

# Guia Técnico

## Configuração Qlik Sense Enterprise com certificado digital e Qlik Sense Mobile V1.0.0



**Autor:** Mario Sergio Medeiros Soares  
**Revisores:** André Vinícius Silva Cavalcante  
Bianca Amazoni Fernandes Soares

Objetivo	Possibilitar acesso aos aplicativos Qlik Sense Enterprise através do app Qlik Mobile utilizando SSL válido	Versão	1.0.0
Autor	Mario Sergio Medeiros Soares ( <a href="https://www.linkedin.com/in/marioserioti/">https://www.linkedin.com/in/marioserioti/</a> )	Data Criação	26/11/2019
Revisores	André Vinícius Silva Cavalcante ( <a href="https://www.linkedin.com/in/andrevcavalcante/">https://www.linkedin.com/in/andrevcavalcante/</a> ) Bianca Amazoni Fernandes Soares	Data Atualização	26/11/2019

## 1. Índice:

2.	Cenário .....	3
3.	Atenção .....	3
4.	Requisitos .....	3
5.	Procedimentos .....	3
5.1.	Infraestrutura de rede .....	3
5.1.1.	Solicitar a TI a criação de uma rota no servidor firewall/roteador para direcionar um IP externo para o IP interno do servidor Qlik Sense Enterprise com a porta .....	3
5.1.2.	Adquirir um domínio da internet e apontar para o IP externo que está direcionado para o servidor Qlik Sense Enterprise .....	3
5.2.	Sistema Operacional .....	4
5.2.1.	Instalar serviço IIS para posteriormente emitir informações em CSR.....	4
5.2.2.	Preparar informações CSR para emissão do certificado .....	11
5.2.3.	Concluir solicitação de certificado no servidor .....	15
5.2.4.	Desativar serviço IIS .....	17
5.2.5.	Importar certificado SSL no servidor onde o Qlik Sense Enterprise está instalado .....	19
5.2.6.	Direcionar busca do domínio externo do certificado em rede local para acessar o IP interno do Qlik Sense Enterprise .....	26
5.2.7.	Adicionar registro no sistema local para evitar loopback de autenticação local no endereço de domínio externo.....	26
5.3.	Qlik Sense Enterprise .....	28
5.3.1.	Configurar “Proxy” (SSL browser certificate thumbprint) .....	28
5.3.2.	Configurar “Virtual proxy” (Host White list e Client Authentication Link) .....	28
5.4.	Qlik Sense Mobile .....	29
5.4.1.	Baixar e instalar aplicativo Qlik Sense no smartphone.....	29
5.4.2.	Acessar o endereço URI do Qlik Sense Enterprise pelo Browser do mobile .....	30
6.	Fontes .....	32
7.	Links interessantes .....	33

---

## 2. Cenário

Windows Server 2016

Qlik Sense Enterprise June 2019 Patch 2

---

## 3. Atenção

Não nos responsabilizamos por problemas técnicos ou erros mediante a utilização deste documento, a intenção é de organizar os procedimentos utilizados em um caso de sucesso

Realize os backups ou snapshots (se for máquina virtual) antes das operações

Foi utilizado usuário de instalação do Qlik Sense Enterprise para a maioria das operações

---

## 4. Requisitos

- IP externo fixo e porta disponível (Simplifica o processo)
  - Rota no Firewall (IP interno <-> IP externo)
  - Domínio FQDN externo (Para certificado SSL)
  - Certificado SSL (Conforme domínio FQDN externo)
  - Qlik Sense Enterprise
  - Aplicativo Qlik Sense Mobile (Android ou IOS)
- 

## 5. Procedimentos

### 5.1. Infraestrutura de rede

---

5.1.1. Solicitar a TI a criação de uma rota no servidor firewall/roteador (existe diferenças de fabricantes e modelos) para direcionar um IP externo com a porta (de preferência 443) para o IP interno do servidor Qlik Sense Enterprise com a porta (padrão 443)

Obs.: Utilizando a porta padrão 443, o usuário não precisará digitar a porta na URL.

Utilizando IP externo fixo, simplifica a estrutura e a manutenção (evitando utilizar DDNS e outros procedimentos)

---

5.1.2. Adquirir um domínio da internet e apontar para o IP externo que está direcionado para o servidor Qlik Sense Enterprise (confirme seção 5.1.1). Ex.: bi.cubotimize.com

Obs.: O endereço de domínio ou subdomínio (se for o caso) de internet deverá ser o mesmo utilizado para registrar o certificado SSL que posteriormente será solicitado a uma autoridade certificadora raiz confiável

---

## 5.2. Sistema Operacional

### 5.2.1. Instalar serviço IIS para posteriormente emitir informações em CSR

5.2.1.1. No servidor com o serviço Qlik Sense Enterprise, vamos instalar o IIS (Internet Information Services)

Obs.: Poderá instalar rapidamente o serviço IIS através do **PowerShell**, neste caso, poderá pular os passos da seção 5.2.1 após 5.2.1.1:

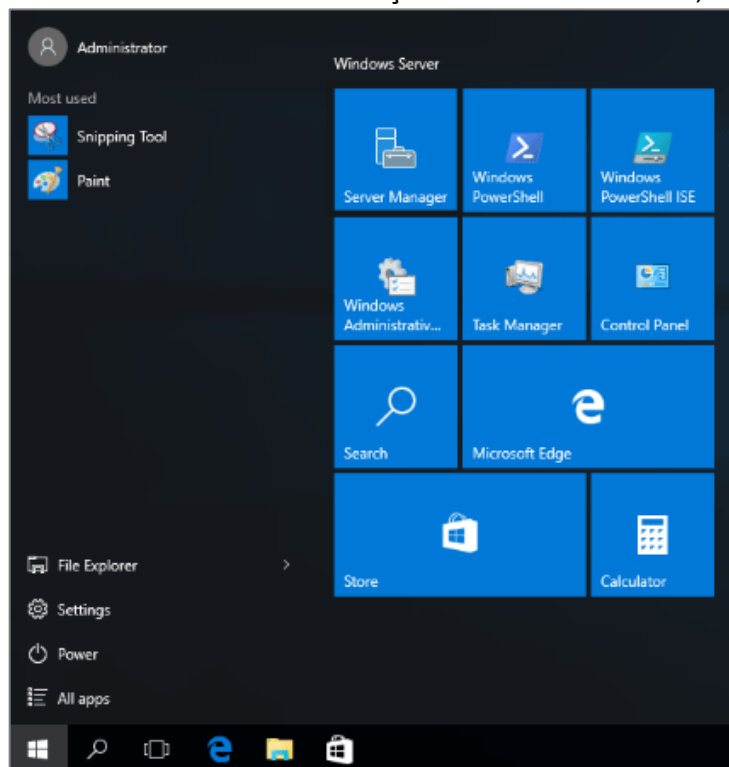
Comando: **Install-WindowsFeature -name Web-Server -IncludeManagementTools**

