AI Brasil

an artificial intelligence community

AI Brasil

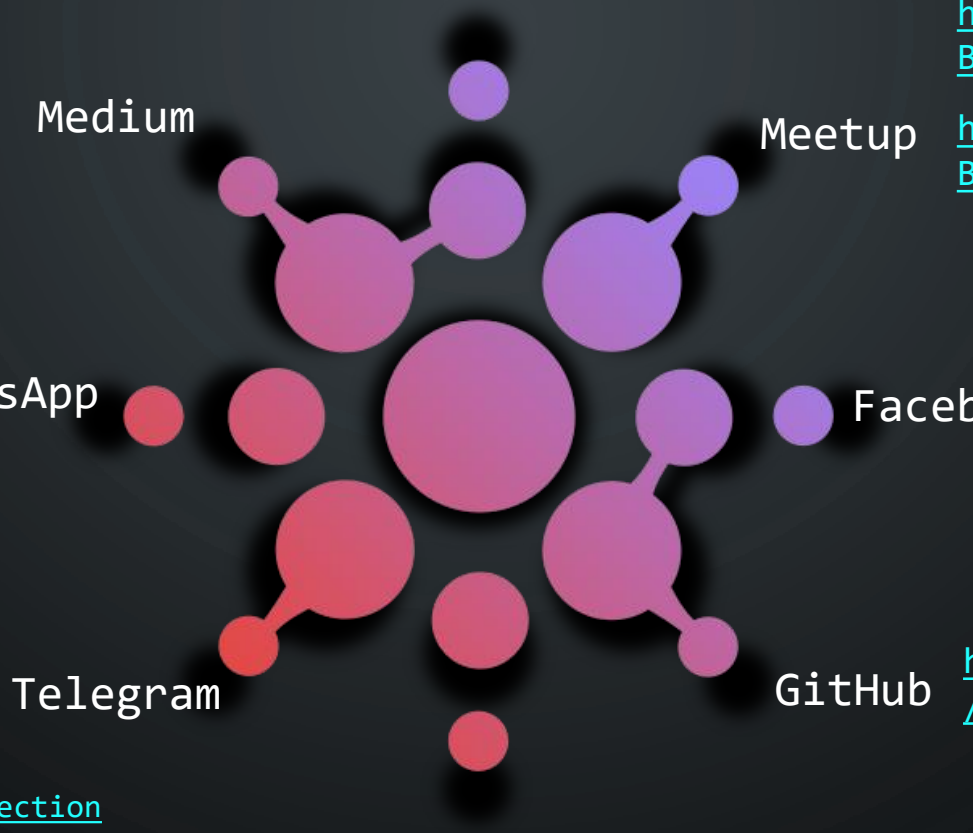
an artificial intelligence community

Criando inteligência artificial para segurança da informação

Mini Treinamento

Security Bsides SP 15
(19 e 20 de Maio de 2018)

CANAIS DE INTERAÇÃO COM AS COMUNIDADES AI BRASIL E SECURITY H1V3



https://medium.com/brasil-ai

https://www.meetup.com/pt-BR/ai-brasil/

https://www.meetup.com/pt-BR/security-hive

AI Brasil
https://chat.whatsapp.com/K04WGgFH1JKC83jBkMzEZG

Security H1V3
https://chat.whatsapp.com/JNtgpzI8bz0CyIk7c6hLkx

www.facebook.com/brasilAI

www.facebook.com/H1V3Sec

https://github.com/ai-brasil

Security H1V3
https://t.me/H1V3SecResurrection

AI Brasil
https://t.me/joinchat/GU8z_RKCm2AJebSB3ozXWg

Vamos começar !!!

ABOUT: “AGENTES VIRTUAIS”

Este guia irá ensinar como criar o seu próprio Agente Virtual, seja para atividades básicas como um chatbot à atividades mais complexas como ... aí é com a sua imaginação.

Agente Virtual em 3 etapas:

1- Criação de conta e preparação dos serviços
    1.1 – Criação de conta no Bluemix
    1.2 – Criação do serviço Watson Conversation (WC)
    1.3 – Criação do app Node-Red Starter
2- Treinamento do Watson Conversation (WC)
    2.1 – Importação do Workspace de exemplo
    2.2 – Teste do Workspace no WC
    2.3 – Criação de diálogo personalizado
3- Configuração do Node-Red Starter com WC
    3.1 – Integração entre Node-Red Starter e WC
    3.2 – Importação e configuração do flow de exemplo
    3.3 – Conclusão da atividade

FAZER DOWNLOAD DOS ARQUIVOS

Este mini treinamento utiliza os arquivos publicados no endereço:

https://github.com/pedrohsbezerra/BSidesSP15_2018

Atividades 1-2-3 https://github.com/pedrohsbezerra/BSidesSP15_2018

O arquivo “Workspace-Agente_Virtual.json” é a AI de segurança, será importada para o Watson Assistant durante o mini treinamento. Esta AI esta treinada para entender o comportamento do usuário quando ele deseja abrir um incidente de segurança.

O arquivo “flow-Node-Red.txt” será importado no Node-Red durante o mini treinamento. Este possui toda a programação necessária para conectar uma interface visual com a AI de segurança.

Atividade 4

Baixar todo o projeto, aproximadamente 500mb, ou seja, demora.

BEGINNER

1- Criação de conta e preparação dos serviços

BEGINNER

1- Criação de conta e preparação dos serviços

1.1 – Criação de conta no IBM Cloud

I. Acessar o link: https://console.bluemix.net/

II. Clicar em “Criar uma conta grátis”

III. Preencher o formulário seguir as instruções de cadastro. Será necessário acessar seu e-mail para validar a conta criada.

IV. Fazer login no IBM Cloud com a conta criada.

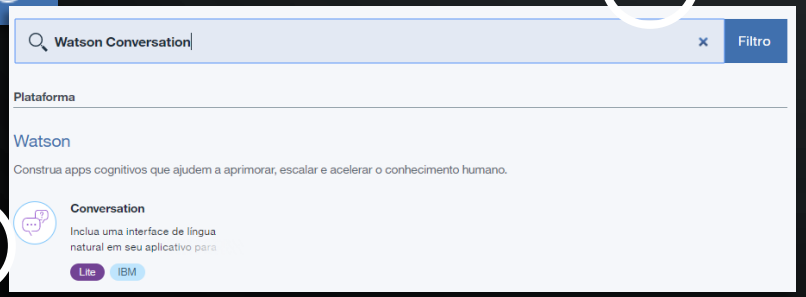
1.2 – Criação do serviço Watson Conversation

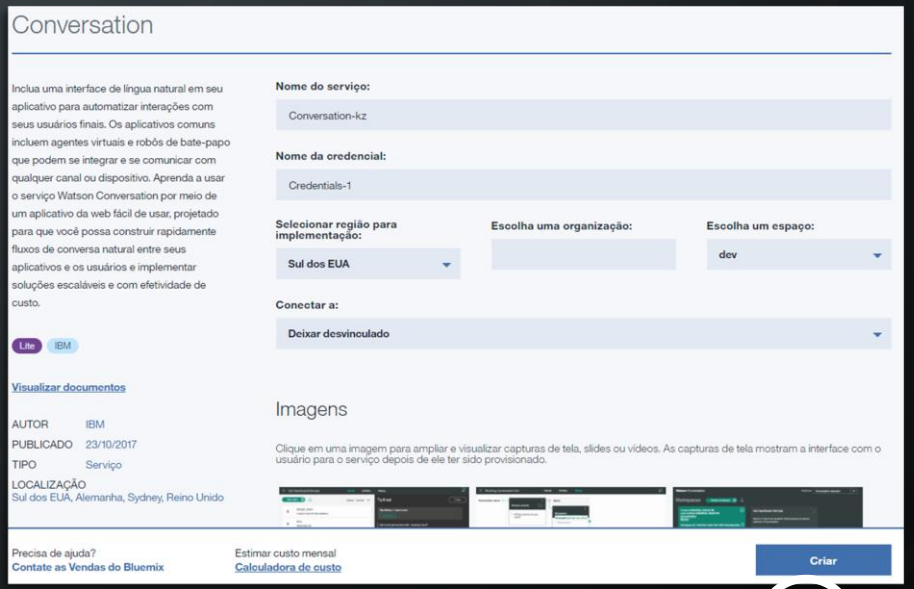
1- Clicar no botão “Criar”

