AOPF/AONOG 2022

Acesso remoto seguro durante pandemia COVID-19

Henri A. Godoy
Mariana Goes
8 e 9 Dezembro 2022

Visão noturna do Campus

UNICAMP - Universidade Estadual de Campinas - Estado de São Paulo. Fundada em 1966.

- Top 3 in Latin América.
- #1 em Patentes no Brasil.
- ~ 90 áreas (Faculdades, Escolas, Institutos e Hospitais).
- Atende ~ 5 milhões de pessoas.

Corpo acadêmico e administrativo

Docentes	1.782
Docentes doutores	99%
Funcionários	7.135

Patentes

Vigentes	1.088
Concedidas	67

Leitos	925
Internações	42.463
Cirurgias	68.239
Partos	4.842

Graduação

Cursos	65
Alunos matriculados	20.085

Pandemia Covid-19

- Março 2020, a Universidade decretou a suspensão das atividades presenciais.
- Necessidade de acessos aos computadores, laboratórios informática, equipamentos de pesquisas, sistemas internos, servidores físicos.
- Aumento descontrolado no uso de sistemas de acesso remoto (RDP, Real VNC, AnyDesk, TeamViewer, LogMeIn, etc...)
- Instalação de softwares nos computadores pessoais para acesso remoto e suporte técnico.

Requisitos necessários

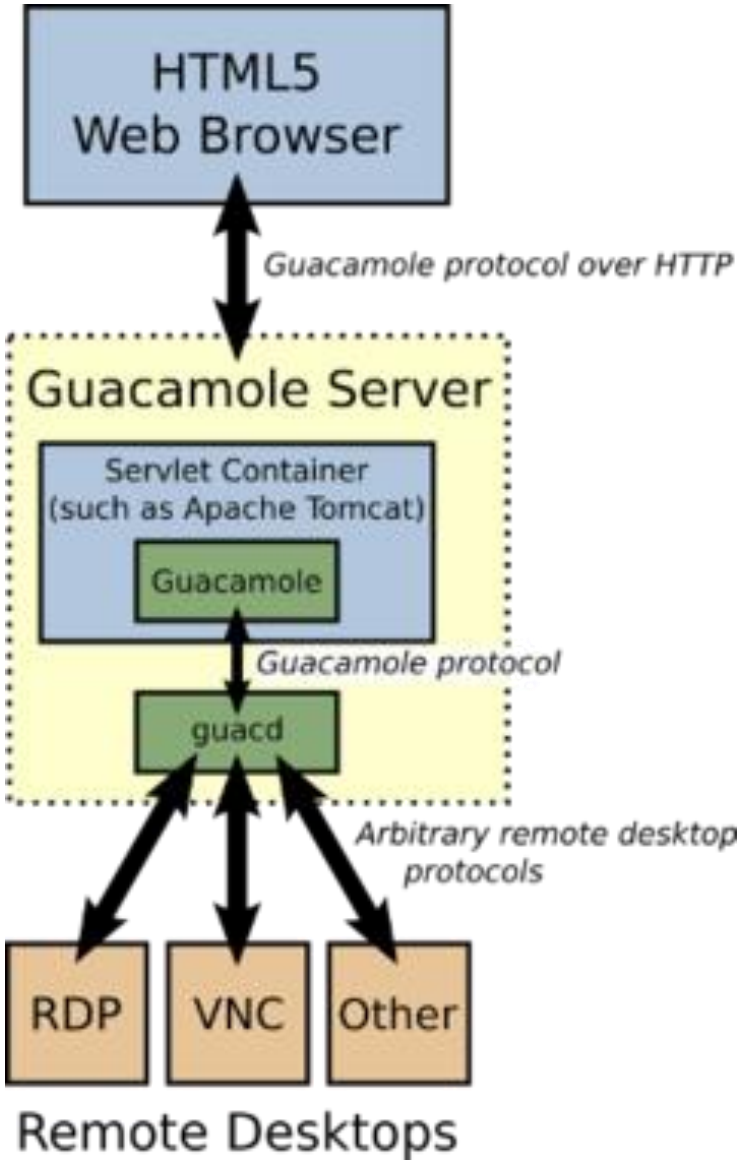
- Busca de uma solução para acesso remoto de maneira orquestrada (gateway).
- De preferência que seja de código aberto.
- Que mantenha um registro das conexões realizadas pelos usuários para fins de auditoria.
- Seguro, com criptografia e integrado a base de usuários.
- Sem a instalação de softwares clientes ou plug-ins.

Solução pesquisada encontrada

- Projeto Apache Guacamole.
- Possibilita o acesso remoto utilizando apenas o Navegador Web (Browser).
- Age como um intermediário (proxy) até o dispositivo computacional interno na rede da Universidade.
- Suporte aos protocolos: RDP, VNC, SSH.
- Seguro com certificado digital em todo o caminho até a aplicação e conexão ao dispositivo final.
- Integrado com as bases de dados (Openldap, Active Directory, MariaDB, MySQL).