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

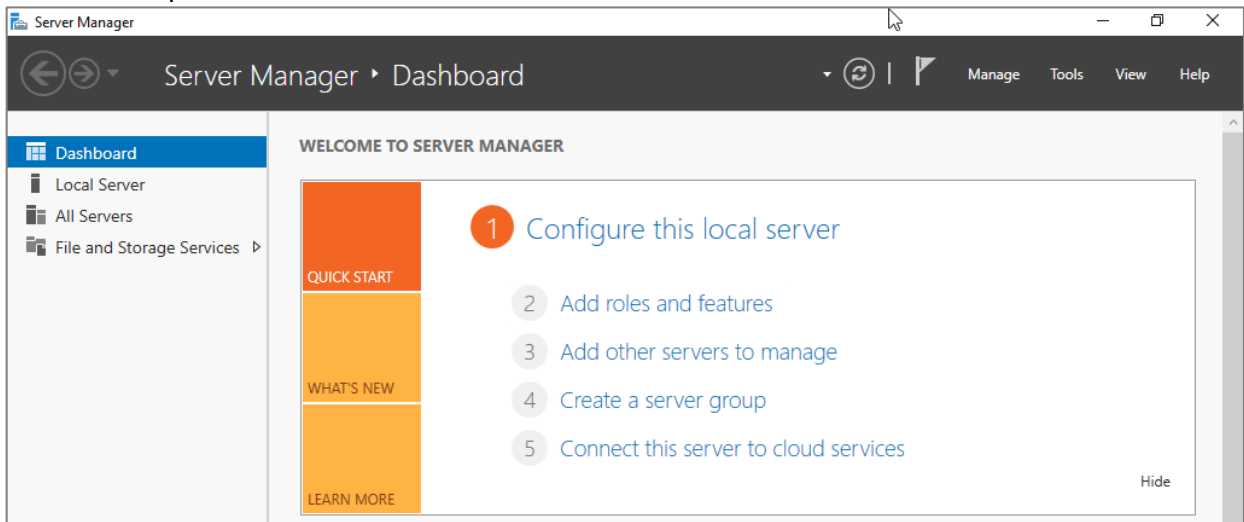
PS C:\Users\Administrator> Install-WindowsFeature -name Web-Server -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
-----
True     No                Success      {Common HTTP Features, Default Document, D...
```

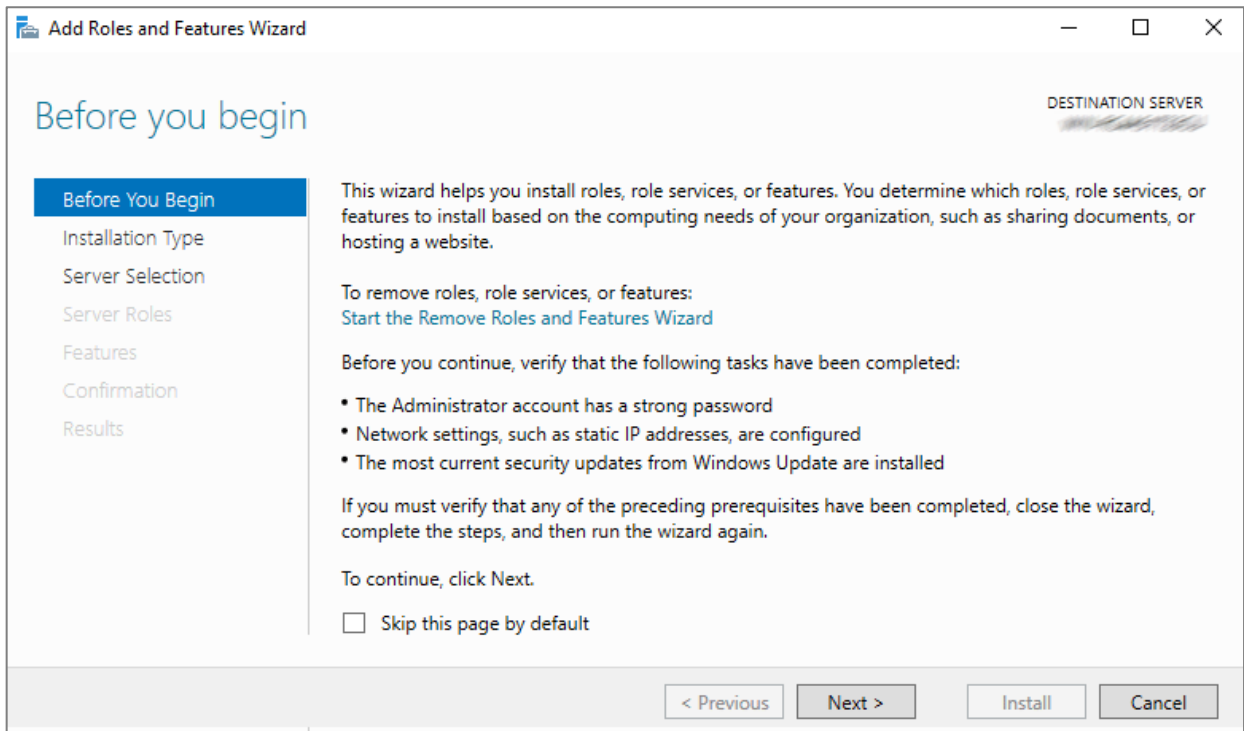
5.2.1.2. Alternativa a instalação do IIS: Menu **Iniciar**, abra **Server Manager**



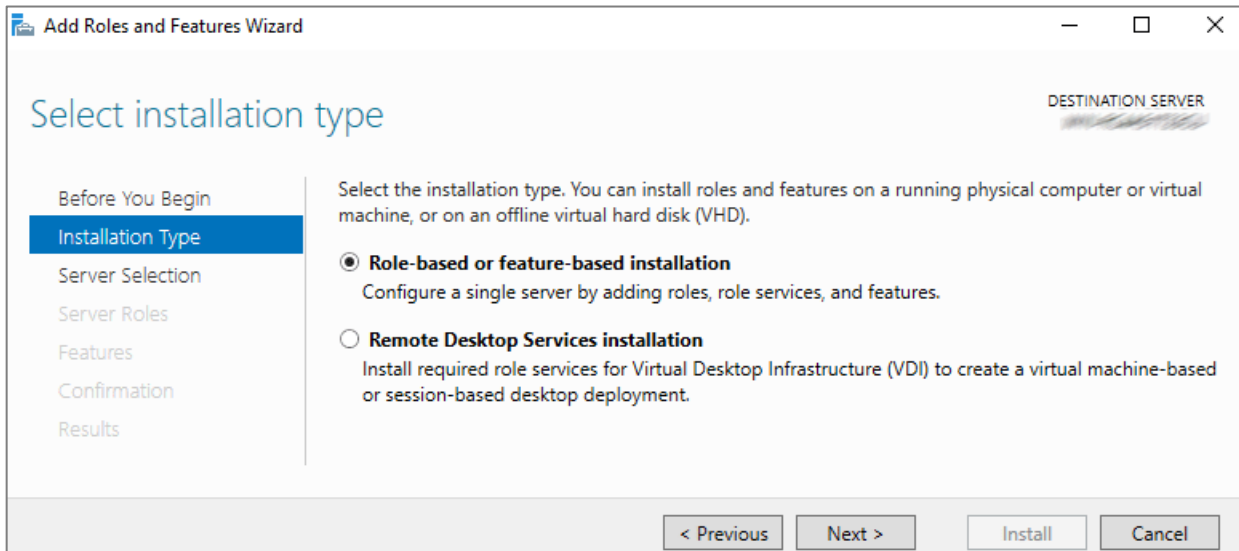
### 5.2.1.3. Clique em **Add roles and features**



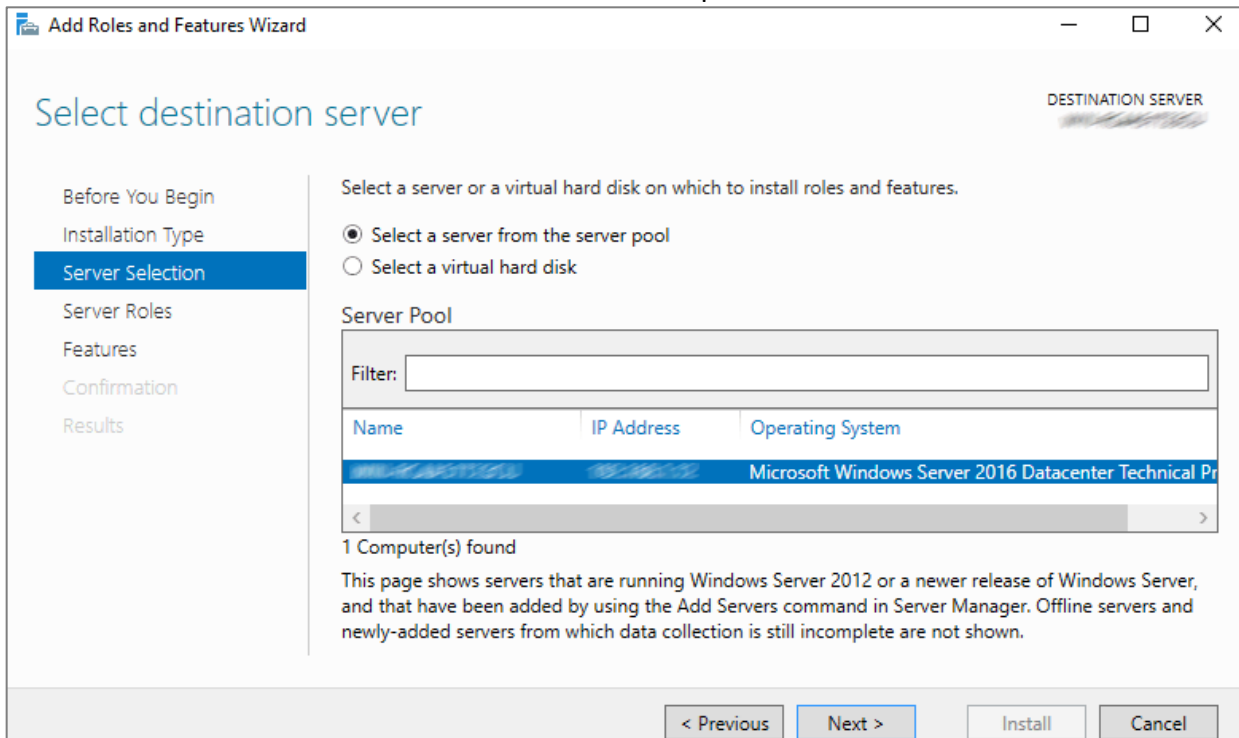
### 5.2.1.4. Na janela **Add Roles and Features Wizard**, na seção **Before You Begin**, simplesmente clique em **Next >**



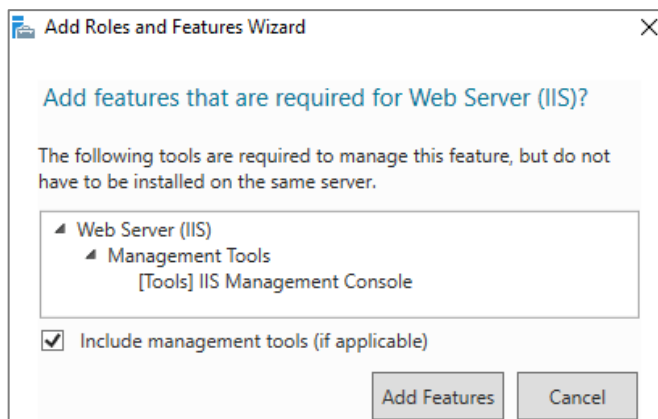
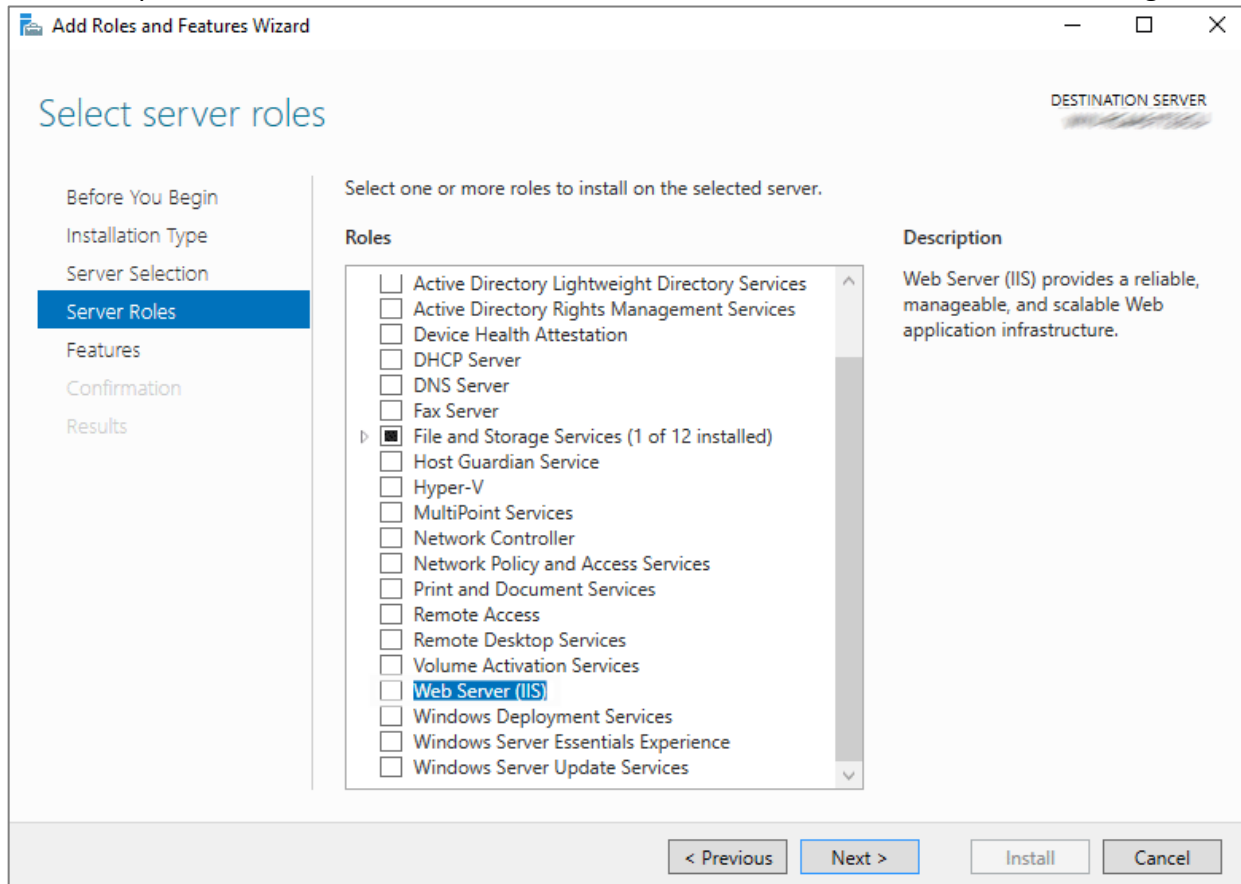
5.2.1.5. Na seção **Installation Type**, escolha **Role-based or feature-based installation** e clique em **Next >**



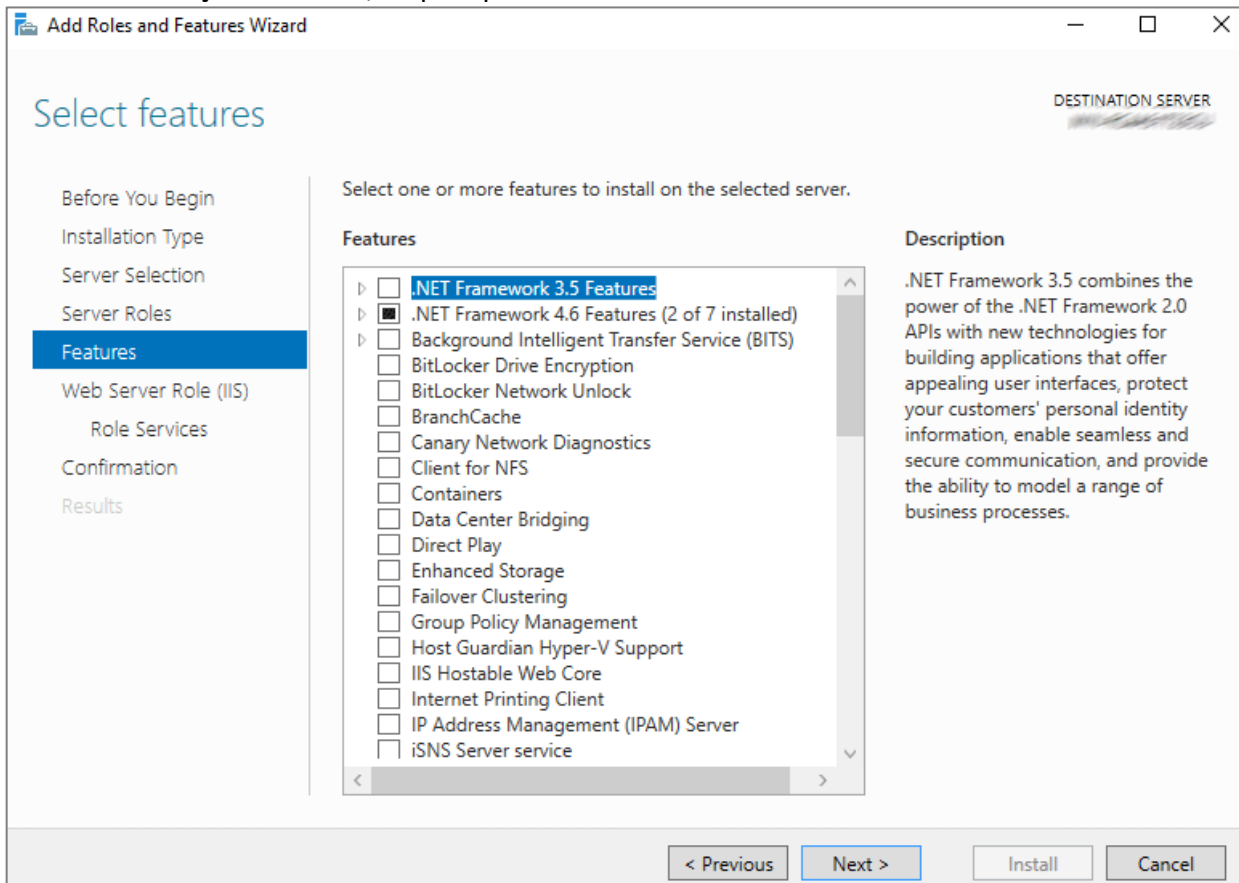
5.2.1.6. Na seção **Server Selection**, mantenha selecionado **Select a server from the server pool**, o nome do servidor local em **Server Pool** e clique em **Next >**



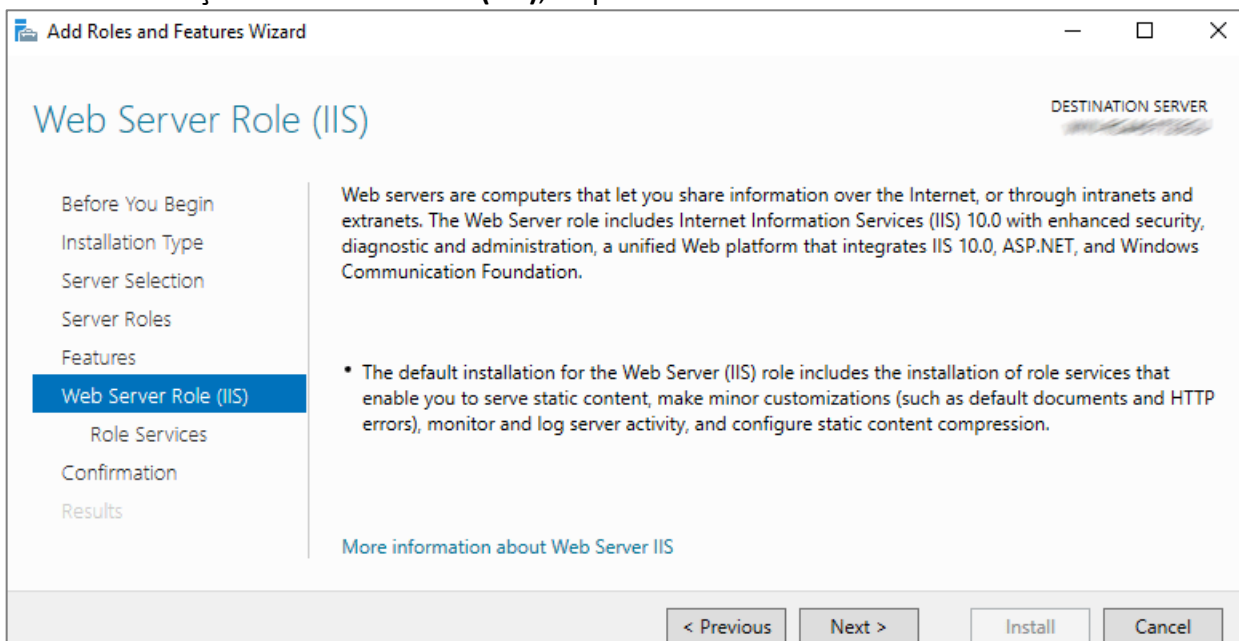
5.2.1.7. Na seção **Server Roles**, marque **Web Server (ISS)**, poderá aparecer uma janela informando que recursos adicionais são necessários, basta clicar em **Add Features** e em seguida **Next >**



### 5.2.1.8. Na seção **Features**, clique apenas em **Next >**

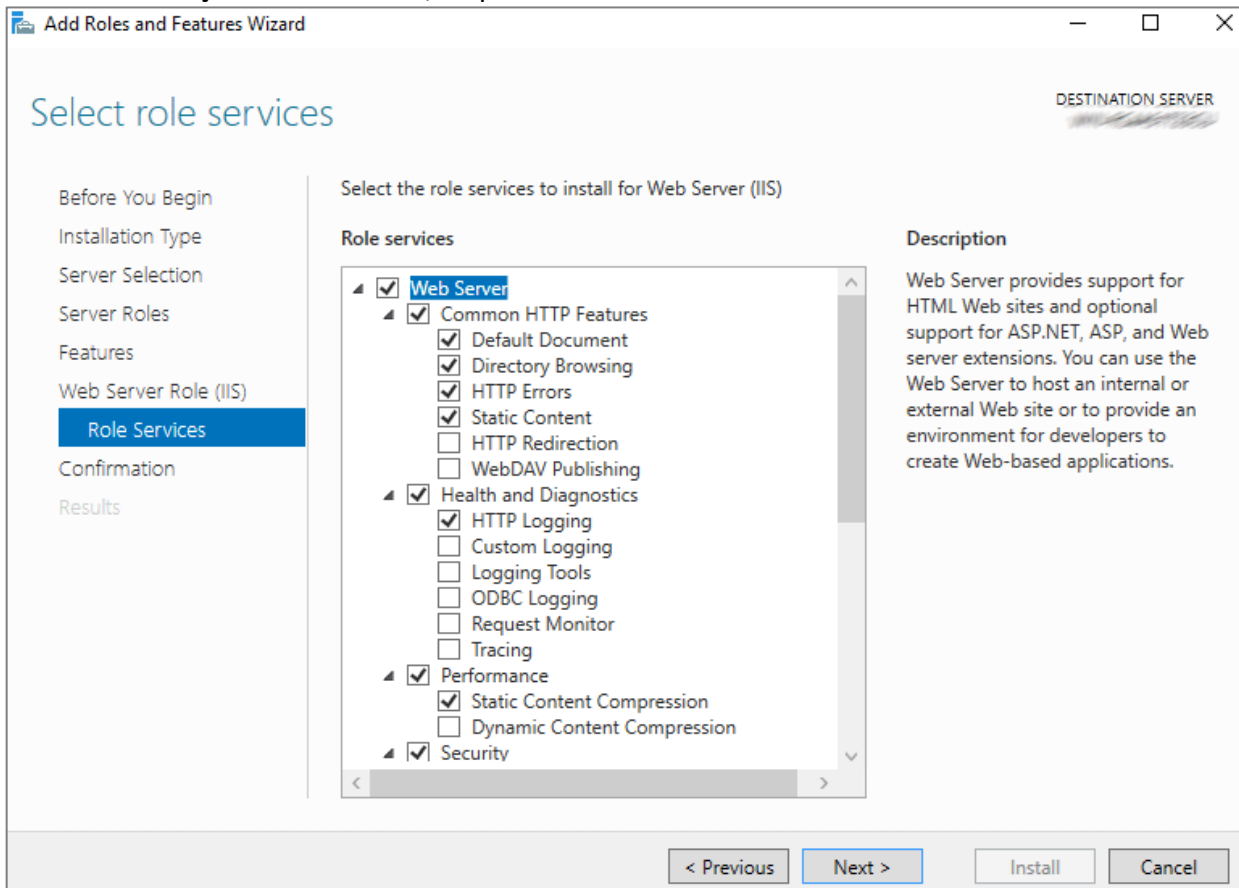


### 5.2.1.9. Na seção **Web Server Role (IIS)**, clique em **Next >**

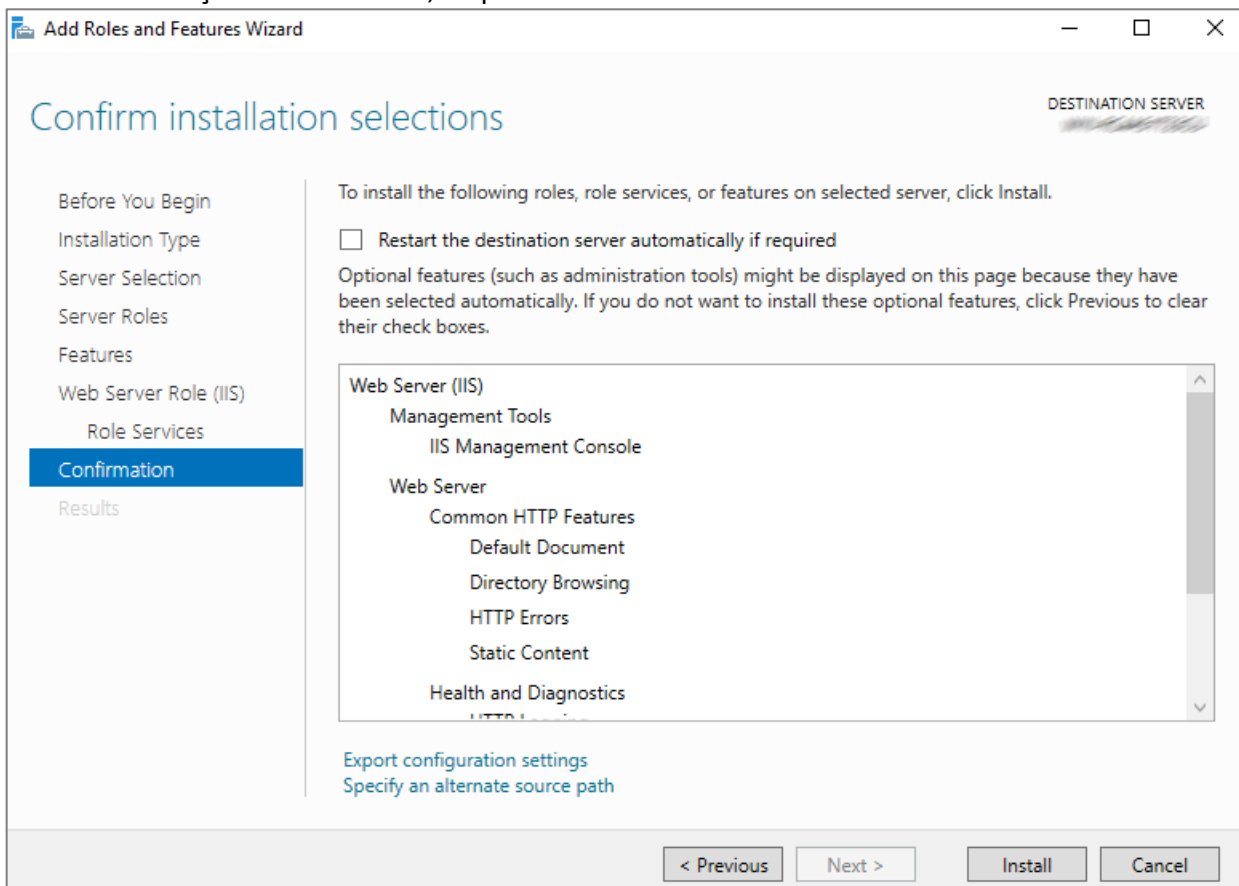




### 5.2.1.10. Na seção **Role Services**, clique em **Next >**

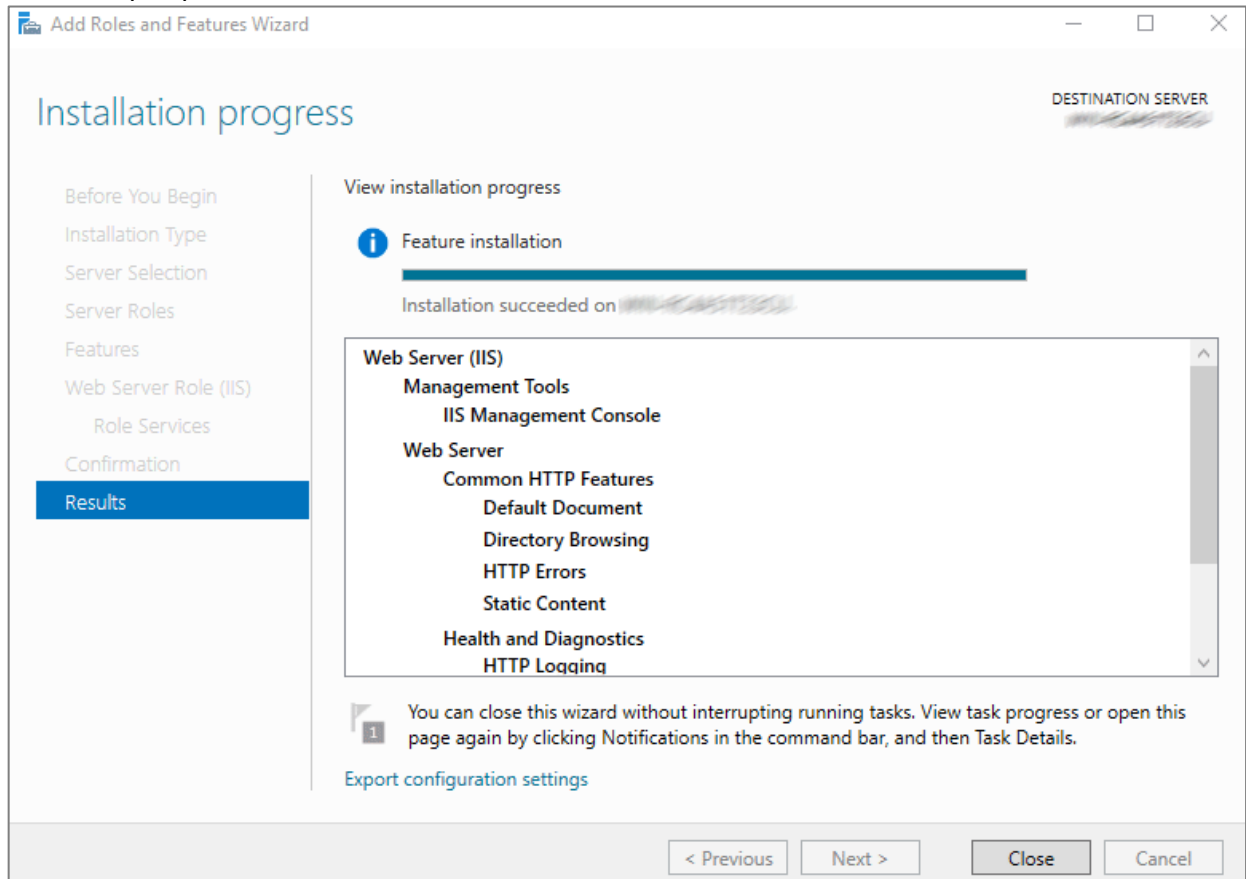


### 5.2.1.11. Na seção **Confirmation**, clique em **Install**

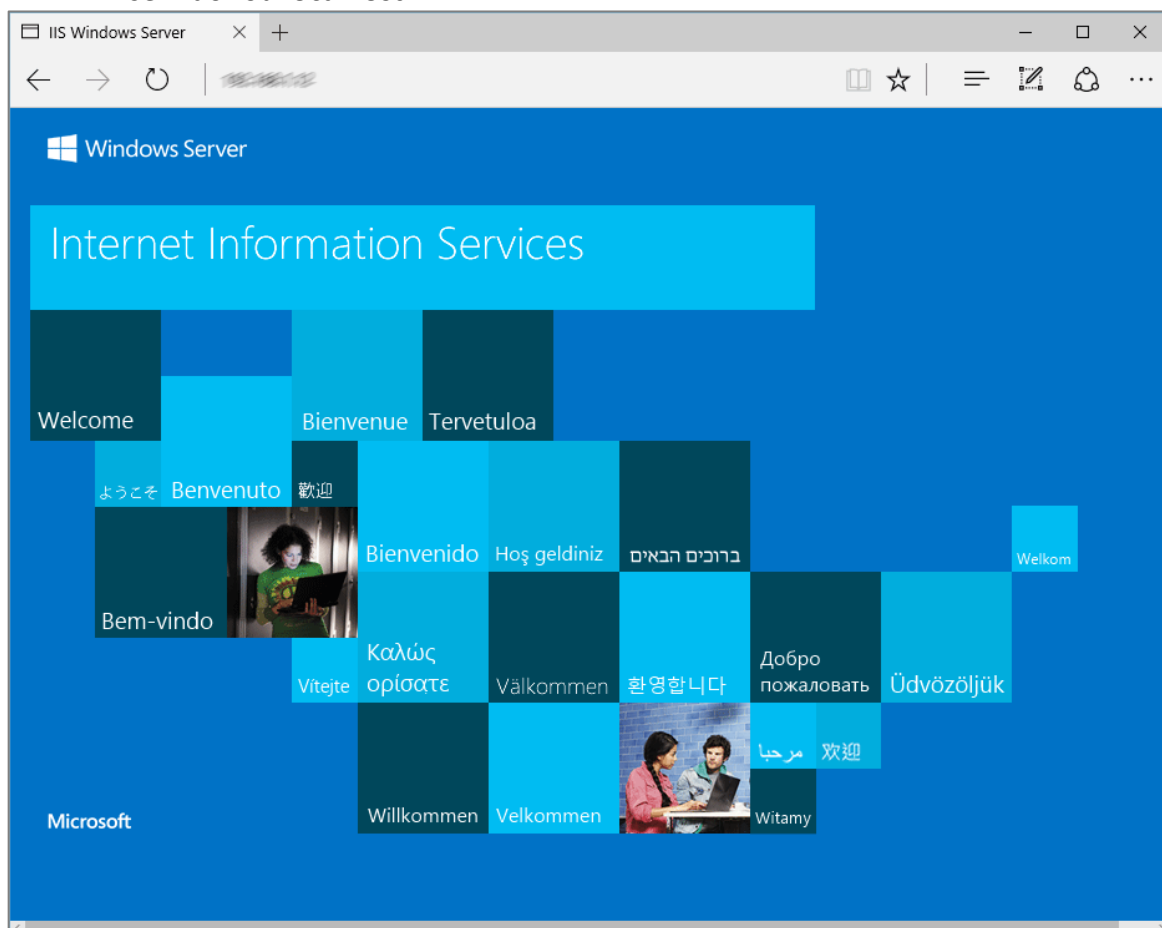


Obs.: Normalmente, não precisa reiniciar o servidor para a instalação deste serviço

5.2.1.12. Na seção **Results**, clique em **Close**, neste ponto o serviço ISS será inicializado na porta 80 por padrão

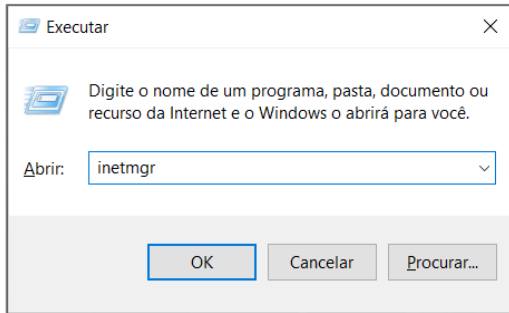


5.2.1.13. Poderá confirmar se o serviço está operante abrindo o navegador e acessando o IP do servidor ou **localhost**

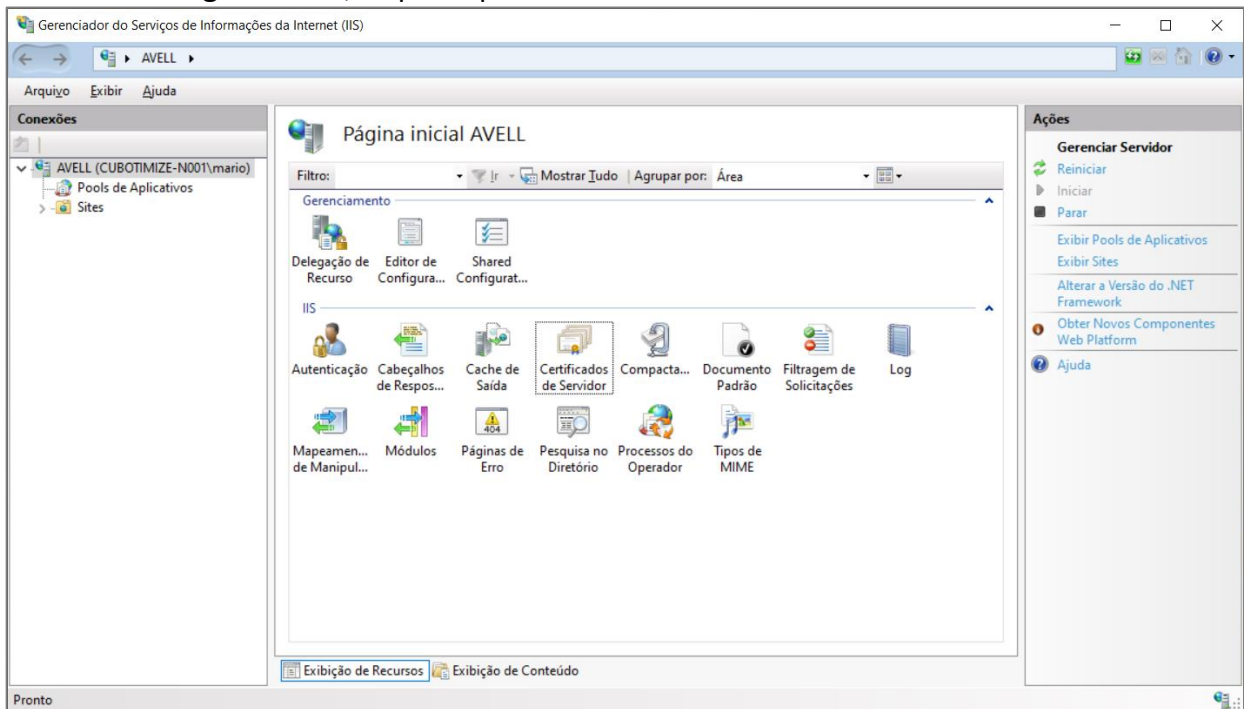


## 5.2.2. Preparar informações CSR para emissão do certificado

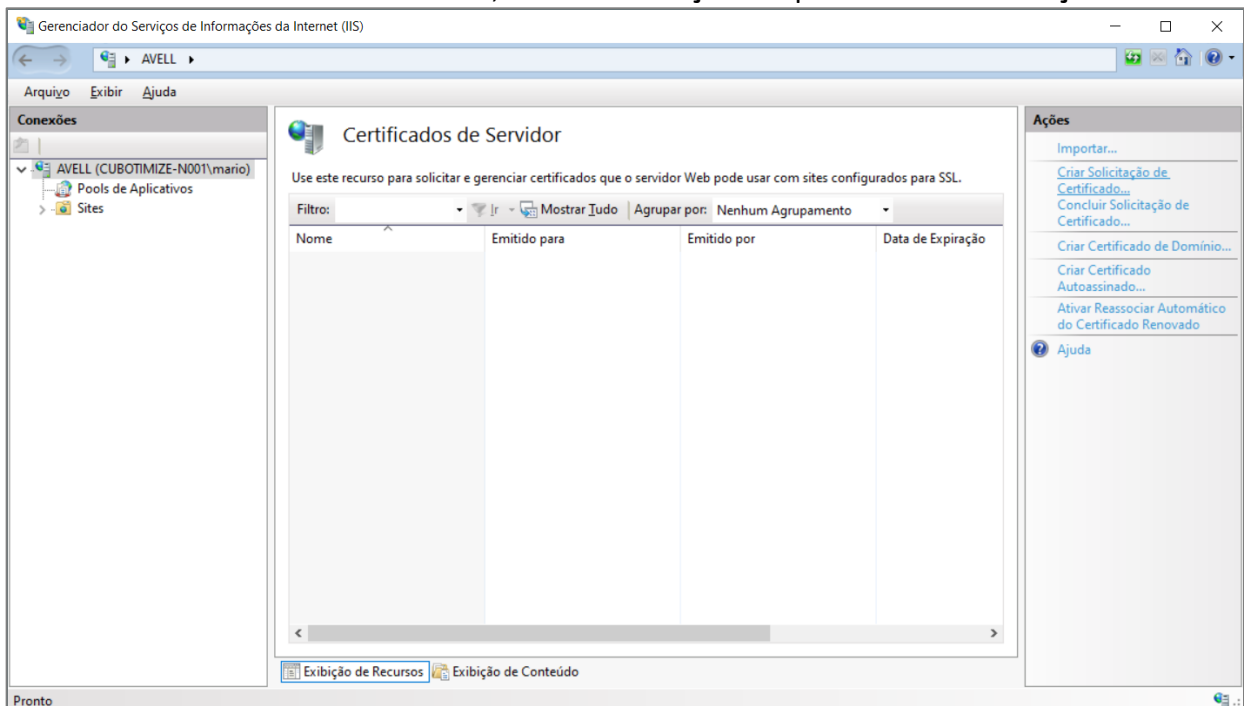