2- No campo “Procura” digitar “Watson Conversation”

3- Clicar no item “Conversation”

4- Na tela seguinte clicar em “Criar”





BEGINNER

1- Criação de conta e preparação dos serviços

1.3 – Criação do app Node-Red Starter

1- Clicar em “Menu” depois em “Painel” para voltar para a tela principal

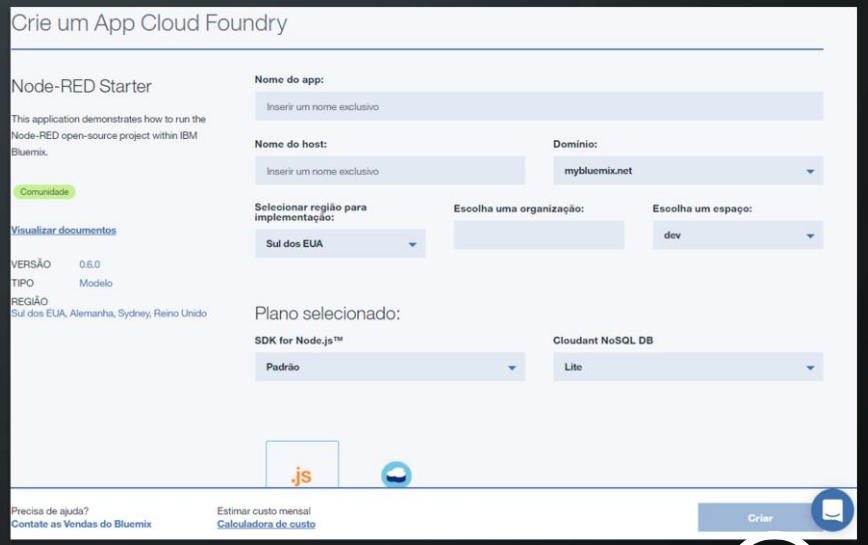
2- Clicar no botão “Criar”

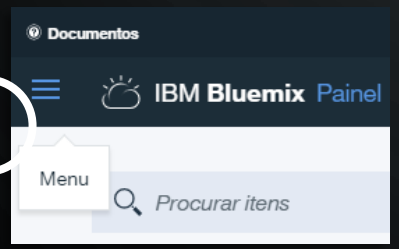
3- No campo “Procura” digitar “Node-Red Starter”

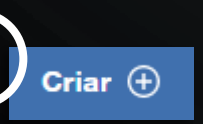
4- Clicar no item “Node-Red Starter”

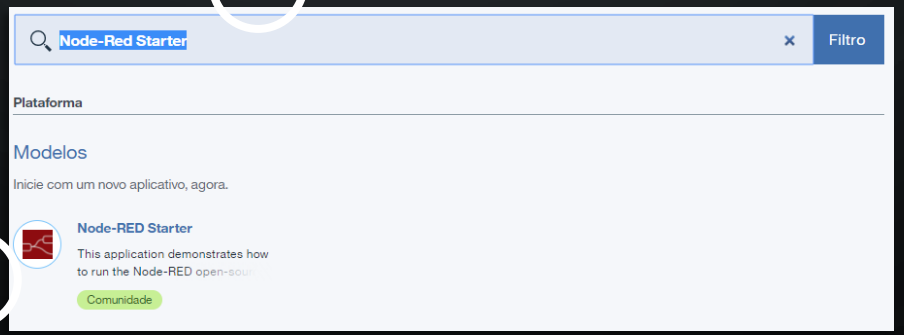
5- Na tela seguinte, nomeie o serviço e clicar em “Criar”

6- Na tela principal visualizar os “Apps Cloud Foundry” e abrir o app (url) criado para o “Node-Red Starter”









BEGINNER

1- Criação de conta e preparação dos serviços

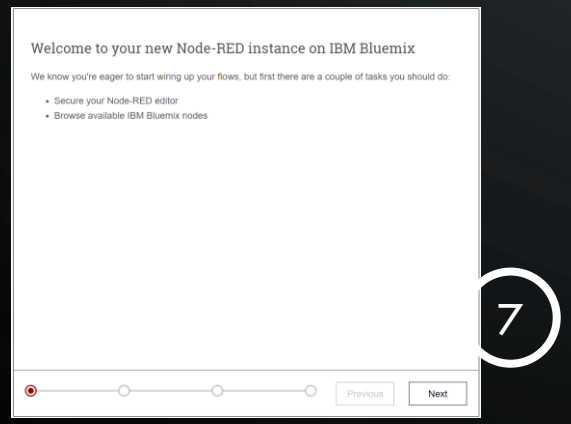
1.3 – Criação do app Node-Red Starter

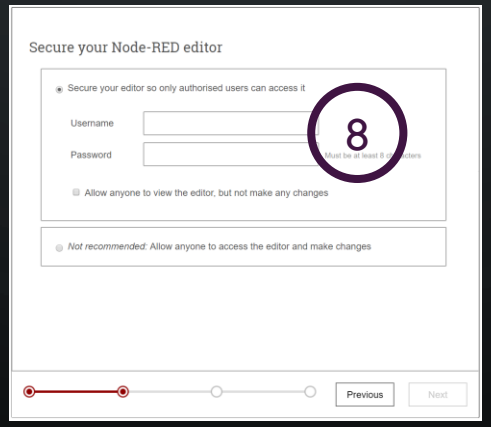
7- A tela principal do Node-Red Starter irá solicitar que sejam aplicadas as configurações iniciais. Clicar em **“Next”**

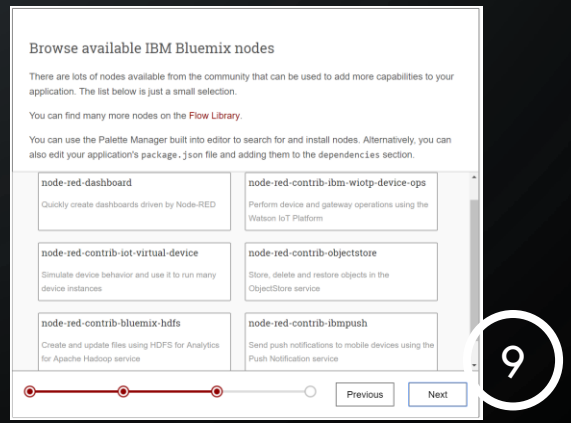
8- Preencher os campos “Username” e “Password” com o usuário e senha que será utilizado para administrar o Node-Red Starter. Lembre-se de usar uma senha longa e complexa para melhorar a segurança do seu Node-Red Starter. Depois clicar em **“Next”**

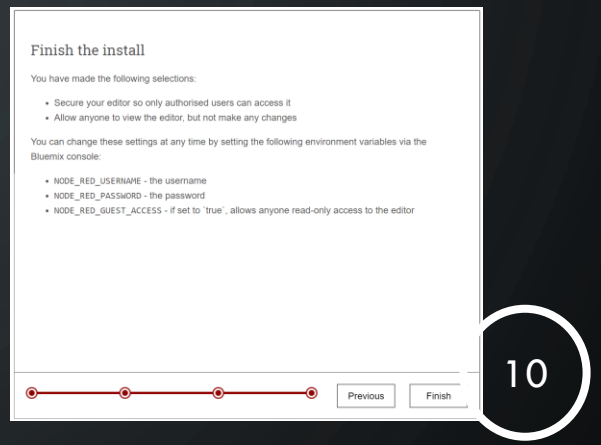
9- Clicar em **“Next”** na próxima tela

10- Clicar em **“Finish”** na próxima tela









INTERMEDIATE

2- Treinamento do Watson Conversation (WC)

INTERMEDIATE

2- Treinamento do Watson Conversation (WC)

2.1 – Importação do Workspace de exemplo

1- Clicar em “Menu” depois em “Painel” para voltar para a tela principal

2- Em “Serviços”, procurar o serviço “Conversation” e clicar sob o nome do serviço.

