.102
```

A porta default do redis é 6379, caso precise alterar esta porta altere a chave **port**.

```
port 6379
```

Procure pela chave **protected-mode**, descomente-a e altere-a para **no**.

```
protected-mode no
```

Procure pela chave **requirepass**, descomente-a e altere-a para o valor do password que desejar. Este password deverá ser informado na configuração do RM.Host.Service.

```
requirepass MYPASSWORD
```

Habilite o Redis no boot

```
sudo systemctl enable redis-server.service
```

Reinicie o Redis

```
sudo systemctl restart redis-server.service
```

Liberando a porta 6379 no firewall

```
sudo ufw allow 6379/tcp
```

Obs: Os comandos de instalação, assim como a localização dos arquivos de configuração, podem variar de acordo com a distribuição do Linux utilizado, porém a sequencia de comandos e configuração permanece a mesma. Caso seja necessário verifique as documentações de referências para sua distribuição Linux na Internet.



## 2. 2. Instalando o Redis via Docker

O Redis pode ser utilizado também via docker container. Para isso assume-se que o docker encontra-se instalado e configurado na maquina e que esta possui acesso à Internet.

Além disso, se a máquina host do Docker for Windows deve haver uma instância do Hyper-V com uma máquina Linux configurada. Mais detalhes podem ser obtidos em <https://forums.docker.com/t/linux-container-on-windows-docker-host/25884>.

Para instalar e rodar o container execute o seguinte comando:

Rodando o container Redis. Configure o parâmetro **-requirepass** com o password desejado.

OBS: Utilizando Powershell (no Windows) deve-se retirar o comando **sudo** e retirar uma das barras no trecho [docker.io//redis ...]

```
sudo docker run -d
  -p 6379:6379
  --name redis-1
  docker.io//redis:4.0.8-alpine
  redis-server
  --appendonly yes
  --requirepass MYPASSWORD
```

Liberando a porta 6379 no firewall

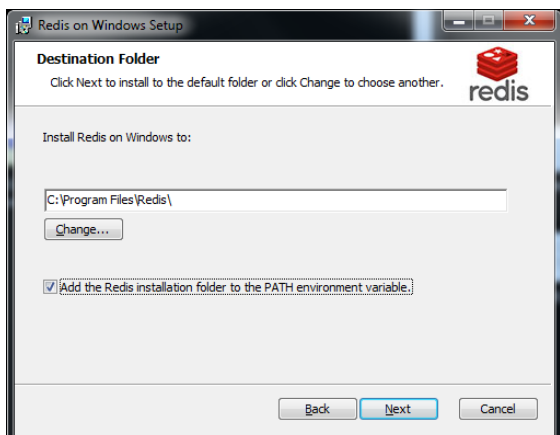
```
sudo ufw allow 6379/tcp
```

## 2. 3. Instalando o Redis no Windows

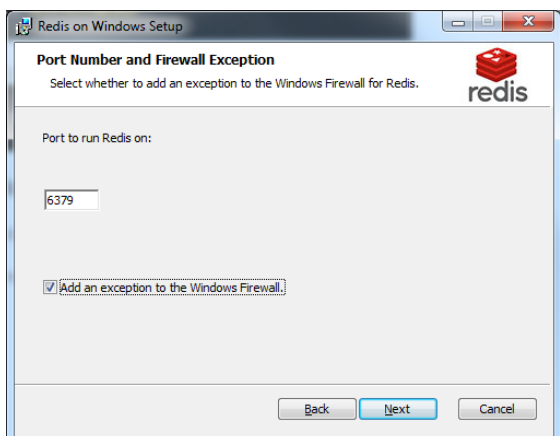
Baixe o arquivo de instalação (msi) em <https://github.com/MicrosoftArchive/redis/releases>.

Inicie o programa de instalação.

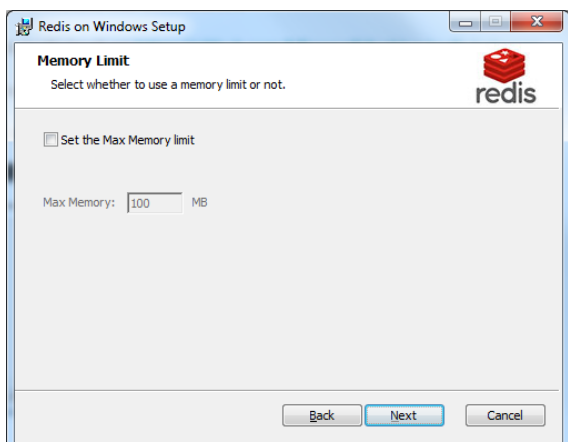
Marque a opção para adicionar o Redis no path da maquina



Marque a opção para adicionar a porta ao firewall.



Desmarque a opção de memory limit



Avance até o final da instalação.

Configurando o Redis – Abra o arquivo de configuração



```
C:\Program Files\Redis\redis.windows-service.conf
```

Procure pela chave **bind**, descomente-a e altere-a para o IP o qual será visto pelos servidores RM. **NÃO** utilize um IP que seja expoto à internet.

```
bind 10.1.21.102
```

Procure pela chave **protected-mode**, descomente-a e altere-a para **no**.

```
protected-mode no
```

Procure pela chave **requirepass**, descomente-a e altere-a para o valor do password que desejar. Este password deverá ser informado na configuração do RM.Host.Service.