### 5.2.2.1. Em **Iniciar** (bandeira do Windows), pesquise e abra **inetmgr** (ou via **Iniciar+R**)



### 5.2.2.2. Na **Página Inicial**, clique duplo em **Certificados de Servidor**



### 5.2.2.3. Em **Certificados de Servidor**, no menu de **Ações** clique em **Criar Solicitação de Certificado...**



5.2.2.4. Na janela **Solicitar Certificado** em **Propriedades de Nome Distinto**, preencha os campos, clique em **Avançar**:

Obs.: Caracteres inválidos: < > ~ ! @ # \$ % ^ \* / \ ( ) ? &

Desconsiderar acentuações nos preenchimentos

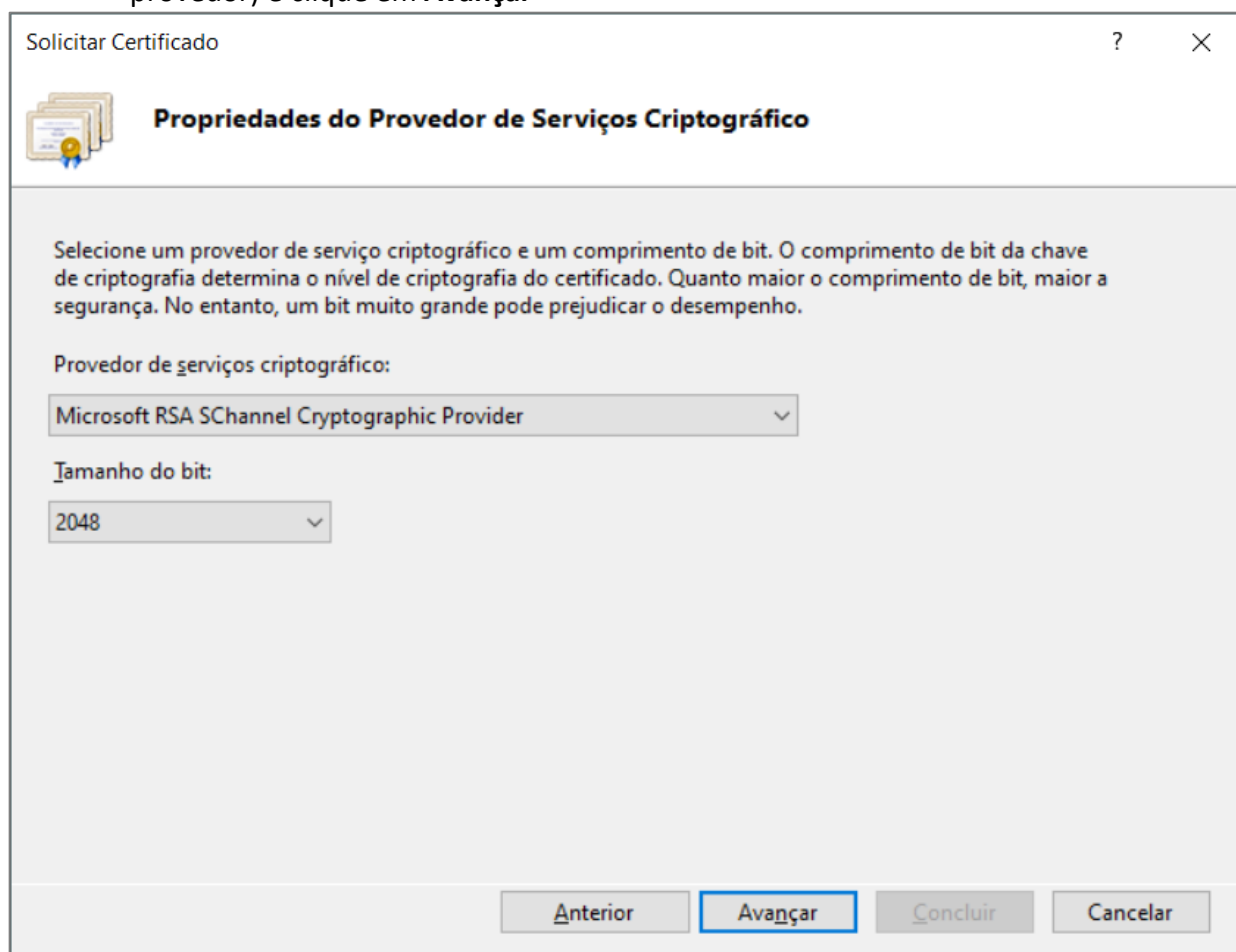
- **Nome comum:** Insira o endereço FQDN (Nome de Domínio Completamente Qualificado), conforme domínio desejado para certificado e Domínio externo.  
Obs.: Se adquirir um certificado do tipo DV (Validação de Domínio), certifique de colocar o endereço correto como bi.cubotimize.com.br que é diferente de www.cubotimize.com
- **Organização:** Insira o nome completo da empresa conforme escrito no cartão de CNPJ
- **Unidade organizacional:** Insira o departamento responsável pelo certificado, exemplo: TI
- **Cidade/localidade:** Insira a cidade da empresa sem abreviação, conforme cartão de CNPJ
- **Estado/província:** Insira o Estado da empresa sem abreviação, conforme cartão de CNPJ
- **País/região:** Insira o país abreviado no padrão ISO (duas letras), conforme cartão de CNPJ  
Vide exemplo abaixo para evitar erros de preenchimento:

A captura de tela mostra a janela de software 'Solicitar Certificado' com o título 'Propriedades de Nome Distinto'. O ícone de uma pasta de certificados está visível no canto superior esquerdo. Abaixo do título, há uma instrução: 'Especifique as informações necessárias do certificado. Estado/província e Cidade/localidade devem ser especificados como nomes oficiais e não podem conter abreviações.' O formulário contém os seguintes campos:


Nome comum:	bi.cubotimize.com
Organização:	Cubotimize Solucoes Em Inteligencia Tecnologica Eireli
Unidade organizacional:	TI
Cidade/localidade:	Itaborai
Estado/província:	Rio de Janeiro
País/região:	BR

Na base da janela, há quatro botões: 'Anterior', 'Avançar' (destacado com um contorno azul), 'Concluir' e 'Cancelar'.