3- Na tela seguinte clicar no botão chamado “Launch Tool”.

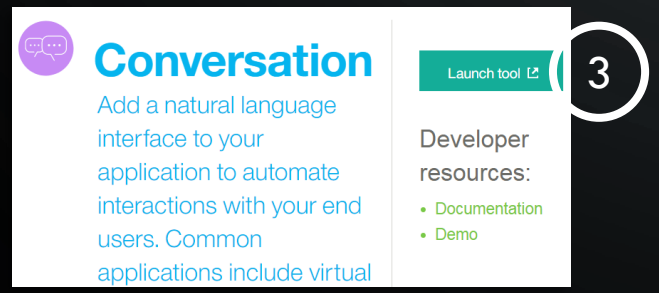
4- Na tela seguinte clicar no botão chamado “Log in with IBM ID”. Caso seja solicitada novas informações de usuário/senha utilizar os mesmos dados utilizados para logar na conta do IBM Cloud.

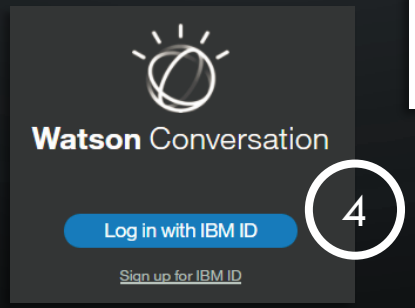
5- Na tela do WC clicar no botão “Import workspace”.

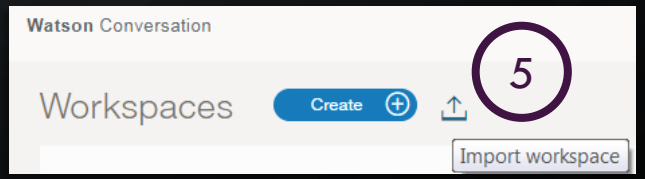
6- Clicar em “choose a file”, procurar e clicar no arquivo **“Workspace-Agente_Virtual.json”, arquivo presente no projeto do Github e demais documentos do mini treinamento.**

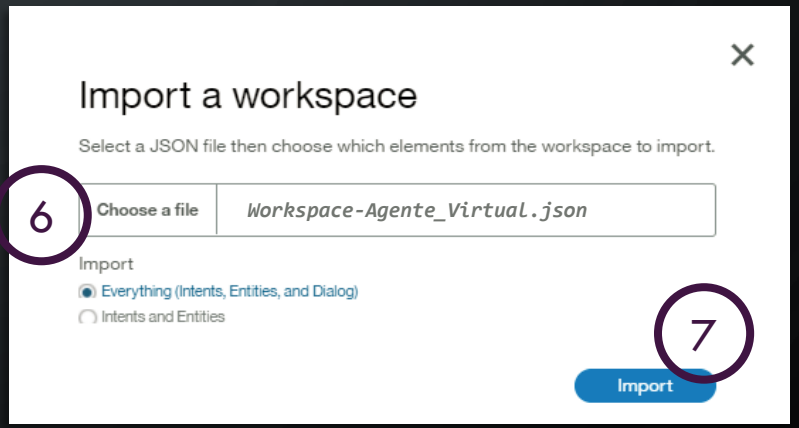
7- clicar no botão “Import”.

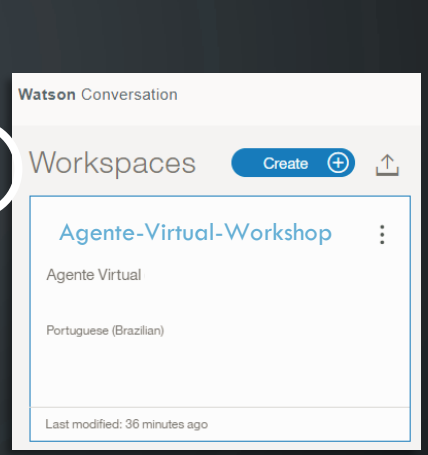
8- Verificar se foi criado o workspace **“Workspace-Agente_Virtual.json”.**











2- Treinamento do Watson Conversation (WC)

2.2 – Teste do Workspace no WC

1- Clicar no workspace **“Agente-Virtual-Workshop”**.

2- Clicar em **“Intents”** e verificar se a tela apresenta conteúdo.

3- Clicar em **“Entities”** e verificar se a tela apresenta conteúdo.

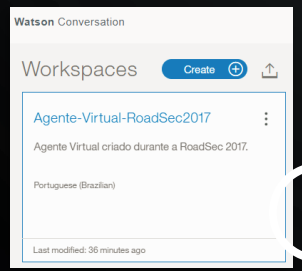
4- Clicar em **“Dialog”** e verificar se a tela apresenta conteúdo.

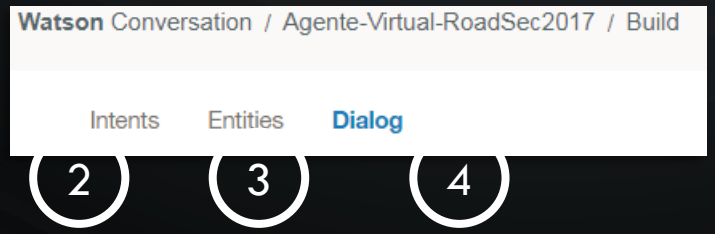
5- Clicar em **“Ask Watson”** e aguardar a abertura da tela de chat.

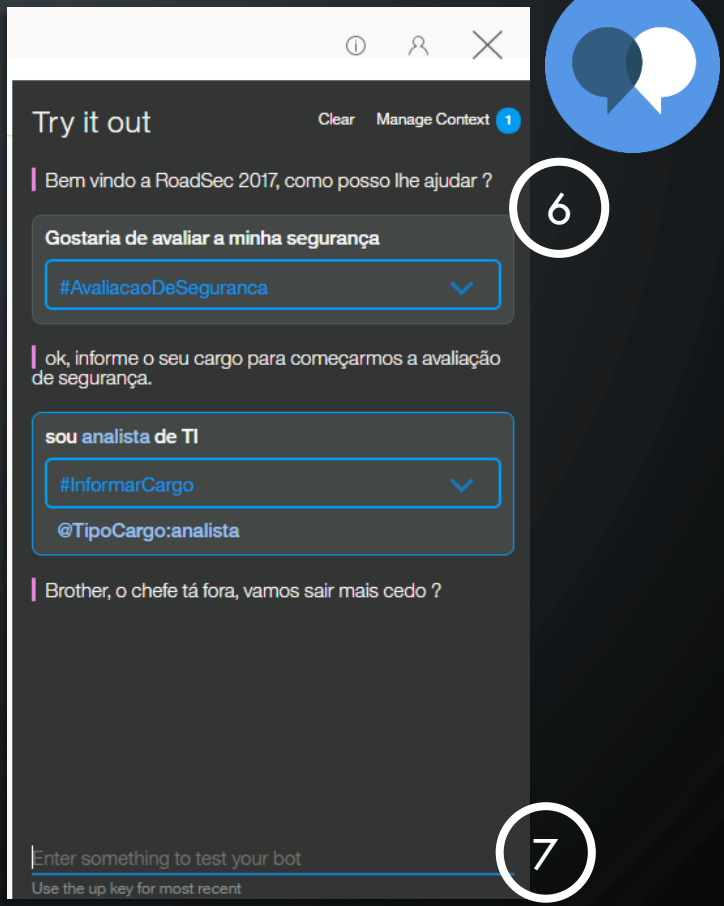
6- Verificar se a frase **“Bem vindo ao Workshop, como posso lhe ajudar ?”** é exibida.