```
requirepass MYPASSWORD
```

Reiniciando o serviço Redis pelo prompt de comando

```
sc stop Redis  
sc start Redis
```

## 3 Configurando SSL

### 3.1. Configurando SSL no Linux

De acordo com o modelo de segurança defendido pelos fornecedores o Redis foi projetado para ser acessado por clientes confiáveis e dentro de ambientes confiáveis. Isto significa que é contraindicado expor uma instância Redis diretamente à Internet ou em um ambiente onde clientes não confiáveis possam acessa-lo diretamente. Mais detalhes a este respeito pode ser encontrado em: <https://redis.io/topics/security>.

Se a utilização de criptografia se fizer necessária isto pode ser feito por meio de tunelamento utilizando o **stunnel**. Seguem abaixo os passos para instalação e configuração:

Instalando do **stunnel**

```
sudo apt-get install stunnel
```

Edite o arquivo de configuração (OBS: /etc/default/stunnel4)

```
sudo vi /etc/default/stunnel
```



Encontre

```
ENABLED=0
```

Troque por

```
ENABLED=1
```

Gere um certificado para o host/ip da máquina onde se encontra instalado o Redis ou que contém o docker container. Altere a tag **HOST\_NAME** com o nome do host ou com o ip

```
sudo openssl req -x509 -nodes -days 3650 \
  -newkey rsa:2048 \
  -subj '/CN=HOST_NAME/O=HOST_NAME' \
  -keyout /etc/stunnel/redis-server.key \
  -out /etc/stunnel/redis-server.crt
```

Altere a permissão dos arquivos gerados

```
Sudo chmod 640 /etc/stunnel/redis-server.key
Sudo Chmod 640 /etc/stunnel/redis-server.crt
```

Crie/Edite o arquivo de configuração

```
sudo vi /etc/stunnel/stunnel.conf
```

Adicione a seguinte configuração

```
pid = /var/run/stunnel.pid

[redis-server]
cert = /etc/stunnel/redis-server.crt
key = /etc/stunnel/redis-server.key
accept = 6380
connect = 127.0.0.1:6379
```

Configurando o Redis - Abra o arquivo de configuração

```
sudo vi /etc/redis/redis.conf
```

Para permitir apenas requisições locais no Redis e assim proteje-lo, procure pela chave **bind**, descomente-a e altere-a para o IP 127.0.0.1.

```
bind 127.0.0.1
```

Habilite o stunnel no boot





```
sudo systemctl enable stunnel
```

Caso o arquivo stunnel.service não exista, devemos criá-lo.

```
sudo vi /lib/systemd/system/stunnel.service
```

Preencha-o com os seguintes comandos

```
[Unit]
Description=SSL tunnel for network daemons
After=network.target
After=syslog.target

[Install]
WantedBy=multi-user.target
Alias=stunnel.target

[Service]
Type=forking
ExecStart=/usr/bin/stunnel
/etc/stunnel/stunnel.conf
ExecStop=/usr/bin/killall -9 stunnel

#Give up if ping don't get an answer
TimeoutSec=600

Restart=always
PrivateTmp=false
```

Reinicie o stunnel

```
sudo systemctl restart stunnel
```

Libere a porta 6380 no firewall e bloqueie a porta 6379

```
sudo ufw allow 6380/tcp
sudo ufw deny 6379
```

## 3. 2. Instalando Certificado no Servidor Windows

Após ter realizado as configurações constantes no item 3.1 deste documento será possível realizar o restante das configurações na máquina onde os serviços RM estão instalados.

Copie o arquivo abaixo do servidor Redis do Linux para a(as) maquina(as) onde os serviços **RM.Host.Service** estão instalados.



```
/etc/stunnel/redis-server.crt
```

Instalando o certificado no servidor RM.Host.Service

- 1- Pressione Windows + R
- 2- Clique com o botão direito e depois em Add/Remove Snap-In
- 3- Clique em Certificates e depois em Add
- 4- Uma nova janela será mostrada, selecione "My user account" -> Finish
- 5- Clique em OK
- 6- Sob Console Root, expanda para "Certificates - Current User."
- 7- Clique em "Trusted Root Certification Authorities" e então em "Certificates".
- 8- Clique em "More Actions" no menu à direita, então em "All Tasks" e então em "Import"
- 9- Uma nova janela abrirá, clique em Next e então selecione o arquivo "redis-server.crt"
- 10- Clique em Next, e então Next e Finish
- 11- Será exibida uma mensagem de advertência, clique em Yes

Edite o arquivo RM.Host.Service.exe.config e altere a tag **port** e a tag **ssl** conforme mostrado abaixo

```
<add key="KVSCacheConfig" value="<IP>:6380, ..., ssl = true " />
```

Após alterar todos os arquivos **RM.Host.Service.exe.config** de seu ambiente, reinicie cada um dos serviços **RM.Host.Service**.

## 4 Configurando o Totvs RM

Este tópico descreverá as instruções para configurar o RM.Host.Service para utilização do cache centralizado.

### 4.1. Configurando o Redis

Edite o arquivo RM.Host.Service.exe.config e insira as chaves abaixo.

Altere a tag **IP**, **PORT** e **MYPASSWORD** com os valores utilizados na instalação do Redis.

A tag **ssl** deve ser configurada como **false** à não ser que a criptografia via SSL esteja habilitada. Neste caso verifique o tópico 3.2 deste documento.



```
<add key="KVSCacheConfig"
value=" IP:PORT,
abortConnect = false,
connectTimeout = 5000,
password = MYPASSWORD,
ssl = false" />
```

Adicione a tag abaixo para habilitar o redirecionamento do cache para o Redis.

```
<add key="KVSCacheRedirectEnabled" value="true" />
```

Adicione a tag abaixo para configurar o tempo padrão de expiração das chaves em segundos.

```
<add key="KVSCacheExpirySec" value="604800" />
```

Reinicie o RM.Host.Service. Realize esta configuração em todos os Servidores de App e Servidores de Job.