5.2.2.5. Em **Propriedades do Provedor de Serviços Criptográfico**, certifique que em **Provedor de serviços criptográfico** esteja **Microsoft RSA SChannel Cryptographic Provider**, em **Tamanho do bit** esteja **2048** (a maioria das autoridades certificadoras exigem, mas consulte o provedor) e clique em **Avançar**



Solicitar Certificado

 **Propriedades do Provedor de Serviços Criptográfico**

Selecione um provedor de serviço criptográfico e um comprimento de bit. O comprimento de bit da chave de criptografia determina o nível de criptografia do certificado. Quanto maior o comprimento de bit, maior a segurança. No entanto, um bit muito grande pode prejudicar o desempenho.

Provedor de serviços criptográfico:

Microsoft RSA SChannel Cryptographic Provider

Tamanho do bit:

2048

Anterior Avançar Concluir Cancelar

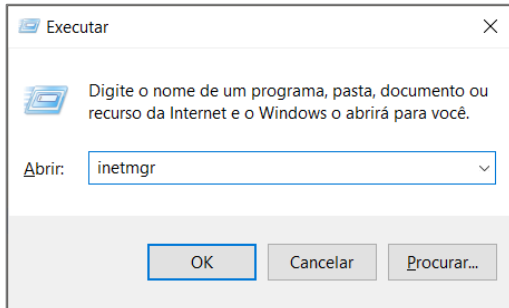


5.2.2.8. Aguarde receber o certificado SSL no formato **CER** para continuar com as configurações da seção 5.2.3

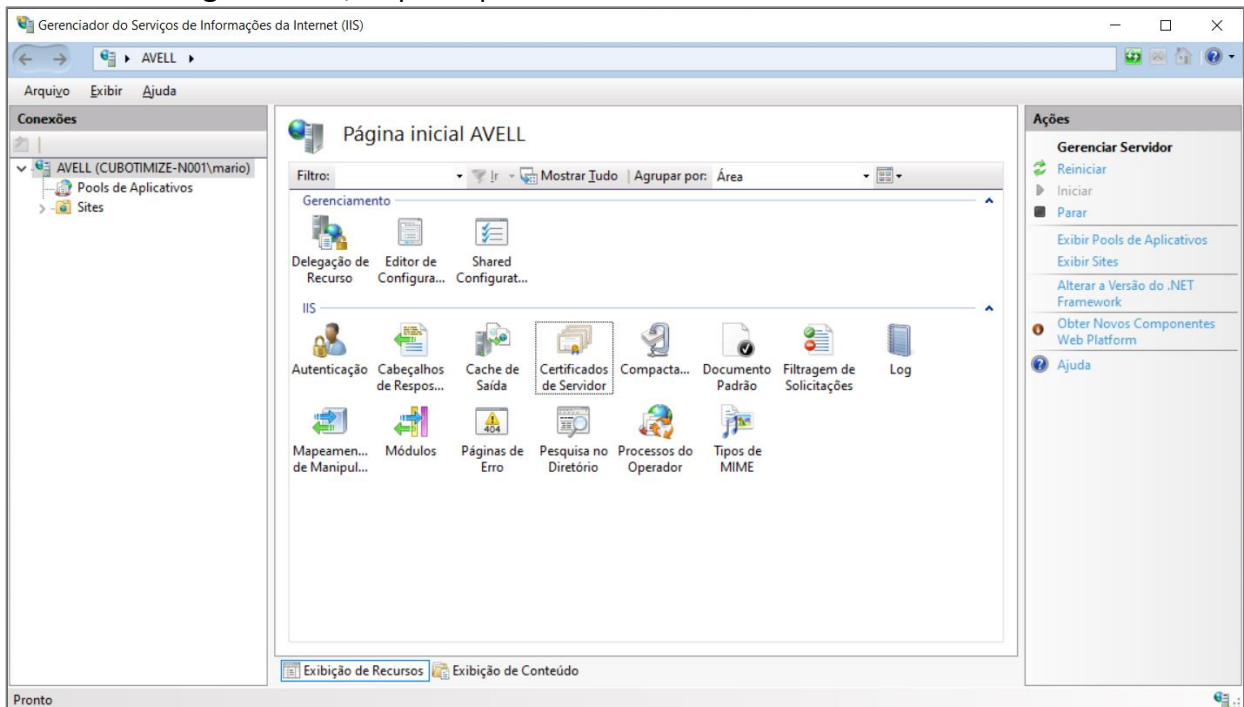
Obs.: Em alguns casos, deverá copiar o bloco de texto recebido por e-mail pelo provedor e abrir um bloco de notas e salvar os dados recebidos com a extensão **CER**

### 5.2.3. Concluir solicitação de certificado no servidor

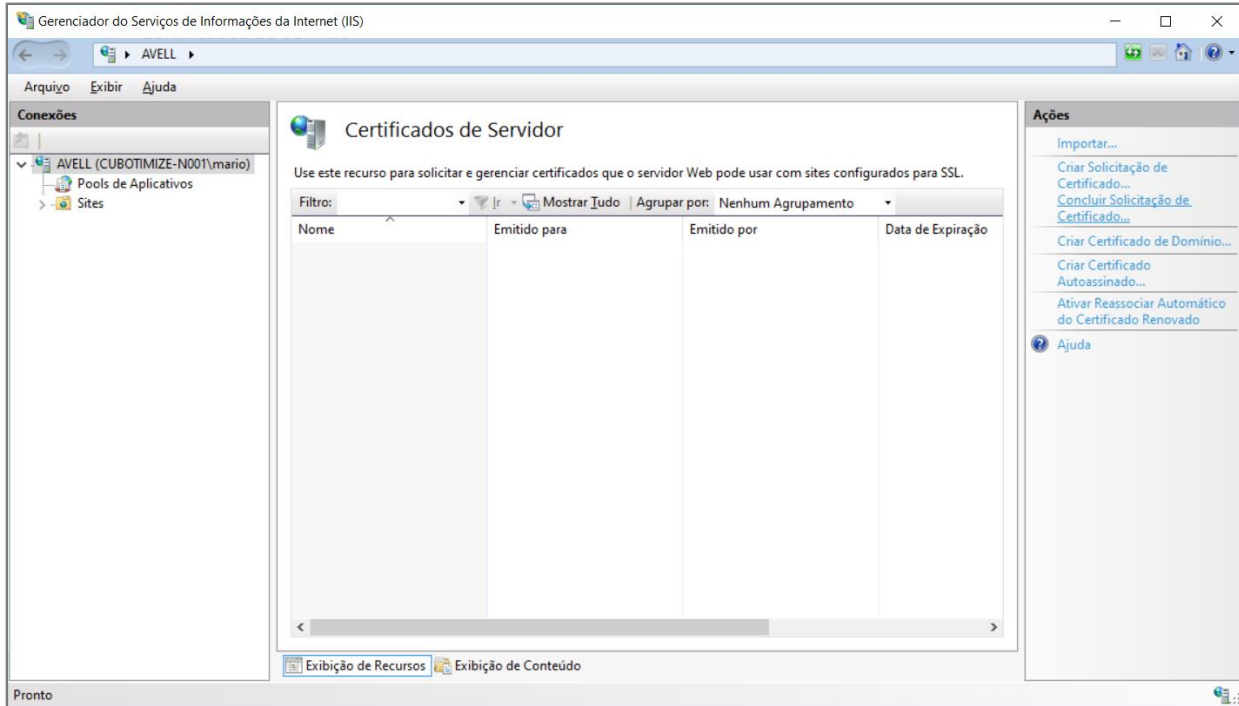
5.2.3.1. Em **Iniciar** (bandeira do Windows), pesquise e abra **inetmgr** (Ou via **Iniciar+R**)



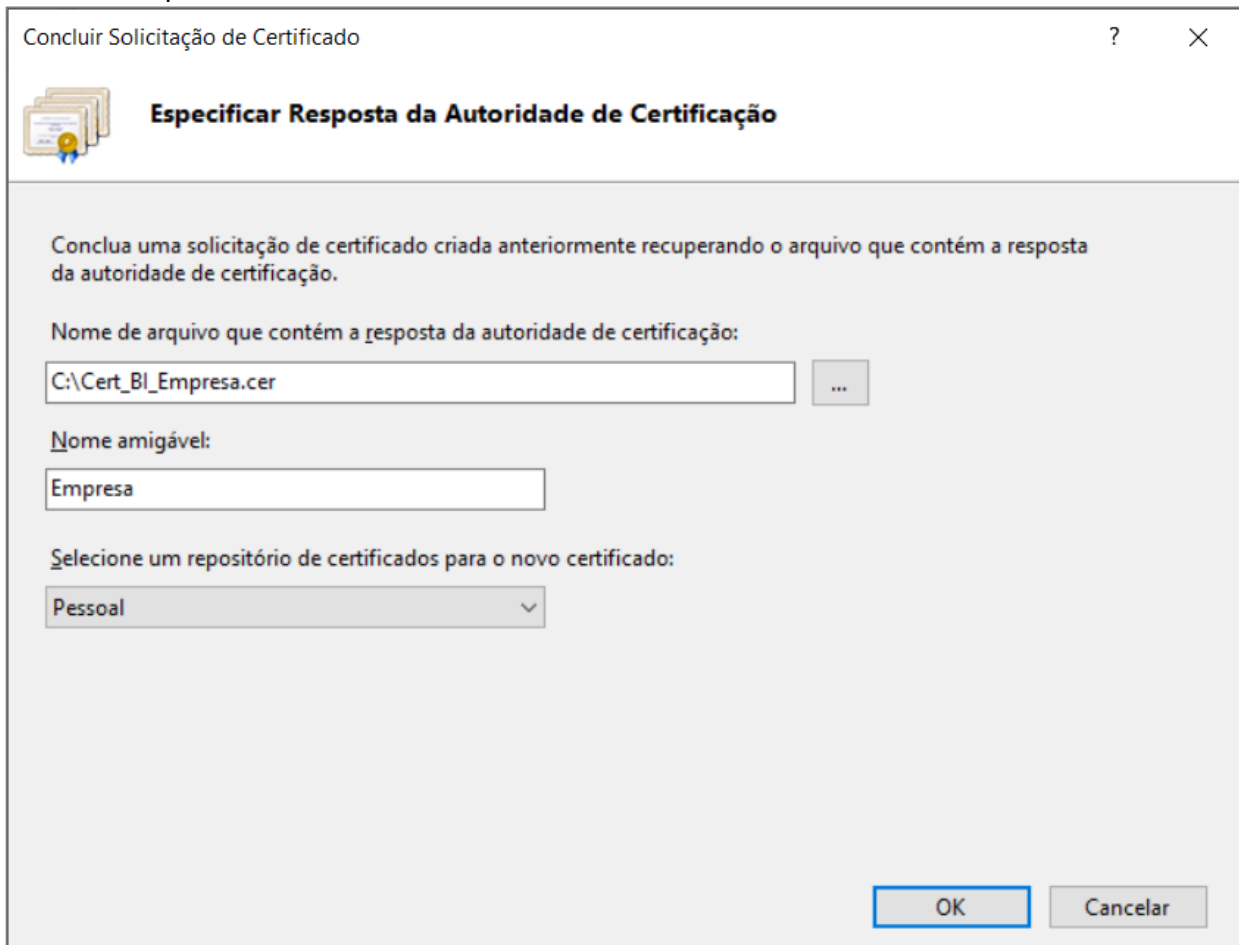
5.2.3.2. Na **Página Inicial**, clique duplo em **Certificados de Servidor**



5.2.3.3. Em **Certificados de Servidor**, no menu de **Ações** (no lado direito), clique em **Concluir Solicitação de Certificado...**

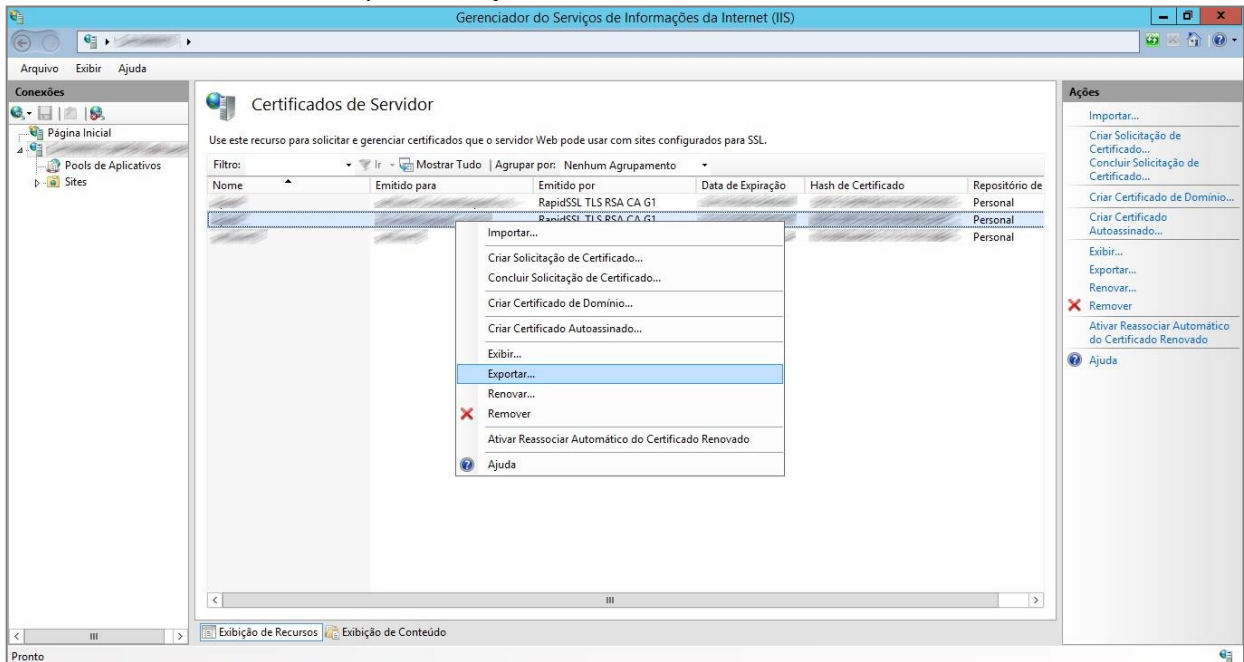


5.2.3.4. Em **Concluir Solicitação de Certificado**, insira **Nome de arquivo que contém a resposta da autoridade de certificação**, podendo pesquisar em [...], insira **Nome amigável** e em seguida clique em **OK**

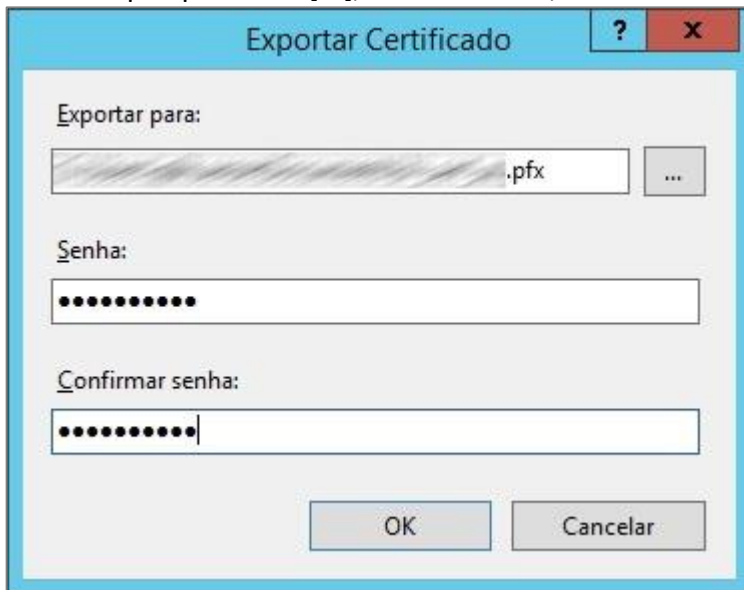




5.2.3.5. Em **Certificados de Servidor**, aparecerá o certificado em questão na lista, clique com o botão direito e clique em **Exportar...**

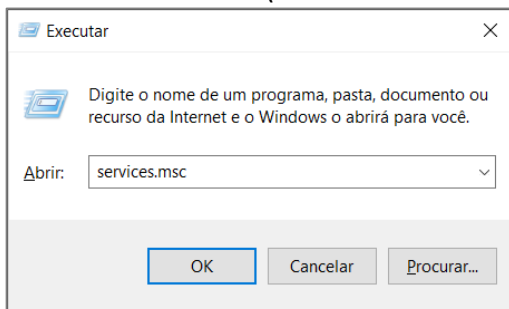


5.2.3.6. Em **Exportar Certificado**, insira o local **Exportar para** com o formato **PFX**, podendo pesquisar em [...], insira a **Senha**, **Confirmar senha** e clique em **OK**

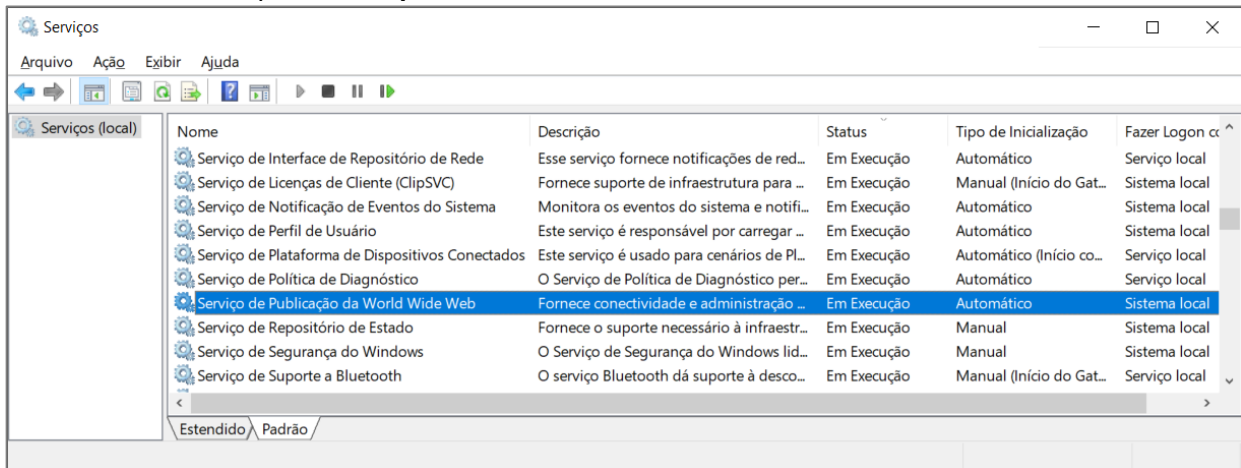