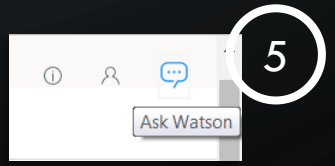
7- No canto inferior direito da tela interagir com o chatbot digitando **“Gostaria de avaliar a minha segurança”** e pressionar **“Enter”** no seu teclado. A resposta deve ser **“ok, informe o seu cargo para começarmos a avaliação de segurança.”**.

8- Interagir com o chatbot digitando **“sou analista de TI”** e pressionar “Enter” no seu teclado. A resposta deve ser **“Brother, o chefe tá fora, vamos sair mais cedo ?”**.









2- Treinamento do Watson Conversation (WC)

2.3 – Criação de diálogo personalizado

1- Clicar em **“Dialog”** e verificar se a tela apresenta conteúdo.

2- Clicar no botão com 3 círculos, na caixa de Bem-vindo, e depois em **“Add node below”.**

3- Colocar o nome “Conta Piada” e informar qual a “Intents” ou “Entities” será usada para executar o nó, ou “Node”, que será criado. Digite “#piadas”.

4- Informar a resposta que será exibida para o usuário do Agente Virtual, digite **“Piada 1”** ou uma piada que realmente seja engraçada. Pressione “Enter” para registrar as configurações.

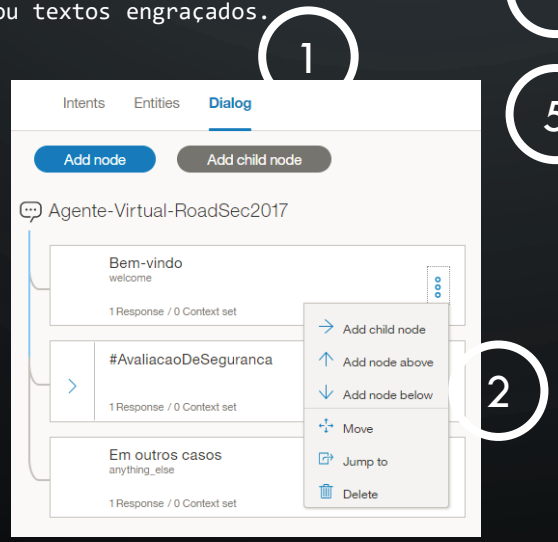
5- Na linha de baixo digite outra piada, também engraçada. Pressione “Enter” para registrar as configurações.

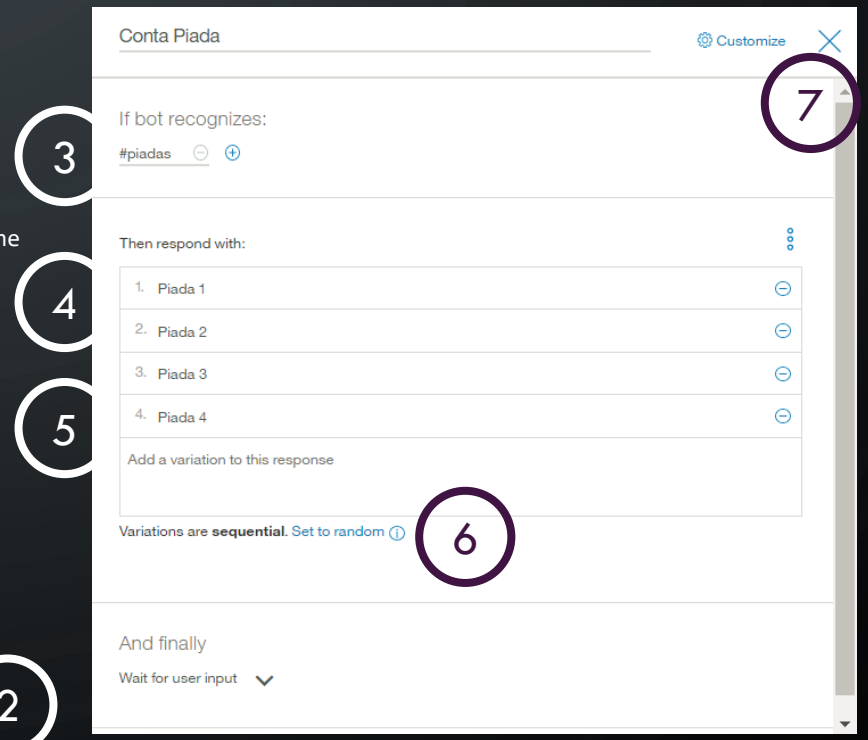
Registre no mínimo 4 piadas, ou textos engraçados.

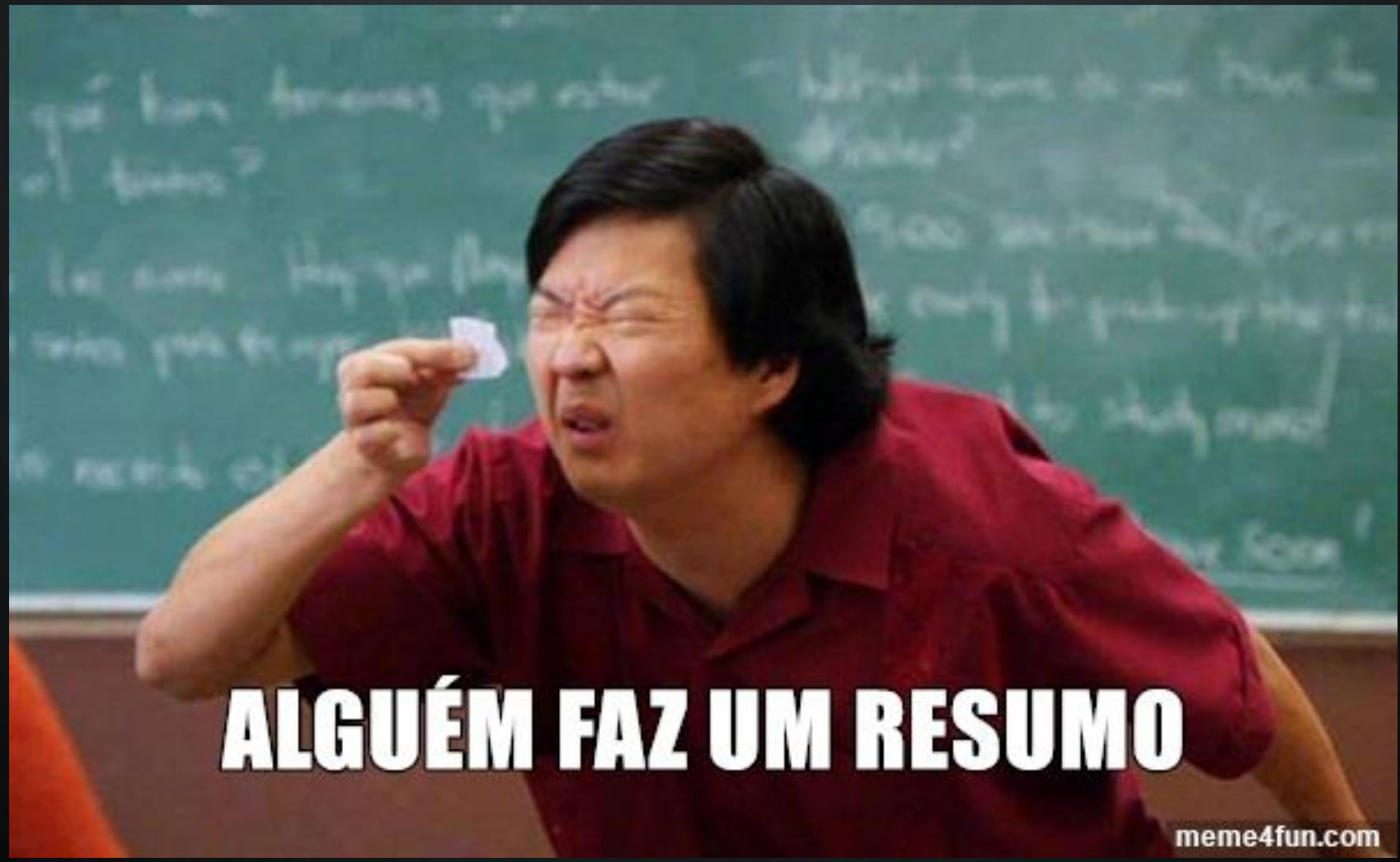
6- Clicar em **“Set to random”** para que as respostas sejam randômicas e mais naturais.