## 5.2.4. Desativar serviço IIS

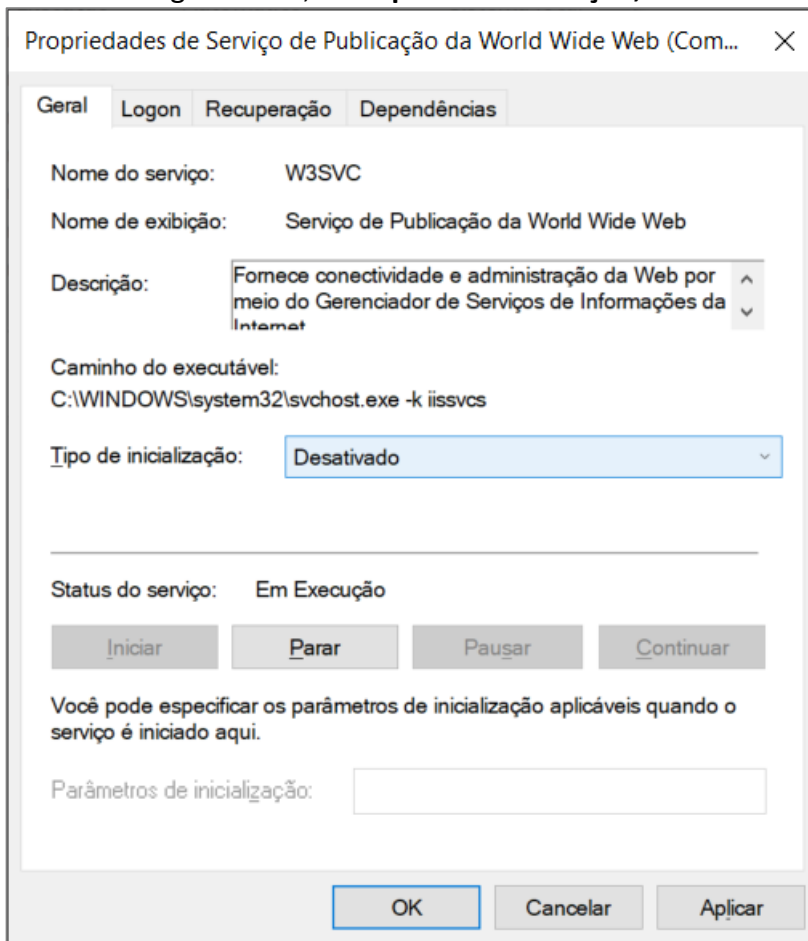
5.2.4.1. Em **Iniciar** (bandeira do Windows), pesquise e abra **services.msc** (Ou via **Iniciar+R**)



5.2.4.2. Na lista, clique com botão direito sobre o serviço **Serviço de Publicação da World Wide Web** e clique em **Propriedades**

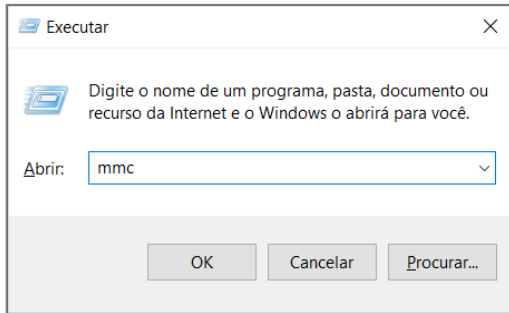


5.2.4.3. Na guia **Geral**, em **Tipo de inicialização**, escolha **Desativado** e em seguida em **OK**

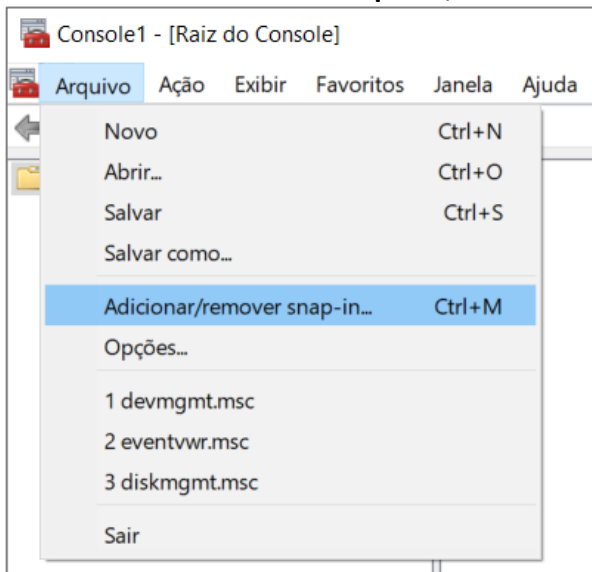


## 5.2.5. Importar certificado SSL no servidor onde o Qlik Sense Enterprise está instalado

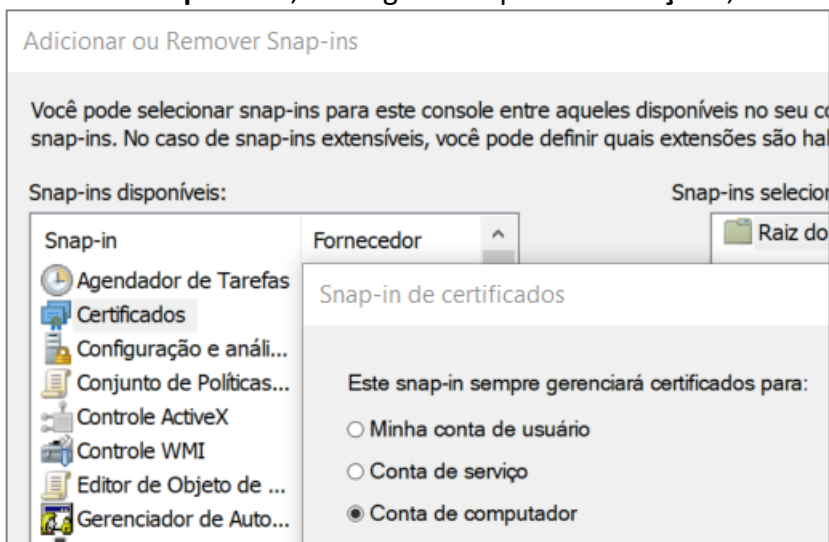
### 5.2.5.1. Em **Iniciar** (bandeira do Windows), pesquise e abra **mmc** (Ou via **Iniciar+R**)



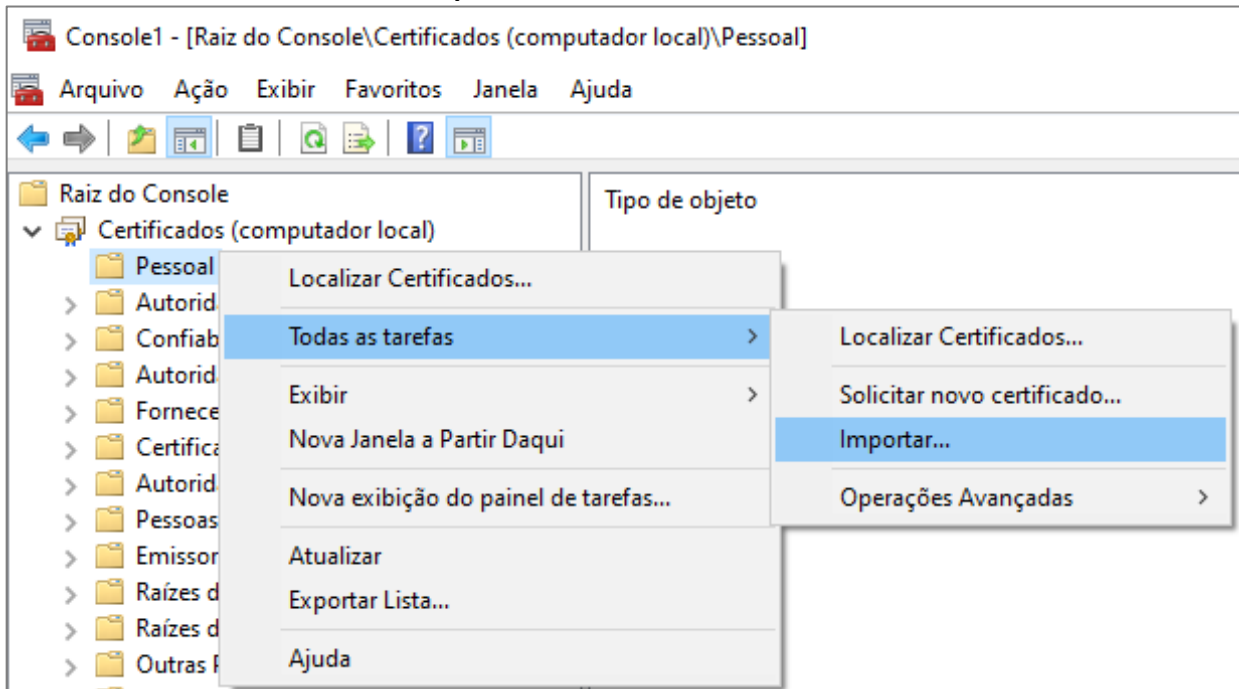
### 5.2.5.2. Em **mmc** vá em **Arquivo / Adicionar/remover snap-in** (Ctrl+M)



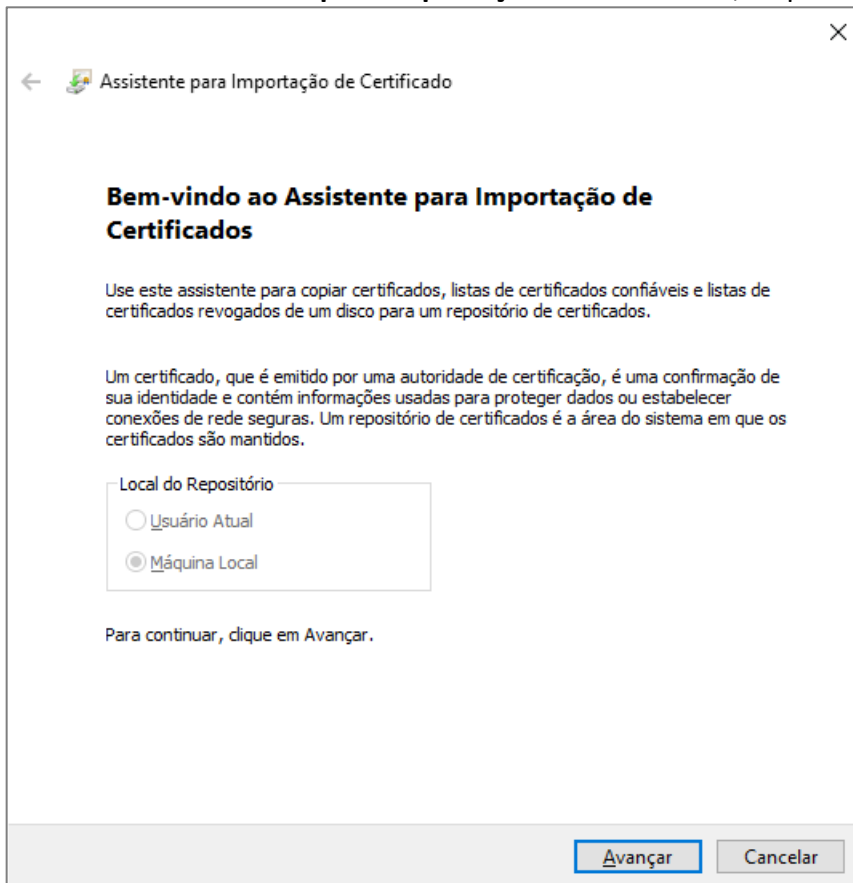
### 5.2.5.3. Em **Adicionar ou Remover Snap-ins**, selecione **Certificados** e escolha **Conta de computador**, em seguida clique em **Avançar >**, **Concluir** e **OK**



5.2.5.4. Expanda **Certificados (computador local)**, clique com o botão direito sobre **Pessoal** e clique em **Todos as tarefas / Importar...**



5.2.5.5. Em **Assistente para Importação de Certificado**, clique em **Avançar**



5.2.5.6. Procure o certificado **PFX** que foi exportado pelo IIS (seção 5.2.3 Concluir solicitação de certificado no servidor onde o Qlik Sense Enterprise está instalado) e clique em **Avançar**

← Assistente para Importação de Certificado

**Arquivo a Ser Importado**  
Especifique o arquivo que você deseja importar.

Nome do arquivo:  
.pfx

Observação: mais de um certificado pode ser armazenado em um único arquivo nos seguintes formatos:

- Troca de Informações Pessoais - PKCS nº 12 (.PFX,.P12)
- Padrão de Sintaxe de Mensagem Criptografada - PKCS nº7 (.P7B)
- Repositório de Certificados Serializado da Microsoft (.SST)

5.2.5.7. Preencha o campo **Senha**, selecione a opção **Marcar esta chave como exportável...** (opcional para backup) e em seguida clique em **Avançar**

← Assistente para Importação de Certificado

**Proteção de chave privada**  
Para manter a segurança, a chave privada foi protegida com uma senha.

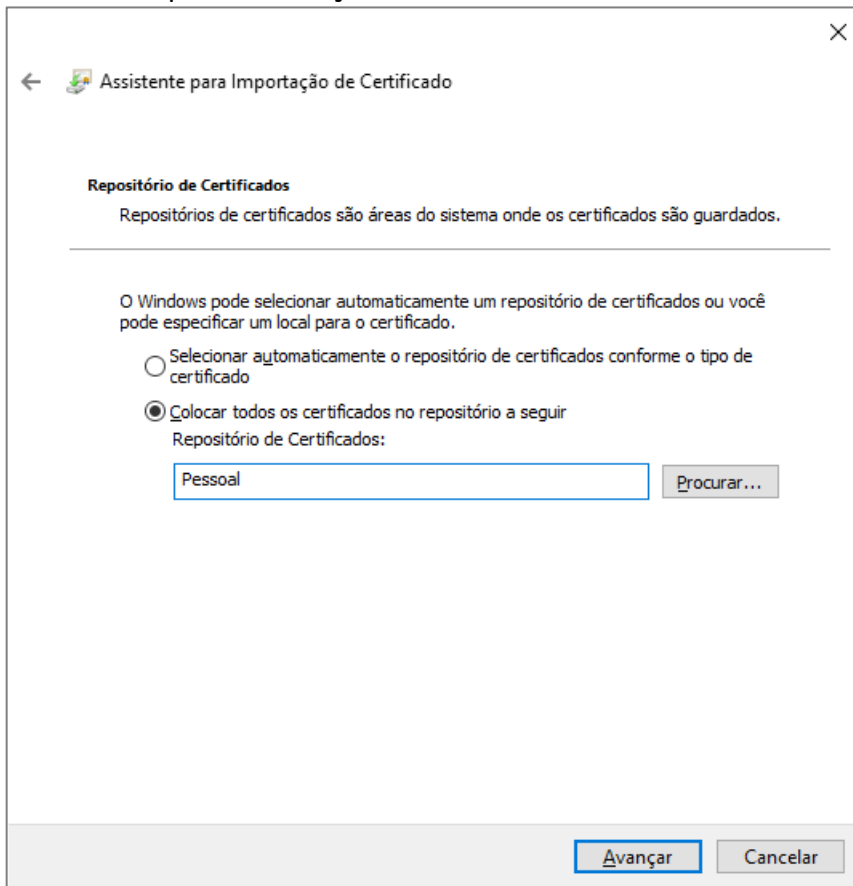
Digite a senha da chave privada.

Senha:  