7- Clicar no X para fechar e aplicar as mudanças.

Parabéns, você treinou sua AI!



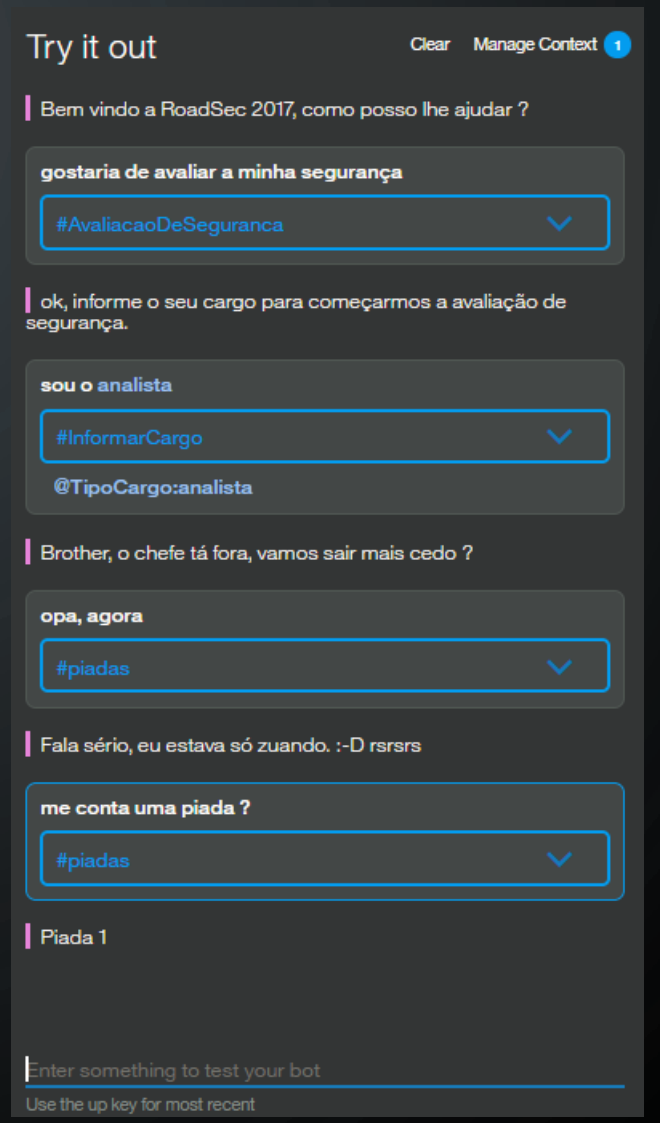



ALGUÉM FAZ UM RESUMO
meme4fun.com

RESUMÃO

Se você fez tudo certo, neste momento você já fez todas as atividades necessárias para criar a sua própria inteligência artificial. Veja o que você já fez, e meus parabéns por chegar até aqui. :-D

1- Criação de conta e preparação dos serviços
    1.1 – Criação de conta no Bluemix
    1.2 – Criação do serviço Watson Conversation (WC)
    1.3 – Criação do app Node-Red Starter
2- Treinamento do Watson Conversation (WC)
    2.1 – Importação do Workspace de exemplo
    2.2 – Teste do Workspace no WC
    2.3 – Criação de diálogo personalizado



ADVANCED

3- Configuração do Node-Red Starter com WC

ADVANCED

3- Configuração do Node-Red Starter com WC

3.1 – Integração entre Node-Red Starter e WC

1- Clicar em **“Menu” depois em “Painel”** para voltar para a tela principal.

2- Na tela principal visualizar os “Apps Cloud Foundry” e clicar no nome do app “Node-Red Starter” criado anteriormente.

3- Na tela seguinte, lado esquerdo superior, clicar em **“Conexões”.**

4- Na tela seguinte, lado direito superior, clicar em **“Conectar existente”.**

5- Na tela seguinte clicar no serviço de **“Conversation”** criado anteriormente e depois em **“Conectar”, canto inferior esquerdo.**

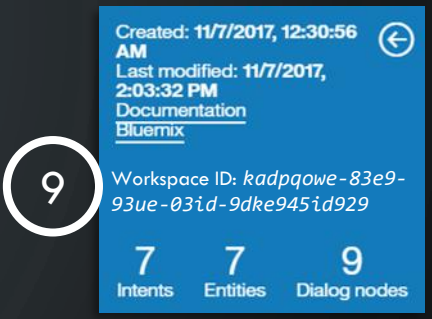
6- Na tela seguinte clicar em **“Estagiar novamente”.**

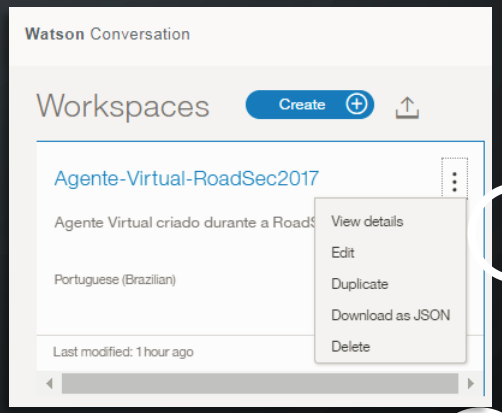
7- Aguardar 5 minutos para que o Node-Red seja reiniciado.

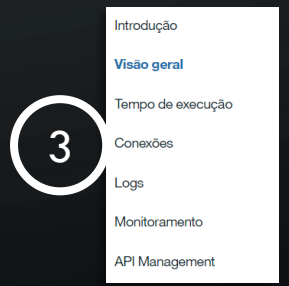
8- Acessar a tela principal do WC, clicar no botão com 3 círculos, do workspace **“Agente-Virtual-Workshop”,** e depois em clicar em **“View details”.**

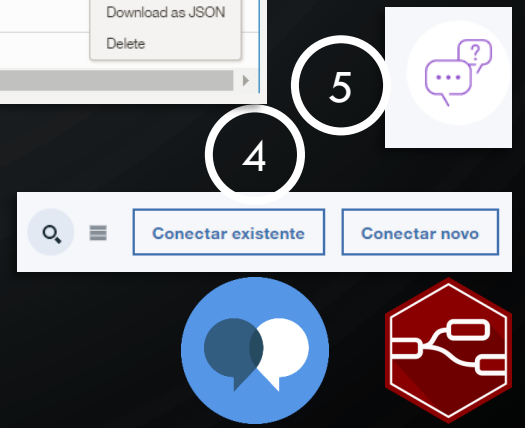
9- Selecionar e copiar o texto apresentado na frente da frase **“Workspace ID”,** um texto parecido com: *kadpqowe-83e9-93ue-03id-9dke945id929*

10- Guardar o Workspace ID para utilização futura no Node-Red.









ADVANCED

3- Configuração do Node-Red Starter com WC

3.2 – Importação e configuração do flow de exemplo

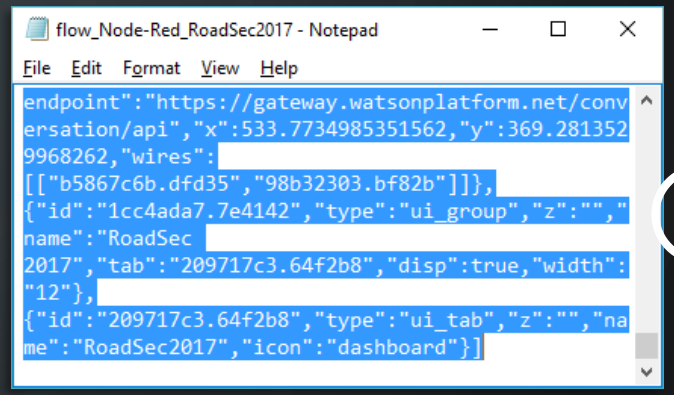
1- Clicar em **"Menu"** para voltar para a tela principal.

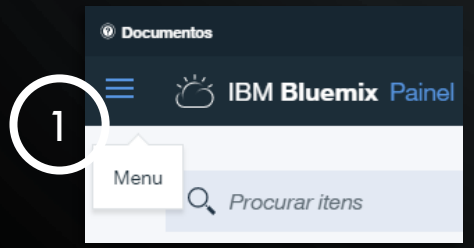
2- Na tela principal visualizar os "Apps Cloud Foundry" e clicar no endereço do app "Node-Red Starter" criado anteriormente (ex.: meuappNodeRed.mybluemix.net).

3- Na tela principal do app (ex.: meuappNodeRed.mybluemix.net) clicar em **"Go to your Node-RED flow editor"**

4- Inserir o usuário e senha definido anteriormente e clicar em **"Login"**. Será aberta a tela principal do "Node-Red Starter".

5- No seu computador, localizar o arquivo **"flow_Node-Red"**. Abrir este arquivo e copiar todo o conteúdo dele para a memória RAM, ou seja, dar um "Copiar" ou "Ctrl+C".





ADVANCED

3- Configuração do Node-Red Starter com WC

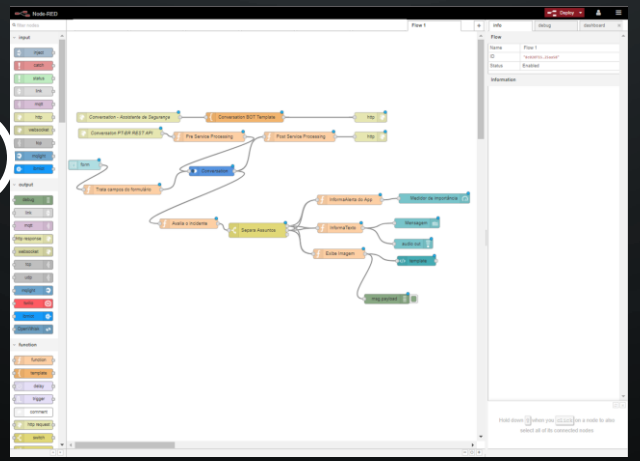
3.2 – Importação e configuração do flow de exemplo

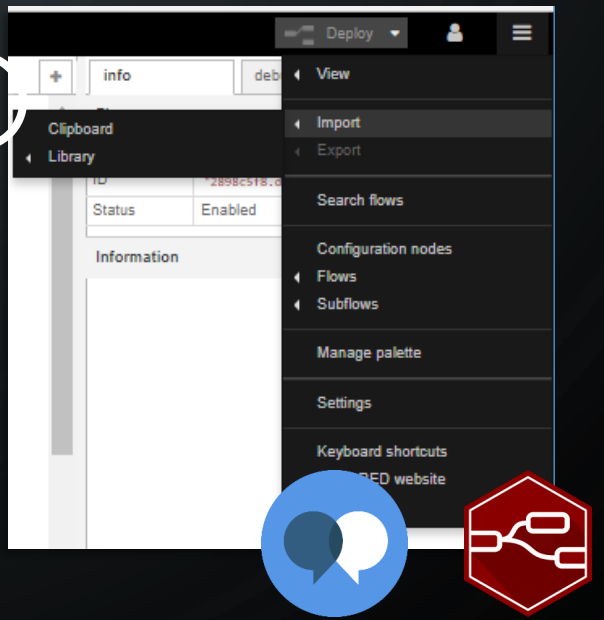
6- Voltar para a tela principal do “Node-Red Starter” e clicar no sinal de **“+”** posicionado no lado direito superior. Será criado um “flow” vazio para que possamos trabalhar.

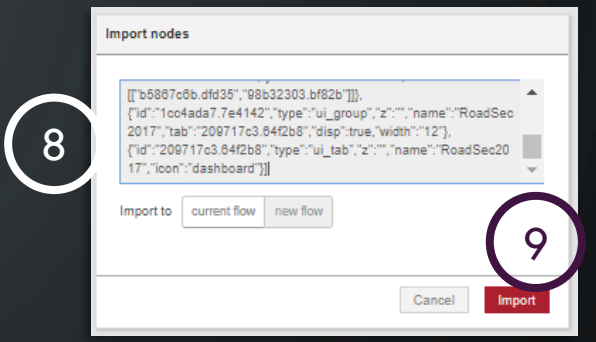
7- Clicar nas **“3 linhas” do canto superior direito** da tela, depois ir em **“Import”**, depois clicar em **“Clipboard”**.

8- Na tela de “Import nodes” deverá ser colado o conteúdo do arquivo **“flow_Node-Red”**, ou seja, clicar no texto **“Paste nodes here”** e **“Ctrl+V”**, também chamado de “Colar”.

9- Clicar em **“Import”** e depois no meio da tela em branco. Assim estará importado o nó de exemplo.







ADVANCED

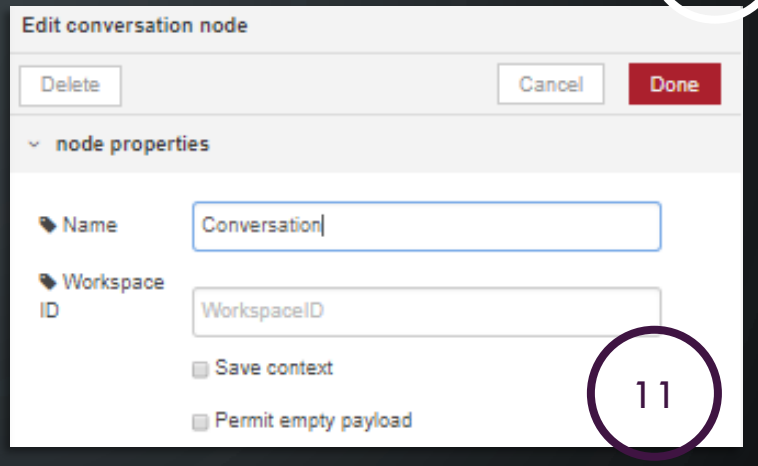
3- Configuração do Node-Red Starter com WC