  Exibir Senha

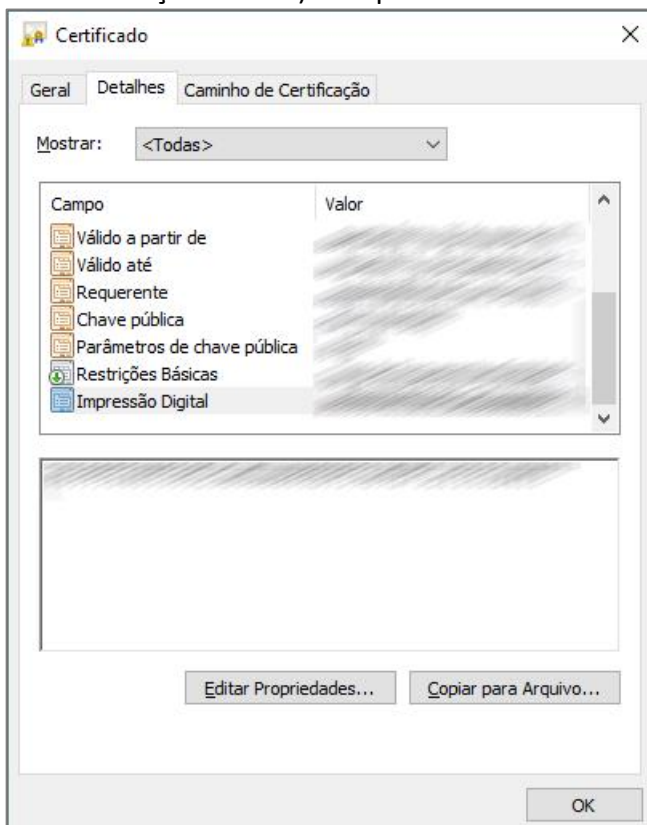
Opções de Importação:

- Habilitar proteção de chaves privadas fortes. Se habilitar essa opção, você será avisado sempre que a chave privada for usada por um aplicativo.
- Marcar esta chave como exportável. Isso possibilitará o backup ou o transporte das chaves posteriormente.
- Incluir todas as propriedades estendidas.

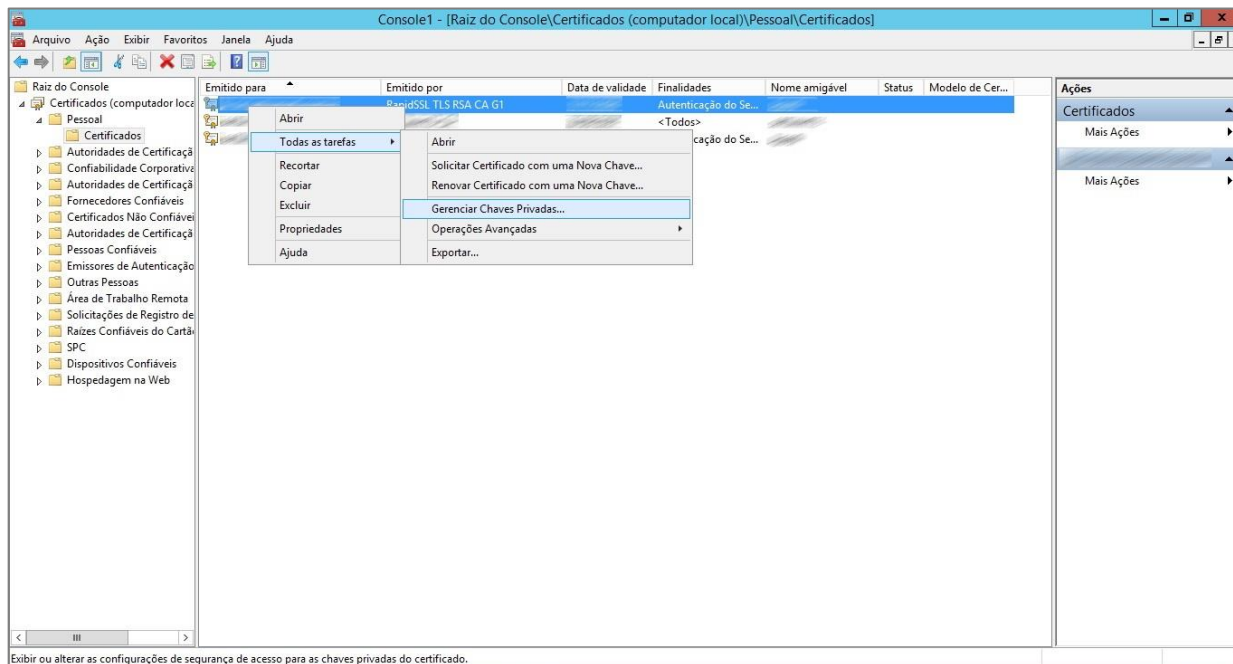
### 5.2.5.8. Clique em **Avançar** e em **Concluir**



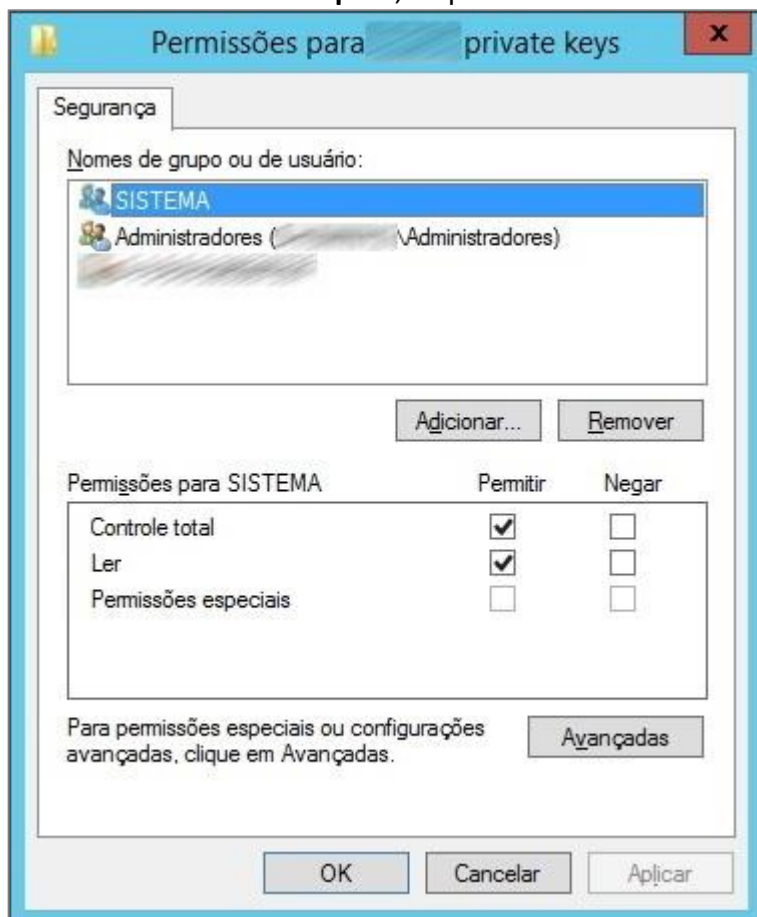
5.2.5.9. Duplo clique sobre o certificado instalado, vá na guia **Detalhes**, clique no campo **Impressão Digital**, na caixa de texto abaixo copie tudo inclusive com espaços entre as letras se houver (guarde para posteriormente inserirmos em **SSL browser certificate thumbprint** no **QMC**, seção 5.3.1.1) e clique em **OK**



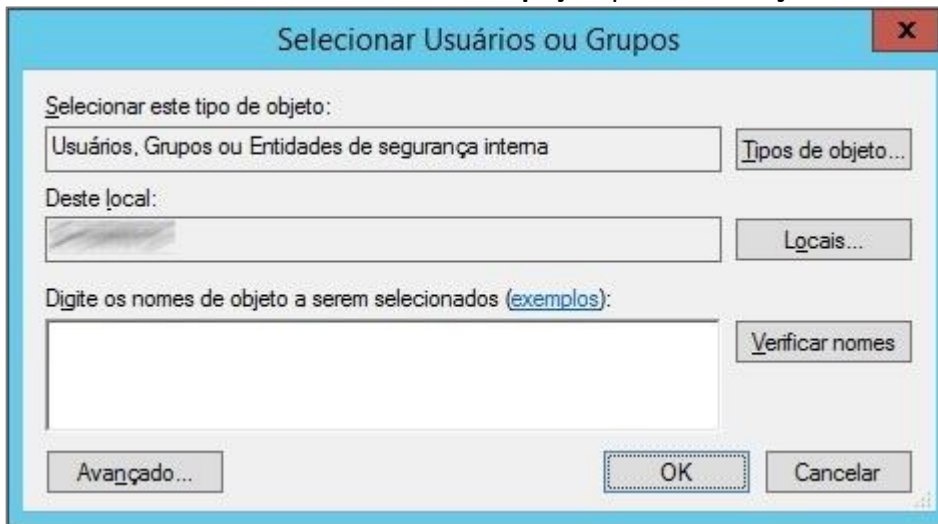
### 5.2.5.10. Clique com botão direito sobre o certificado importado e clique em **Todas as tarefas / Gerenciar Chaves Privadas...**



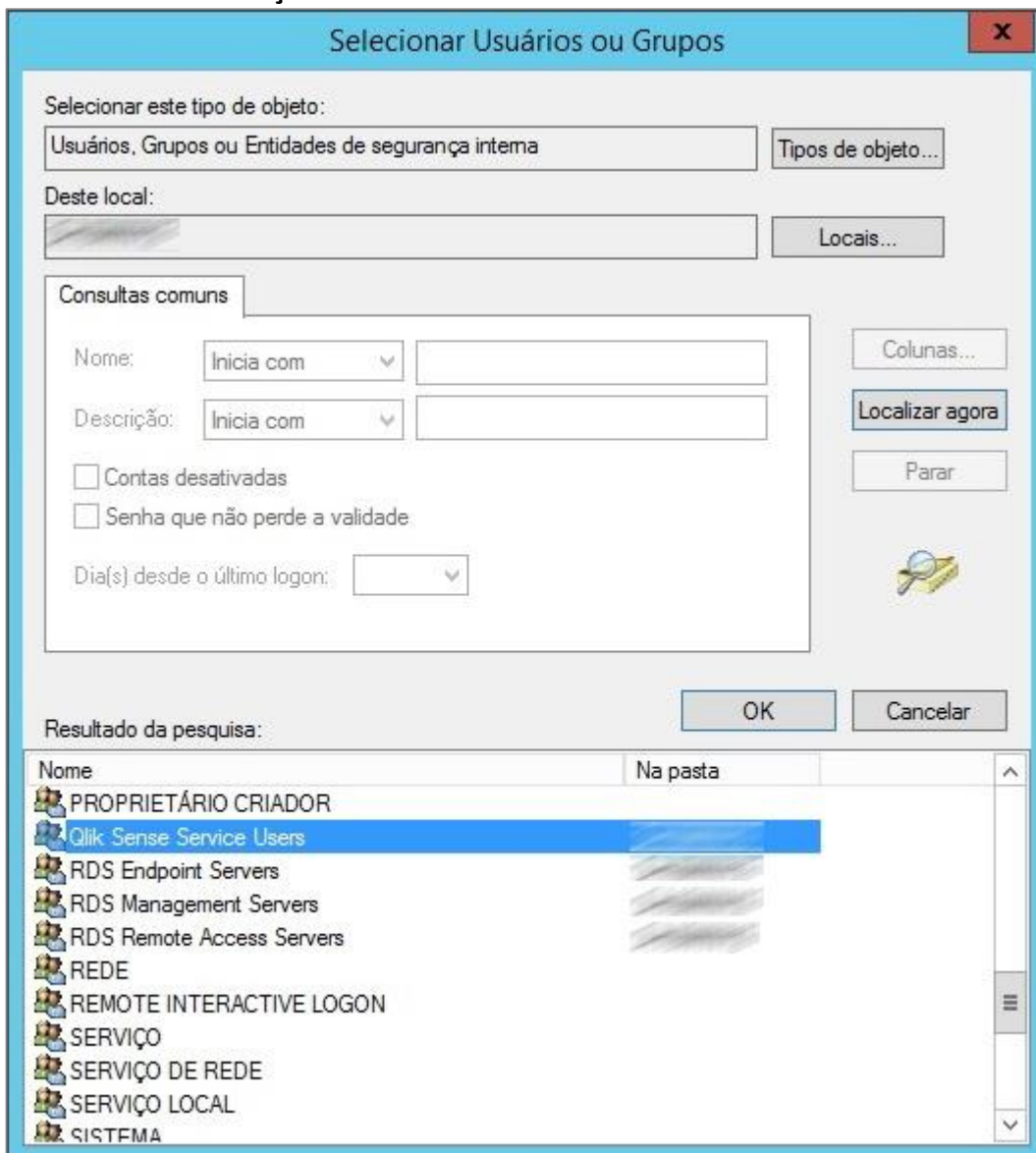
### 5.2.5.11. Em **Permissões para**, clique em **Adicionar...**



5.2.5.12. Em **Selecionar Usuário ou Grupo**, clique em **Avançado...**



5.2.5.13. Para poder pesquisar todos os grupos locais, altere **Locais...**, selecione a primeira opção da lista (nome do computador local) e **OK**, clique em **Localizar agora**, em seguida na lista **Resultado da pesquisa**, escolha **Qlik Sense Service Users** e clique em **OK** para concluir o modo **Avançado**

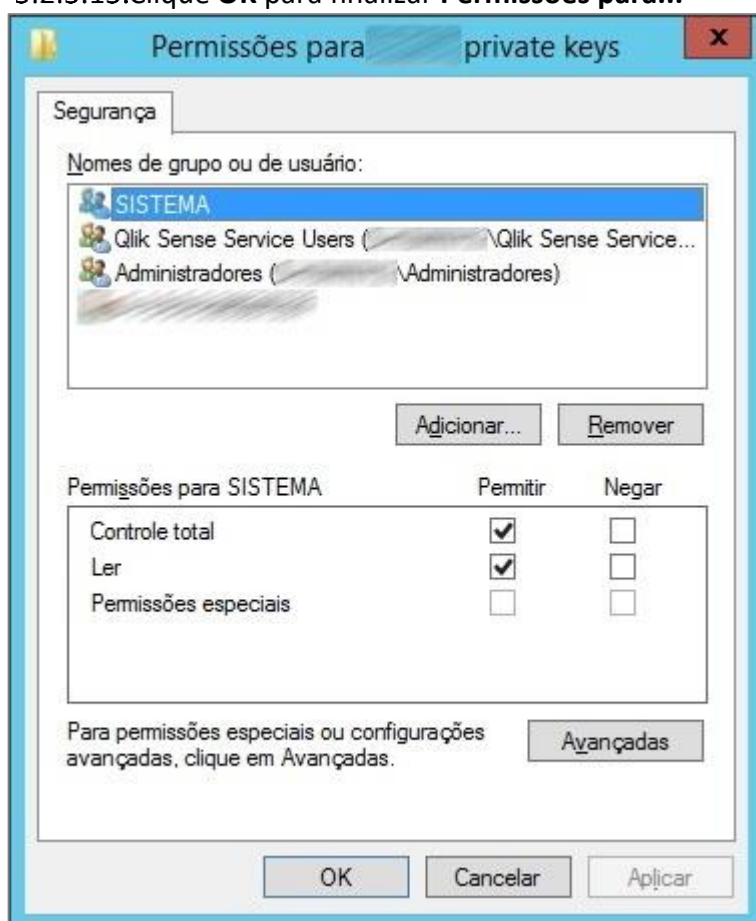




#### 5.2.5.14. Clique **OK** para concluir **Selecionar Usuários ou Grupos**



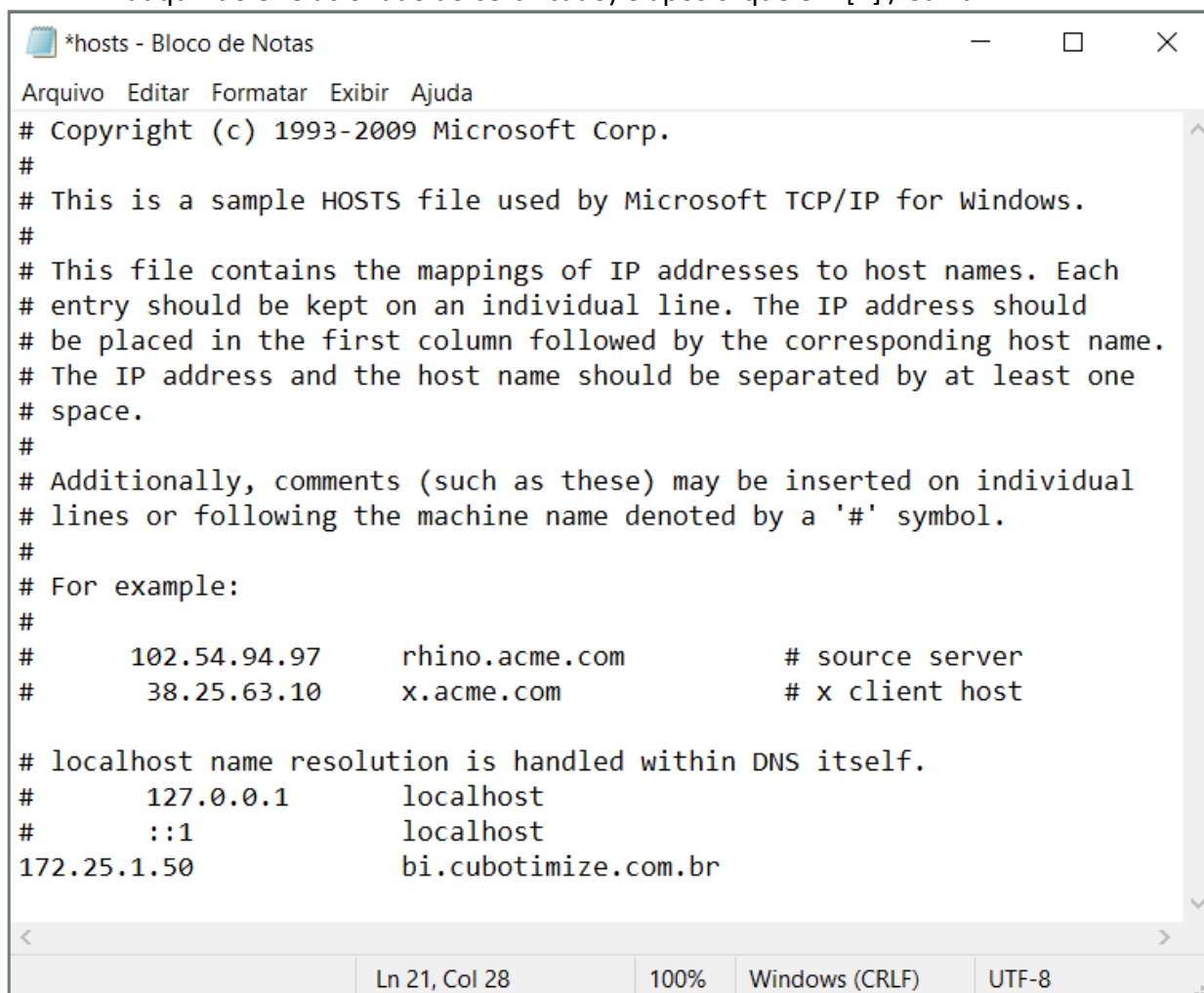
#### 5.2.5.15. Clique **OK** para finalizar **Permissões para...**



---

## 5.2.6. Direcionar busca do domínio externo do certificado em rede local para acessar o IP interno do Qlik Sense Enterprise (Recomendado utilizar o Server DNS, vide com a TI)

- 5.2.6.1. Alternativa com arquivo **Host** para testes: Em **Iniciar** (bandeira do Windows), digite e abra **notepad %SystemRoot%\system32\drivers\etc\hosts** (Ou via **Iniciar+R**), adicione uma linha ao final do arquivo para inserir o IP e ao lado o nome de domínio FQDN (domínio adquirido e relacionado ao certificado) e após clique em **[X] / Salvar**