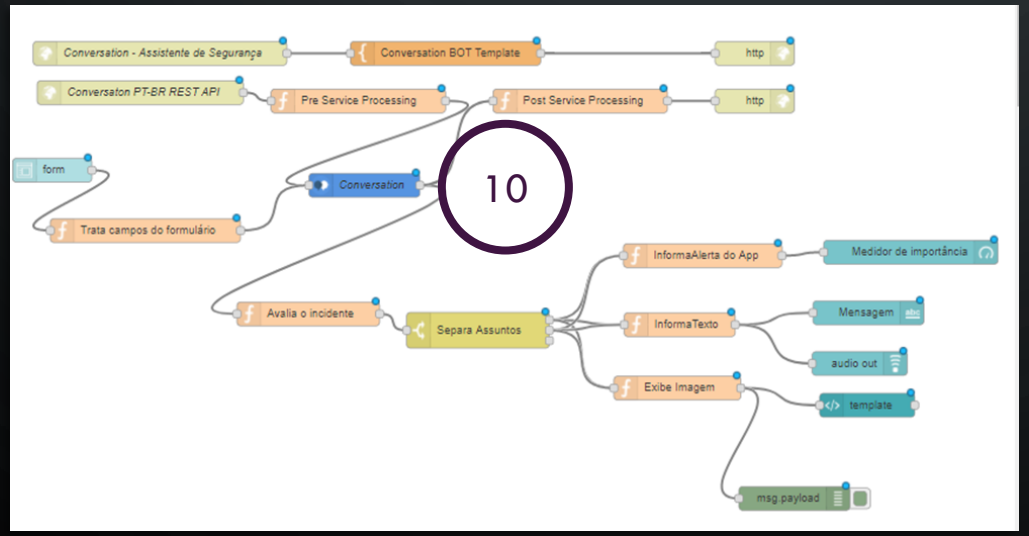
3.2 – Importação e configuração do flow de exemplo

10- Visualize o nó chamado **“Conversation”** e clique duas vezes para que ele seja aberto.

11- Na tela que se abre, no campo “Workspace ID” insira o workspace ID copiada nas atividades anteriores (atividade 9 do passo 3.1).

12- Clique em **“Done”** a para efetivar a alteração.





ADVANCED

3- Configuração do Node-Red Starter com WC

3.2 – Importação e configuração do flow de exemplo

13-Clicar nas **“3 linhas” do canto superior direito** da tela, depois ir em **“Manage palette”.**

14- Na tela seguinte clicar na aba **“Install”**

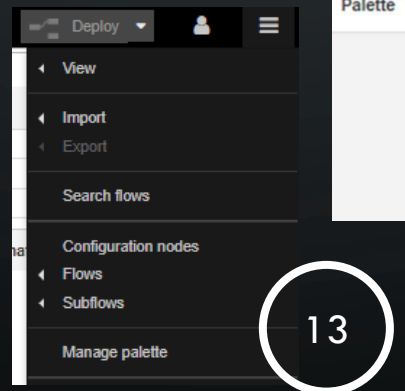
15- No campo **"search modules"** digitar **"node-red-dashboard“.**

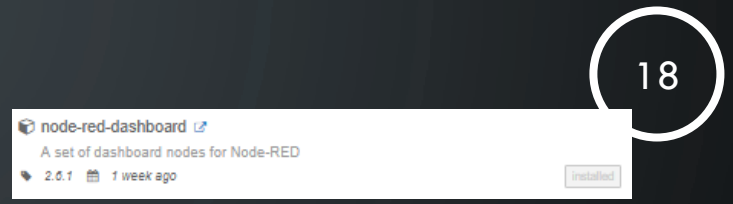
16- No módulo **“node-red-dashboard”** clicar em **“install”.**

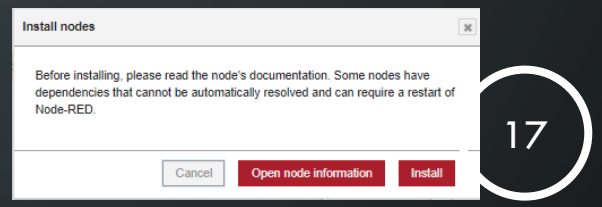
17- Na tela seguinte clicar no botão **"Install“.**

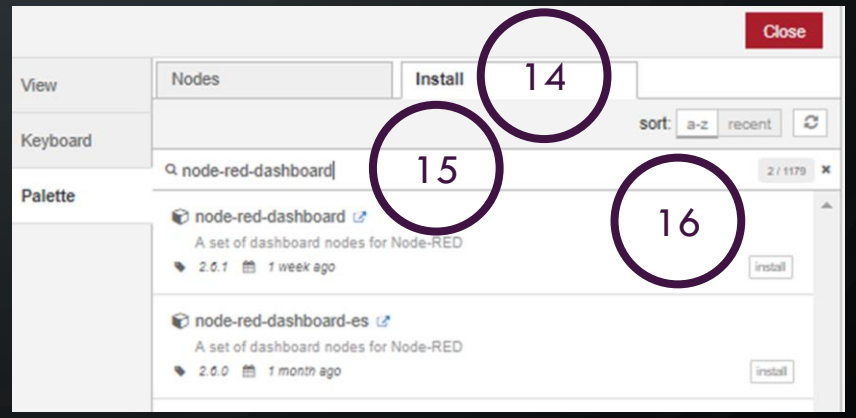
18- Aguardar a instalação do módulo, pode ser que o servidor seja reiniciado. O botão **“install”** será alterado para **"installed“** ao término da instalação.

19- Testar o seu Node-Red Starter acrescentando /ui no final do endereço para testar o dashboard (ex.: meuappNodeRed.mybluemix.net/ui). Terá aparecer apenas uma barra azul claro no top do navegador.









ADVANCED

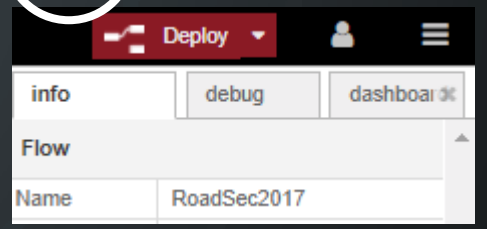
3- Configuração do Node-Red Starter com WC

3.2 – Importação e configuração do flow de exemplo

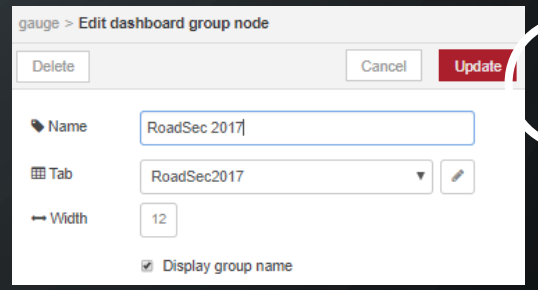
20- Clique 2 vezes no bloco **"Medidor de importância"**.
21- Na tela seguinte visualizar o **"Group"** e clicar no ícone do lápis para editar o grupo.
22- Na tela seguinte clique no botão vermelho **"Update"**.
23- Depois clique em **"Done"** para efetivar a atualização.

24- Clique 2 vezes no bloco **"Mensagem"**, depois no botão **"Done"**.
25- Clique 2 vezes no bloco **"audio out"**, depois no botão **"Done"**.
26- Clique 2 vezes no bloco **"template"**, depois no botão **"Done"**.
27- Clique 2 vezes no bloco **"form"**, lado esquerdo da tela, depois no botão **"Done"**.
28- Clicar em **"Deploy"** no canto superior direito da tela e aguardo a efetivação das mudanças.

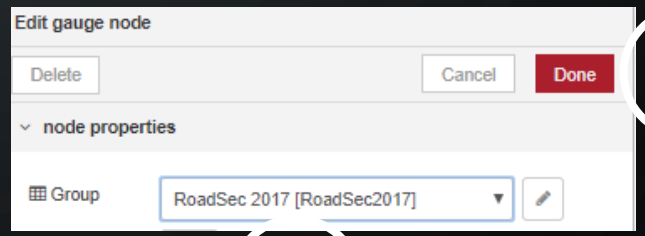
20



28

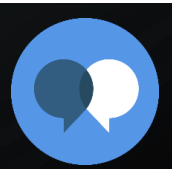


22



23

21



ADVANCED

3- Configuração do Node-Red Starter com WC

3.3 – Conclusão da atividade

1- Acessar o endereço internet do app acrescentando o **“/asiworkshop”** ao final do endereço (ex.: meuappNodeRed.mybluemix.net/asiworkshop).

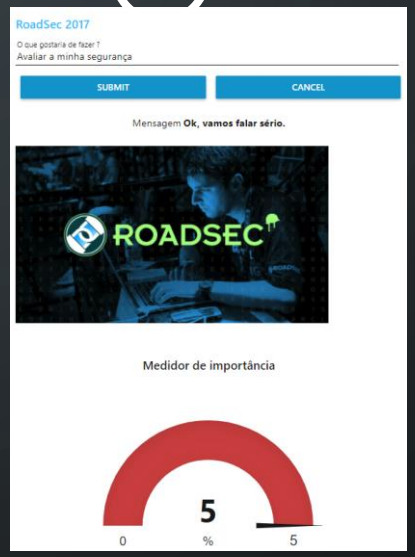
2- No campo de texto digite “Gostaria de uma piada”. Depois clicar no botão **“Enviar”**. A resposta deverá ser uma piada, ou frase engraçada, treinada por você no WC em atividades anteriores.

3- Acessar o endereço internet do app acrescentando o **“/ui”** ao final do endereço (ex.: meuappNodeRed.mybluemix.net/ui).

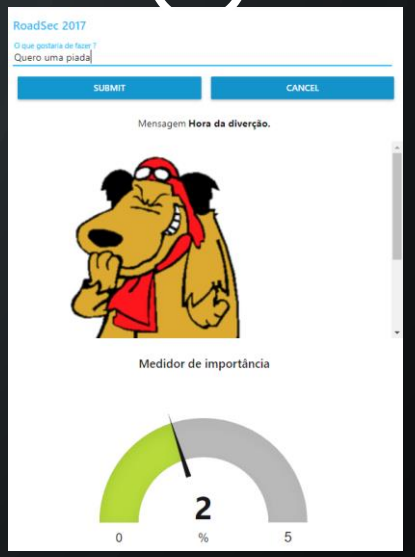
4- Clicar em **“O que gostaria de fazer ?”** e digitar a frase **“Avaliar a minha segurança”**, depois clicar no botão **“Submit”**. A mensagem será interpretada pelo WC e a resposta será a interação na tela.

5- Clicar em **“O que gostaria de fazer ?”** e digitar a frase **“Quero uma piada”**, depois clicar no botão **“Submit”**. A mensagem será interpretada pelo WC e a resposta será a interação na tela.

4

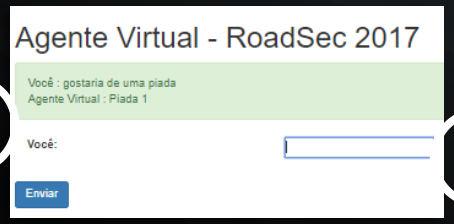


5



1

2



3


CÊ É UM CARA FODA BRO
meme4fun.com

PARABÉNS, AGORA VOCÊ TEM UM AGENTE VIRTUAL SÓ SEU !!!

Esta atividade acaba aqui ...mas seguem algumas dicas de coisas que você poderá fazer com seu agente virtual se trabalhar o seu código e/ou treinar o seu WC:

- Fazer ele contar piadas.
- Treinar mais interações no WC e fazer o seu Agente Virtual responder outros assuntos.
- Adicionar outros serviços no Node-Red e mandar o seu Agente Virtual acender a luz do seu quarto.

😯 😀

INSANE MODE

4-App Android alertando vazamento de dados

INSANE MODE

4-App Android alertando vazamento de dados

A quarta etapa do mini treinamento irá utilizar uma variação do projeto público do TensorFlow Lite para identificar um computador ou notebook através da câmera do dispositivo. Assim que identificado, especificamente o computador ou notebook, um alerta é enviado para um servidor Node-Red, assim possibilitando que o time de segurança possa atuar no possível vazamento de informações confidenciais ou sensíveis.

A atividade necessita de conhecimentos básicos de Android Studio e desenvolvimento de aplicativos Android.

https://github.com/tensorflow

https://nodered.org/

* Essa atividade pressupõe que você tenha o Android Studio instalado e atualizado, com SDK maior que 26, NDK maior que 14 e instalado as extensões do Gradle.

4-App Android alertando vazamento de dados

4.1 – Abrindo o projeto TensorFlow Lite no Android Studio

1- Acessar o endereço https://github.com/pedrohsbezerra/BSidesSP15_2018

2- Clicar no botão “Clone or download” e baixar o projeto. O arquivo tem aproximadamente 400 mb.

3- Descompactar o arquivo no seu computador

4- Abrir o Android Studio* e abrir o projeto baixado nos itens acima

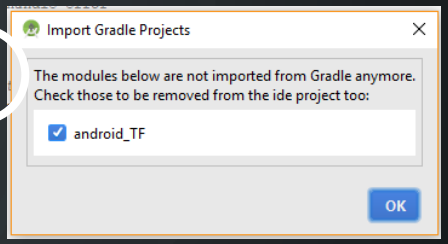
5- Clicar em “Ok”

6- Dentro do Android Studio, na visão de Project, abrir a pasta BSidesSP15_2018-Master, depois SRC, depois org.tensorflow.demo, depois tracking, depois o arquivo ClassifierActivity.java

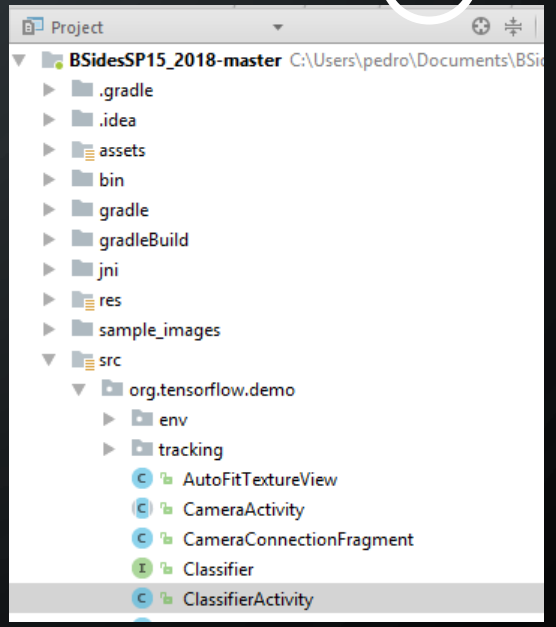
7- Ir para a linha 105

8- Alterar a URL para o endereço do seu servidor Node-Red, e variável que receberá os objetos identificados pela TensorFlow Lite.

5



6



7

```
104
105     String url ="http://seguranca.mybluemix.net/monitoramentoappandroidget?texto="+objetoidentificado2;
106
```

* Essa atividade pressupõe que você tenha o Android Studio instalado e atualizado, com SDK maior que 26, NDK maior que 14 e instalado as extensões do Gradle.

PARABÉNS VOCÊ CONCLUIU O MINI TREINAMENTO:

CRIANDO INTELIGÊNCIA ARTIFICIAL PARA SEGURANÇA DA INFORMAÇÃO