```
*hosts - Bloco de Notas
Arquivo Editar Formatar Exibir Ajuda
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10      x.acme.com          # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
172.25.1.50             bi.cubotimize.com.br
```

Obs.: Realize esta operação nos computadores da rede local que deve acessar o Qlik Sense Enterprise, recomendado utilizar Group Policy do Active Directory para propagar a alteração em massa com mais facilidade. Como boa prática, é recomendado realizar a configuração no servidor DNS da infraestrutura para realizar a mesma tarefa e com mais segurança, evitando assim, alterar o arquivo Hosts.

---

## 5.2.7. Adicionar registro no sistema local para evitar loopback de autenticação local no endereço de domínio externo

- 5.2.7.1. No servidor com o serviço Qlik Sense Enterprise, vamos imputar um novo registro  
Obs.: Poderá inserir rapidamente o registro através do **PowerShell**, neste caso, poderá pular os passos da seção 5.2.7 após 5.2.7.1

Comando exemplo (altere o domínio): **Get-Item -path**

```
"HKLM:\System\CurrentControlSet\Control\Lsa\MSV1_0" | new-ItemProperty -Name  
"BackConnectionHostNames" -Value ("bi.cubotimize.com.br") -PropertyType  
"MultiString"
```

Em seguida, deverá reiniciar o servidor. Comando: **Restart-Computer**

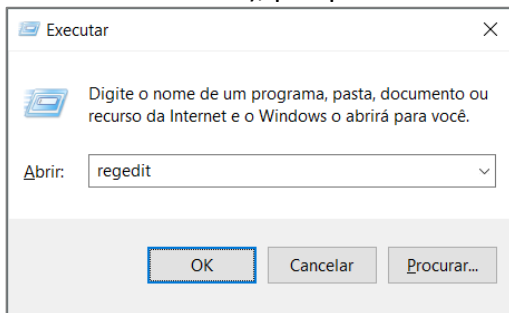
```

Administrator: Windows PowerShell
PS C:\Users\administrator.CORP> Get-Item -path "HKLM:\System\CurrentControlSet\Control\Lsa\MSV1_0" | new-ItemProperty -Name "BackConnectionHostNames" -Value ("", "") -PropertyType "MultiString"

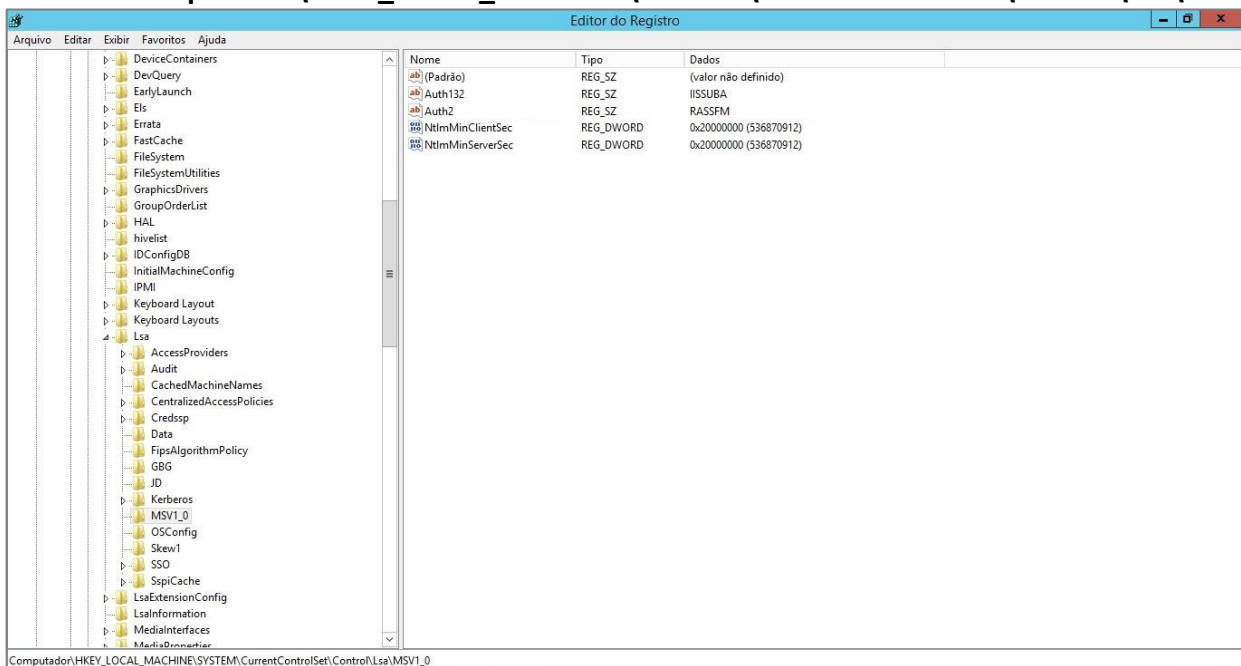
BackConnectionHostNames : {
PSPath                    : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0
PSParentPath              : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\MSV1_0
PSChildName               : MSV1_0
PSProvider                : Microsoft.PowerShell.Core\Registry
PS C:\Users\administrator.CORP>

```

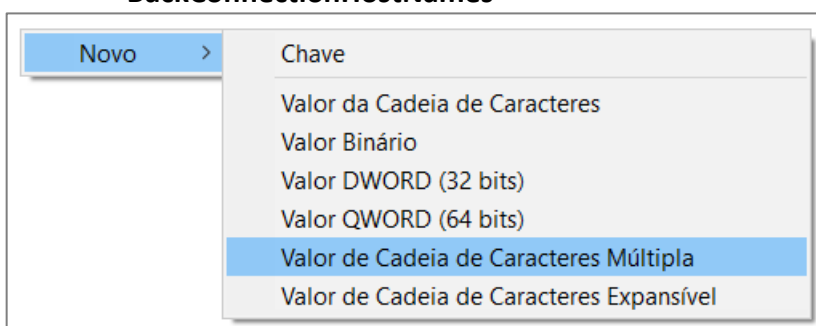
5.2.7.2. Alternativa a adição do registro **BackConnectionHostNames**: Em **Iniciar** (bandeira do Windows), pesquise e abra **regedit** (Ou via **Iniciar+R**)



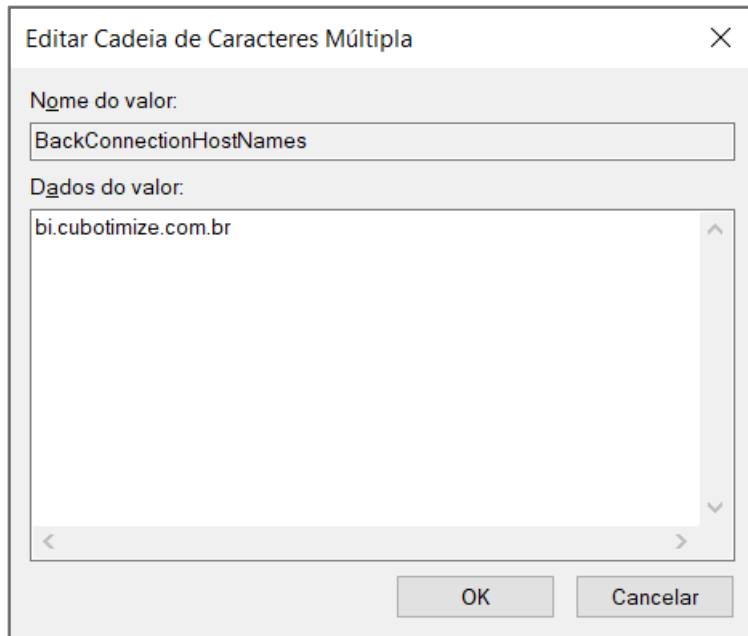
5.2.7.3. Em **Editor do Registro**, navegue até **Computador\HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1\_0**



5.2.7.4. Clique com o botão direito na área branca a esquerda, clique em **Novo / Valor de Cadeia de Caracteres Múltiplos**, altere o nome do registro para exatamente **BackConnectionHostNames**



5.2.7.5. Clique duplo sobre o novo registro para abrir a janela **Editar Cadeia de Caracteres Múltipla**, adicione em **Dados do valor** o nome do domínio FQDN externo e clique em **OK**. Ex.: bi.cubotimize.com.br

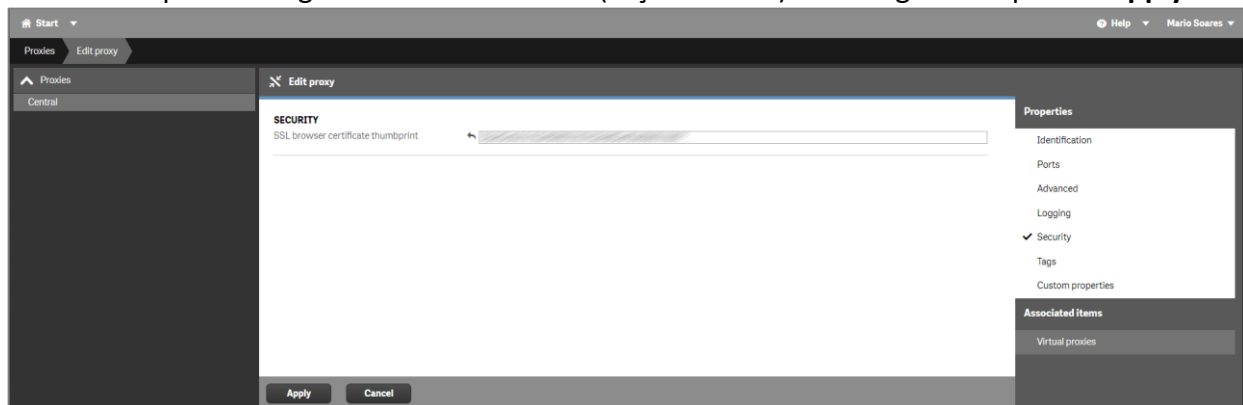


5.2.7.6. Reinicie o servidor para aplicar a alteração do registro

### 5.3. Qlik Sense Enterprise

5.3.1. Configurar “Proxy” (SSL browser certificate thumbprint) | Caminho: **QMC / Proxies / {Central}**

5.3.1.1. Em **Properties / Security**, na área **SSL browser certificate thumbprint**, adicione valor Impressão Digital do certificado SSL (seção 5.2.5.9) e em seguida clique em **Apply**

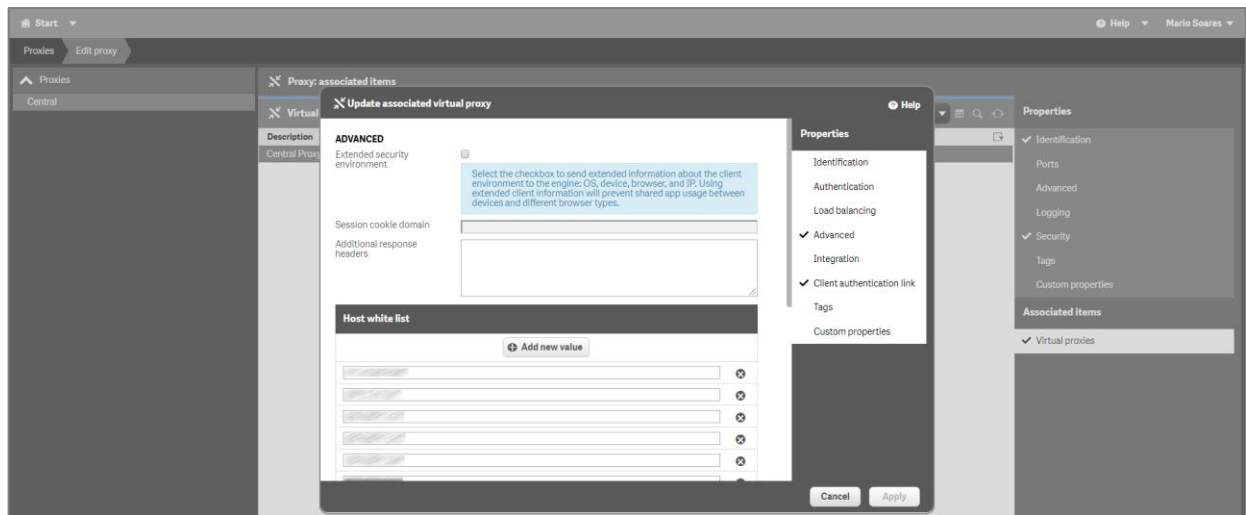


Obs.: Aparecerá uma janela informando que será necessário reiniciar o serviço Proxy para aplicar a alteração

5.3.2. Configurar “Virtual proxy” (Host White list e Client Authentication Link) | Caminho: **QMC / Virtual proxies / {Central Proxy (Default)}**

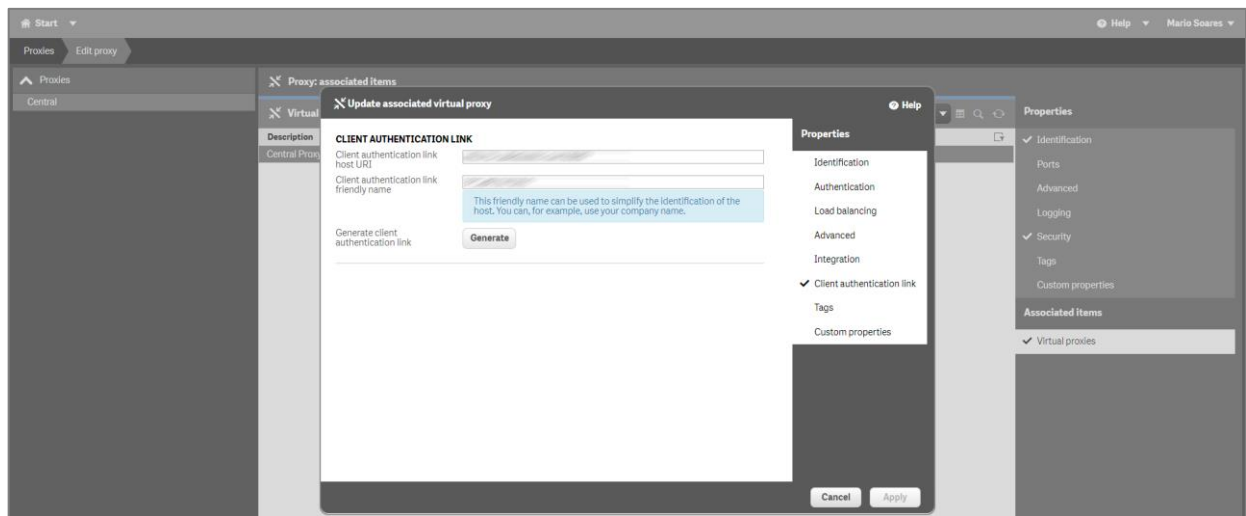
5.3.2.1. Em **Properties / Advanced**, na área **Host White list**, adicionar o link URI de acesso externo. Ex.: https://bi.cubotimize.com.br

Obs.: Poderá adicionar porta externa se houver. Utilizando https, fica implícito a porta 443



### 5.3.2.2. Em **Properties / Client Authentication Link**, na aba **CLIENT AUTHENTICATION LINK**, em **Client authentication link host URI**:

- **Client authentication link host URI**: Insira o link URI de acesso externo, com o mesmo domínio FQDN externo utilizado na geração do certificado SSL. Ex.: <https://bi.cubotimize.com.br>
- **Client authentication link friendly name**: Insira um nome amigável da conexão da empresa (apelido). Ex.: Nome Empresa - BI
- Clique em **Generate**
- Clique em **Apply**



## 5.4. Qlik Sense Mobile

### 5.4.1. Baixar e instalar aplicativo Qlik Sense no smartphone

#### 5.4.1.1. Para Android:

<https://play.google.com/store/apps/details?id=com.qlik.qliksense.mobile&hl=pt-BR>

#### 5.4.1.2. Para IOS:

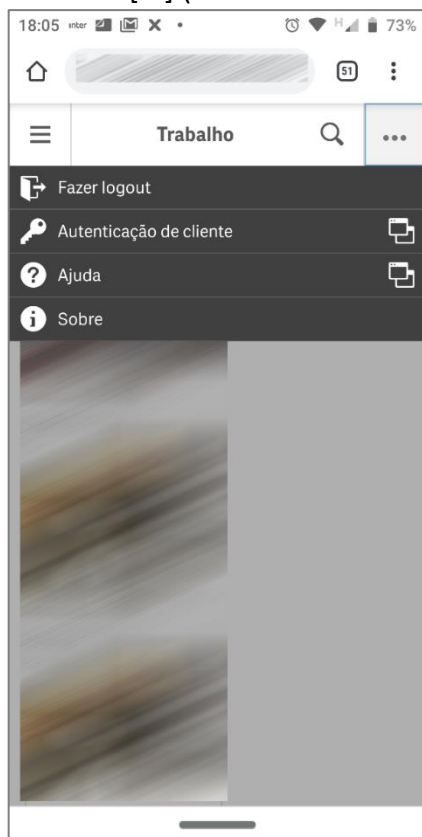
<https://apps.apple.com/br/app/qlik-sense-mobile/id1217049362>

---

#### 5.4.2. Acessar o endereço URI do Qlik Sense Enterprise pelo Browser do mobile (Autenticação do cliente)

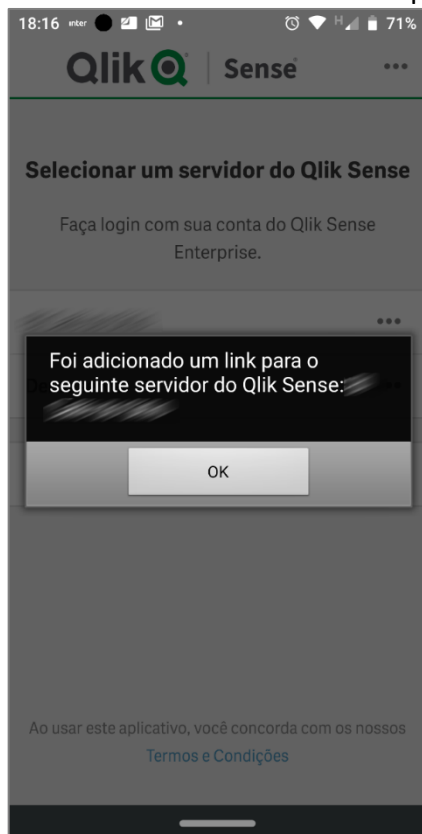
---

5.4.2.1. Utilizando internet externa. Abra o navegador (Google Chrome, exemplo), insira o endereço URI de acesso externo ao Qlik Sense Enterprise, realize o login, na tela do **HUB**, clique em [...] (menu no canto superior direito da página) e clique em **Autenticação do cliente**

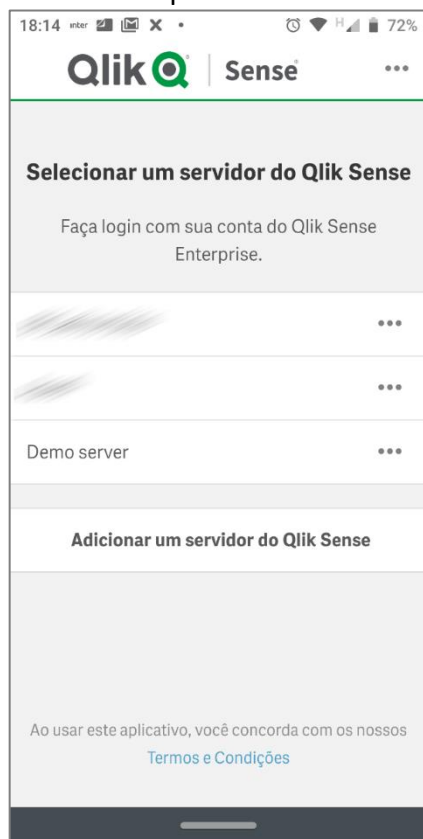


---

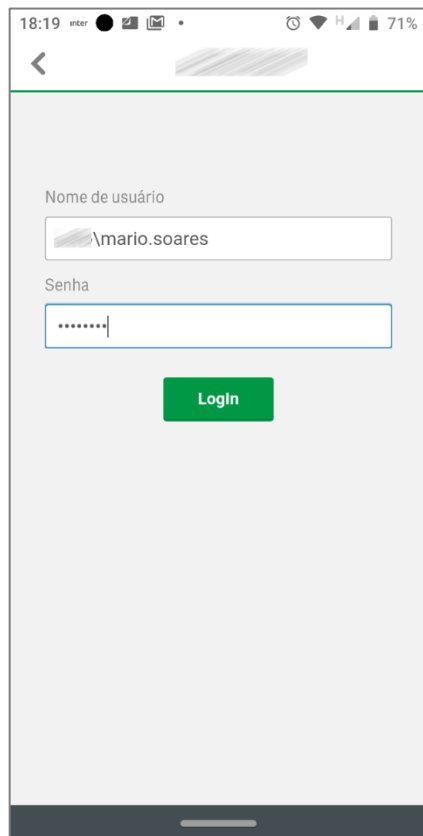
5.4.2.2. Será direcionado ao aplicativo **Qlik Sense** instalado no mobile, clique em **OK**



5.4.2.3. No aplicativo **Qlik Sense**, aparecerá o nome amigável da conexão da empresa, clique sobre o apelido



5.4.2.4. Insira **Nome de usuário**, **Senha** e clique em **Login**



#### 5.4.2.5. Acesso realizado com sucesso



## 6. Fontes

<https://www.rootusers.com/how-to-install-iis-in-windows-server-2016/>

[https://www.comodobr.com/suporte/csr\\_iis7.php](https://www.comodobr.com/suporte/csr_iis7.php)

<https://www.certisign.com.br/duvidas-suporte/certificado-servidor/instalacao-configuracao/iis7.0>

<https://br.godaddy.com/help/instalacao-manual-de-um-certificado-ssl-no-servidor-iis-7-4801>

<https://blog.blksth1.com/2013/05/07/a-quick-guide-to-configuring-the-loopback-check/>

<https://help.qlik.com/en->

[US/sense/June2019/Subsystems/PlanningQlikSenseDeployments/Content/Sense\\_Deployment/Qlik-Sense-mobile-app-security.htm](https://help.qlik.com/en-US/sense/June2019/Subsystems/PlanningQlikSenseDeployments/Content/Sense_Deployment/Qlik-Sense-mobile-app-security.htm)

<https://help.qlik.com/en->

[US/sense/June2019/Subsystems/ManagementConsole/Content/Sense\\_QMC/change-to-signed-server-proxy-certificate.htm](https://help.qlik.com/en-US/sense/June2019/Subsystems/ManagementConsole/Content/Sense_QMC/change-to-signed-server-proxy-certificate.htm)

<https://help.qlik.com/en->

[US/sense/June2019/Subsystems/ManagementConsole/Content/Sense\\_QMC/configure-client-authentication.htm](https://help.qlik.com/en-US/sense/June2019/Subsystems/ManagementConsole/Content/Sense_QMC/configure-client-authentication.htm)

<https://help.qlik.com/en->

[US/sense/June2019/Subsystems/PlanningQlikSenseDeployments/Content/Sense\\_Deployment/Deploying-Qlik-Sense-mobile.htm](https://help.qlik.com/en-US/sense/June2019/Subsystems/PlanningQlikSenseDeployments/Content/Sense_Deployment/Deploying-Qlik-Sense-mobile.htm)



---

## 7. Links interessantes

SSL VA gratuito: <https://www.secnet.com.br/blog/certificado-ssl-gratuito-para-toda-internet>

Gerador on-line de CSR: <https://ssl4less.com.br/ssl-tools/csr-generator.html>