Guacamole - Ambiente

- VM Oracle Linux 8 (4 vCPU, 4 GB RAM)
- Tomcat 9
- Java OpenJDK 11
- Apache Guacamole Server 1.4
- Guacamole Client (guacd)



Certificados e Segurança

- Certificados digitais em todos os componentes da arquitetura do Guacamole.

Importando o certificado raiz e intermediário da autoridade certificadora:

```
# keytool -import -trustcacerts -alias root -file ac-raiz.pem -keystore .keystore
# keytool -import -trustcacerts -alias intermediate -file cadeia-intermediaria.pem -keystore .keystore
```

Importando o certificado recebido da autoridade certificadora:

```
# keytool -import -trustcacerts -alias tomcat -file certificado.pem -keystore .keystore
```

Certificados e Segurança

Configurando o Conector Tomcat editando o arquivo server.xml:

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
               maxThreads="150" SSLEnabled="true" scheme="https" secure="true"
               keystoreFile=".keystore" keystorePass="password"
               clientAuth="false" sslProtocol="TLS" />
```

Importar o certificado digital da autoridade certificadora no armazenamento de chaves do Java:

```
# keytool -importcert -alias "guacd" -keystore /etc/pki/java/cacerts -file /etc/pki/tls/certs/certificado.pem
```

Alterar o arquivo de serviços guacd.service do systemctl e incluir o caminho do certificado e da chave:

```
ExecStart=/usr/local/sbin/guacd -f $OPTS -C /etc/pki/tls/certs/certificado.pem -K /etc/pki/tls/certs/key.pem
```

Interface Administração

Active Sessions | History | Users | Groups | Connections | Preferences

History records for past connections are listed here and can be sorted by clicking the column headers. To search for specific records, enter a filter string and click "Search". Only records which match the provided filter string will be listed.

Filter | Search | Download

Username	Start time ▲	Duration	Connection name	Remote host
pedro.	2022-11-30 14:47:52	19 seconds	UL57-D55	2801:8a:c040:fca9:0:0:0:
pedro.	2022-11-30 14:47:22	31 seconds	UL57-D01	2801:8a:c040:fca9:0:0:0:
pedro	2022-11-30 14:40:51	6.1 minutes	UL57-D01	2801:8a:c040:fca9:0:0:0
anthony.	2022-11-30 11:23:05	4.7 hours	DESK-ANTHONY	2801:8a:c040:fca9:0:0:0:
anthony.	2022-11-30 09:38:56	1.6 hours	DESK-ANTHONY	2801:8a:c040:fca9:0:0:0:
anthony.	2022-11-30 09:38:24	31 seconds	DESK-ANTHONY	2801:8a:c040:fca9:0:0:0:
anthony.	2022-11-30 09:38:20	3 seconds	DESK-ANTHONY	2801:8a:c040:fca9:0:0:0:
anthony.c	2022-11-30 09:37:49	31 seconds	DESK-ANTHONY	2801:8a:c040:fca9:0:0:0:
anthony.	2022-11-30 09:37:18	30 seconds	DESK-ANTHONY	2801:8a:c040:fca9:0:0:0:
anthony.c	2022-11-30 09:36:59	17 seconds	DESK-ANTHONY	2801:8a:c040:fca9:0:0:0:
anthony.	2022-11-30 09:36:28	31 seconds	DESK-ANTHONY	2801:8a:c040:fca9:0:0:0
anthon	2022-11-30 09:02:00	34.3 minutes	DESK-ANTHONY	2801:8a:c040:fca9:0:0:0:
henri.	2022-11-29 21:29:46	42.7 minutes	DESK-HENRI	2801:8a:c040:fca9:0:0:0:
henri.	2022-11-26 10:53:56	17 seconds	DESK-HENRI	2801:8a:c040:fca9:0:0:0:
johan	2022-11-25 15:22:41	24 seconds	LABFIC02	2801:8a:c040:fca9:0:0:0:
johan.	2022-11-25 15:22:02	37 seconds	LABFIC02	2801:8a:c040:fca9:0:0:0:
johan	2022-11-25 15:14:26	7.4 minutes	LABFIC02	2801:8a:c040:fca9:0:0:0:

Interface Administração

Active Sessions | History | Users | Groups | Connections | Preferences

Options below are related to the locale of the user and will impact how various parts of the interface are displayed.

Display language:

Timezone: America / Sao Paulo

DEFAULT INPUT METHOD

The default input method determines how keyboard events are received by Guacamole. Changing this setting may be necessary when using a mobile device, or when typing through an IME. This setting can be overridden on a per-connection basis within the Guacamole menu.

- (•) None

  No input method is used. Keyboard input is accepted from a connected, physical keyboard.

- ( ) Text input

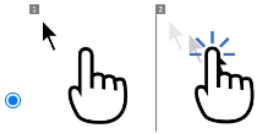
  Allow typing of text, and emulate keyboard events based on the typed text. This is necessary for devices such as mobile phones that lack a physical keyboard.

- ( ) On-screen keyboard

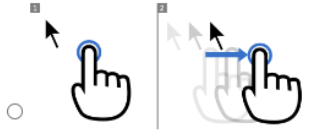
  Display and accept input from the built-in Guacamole on-screen keyboard. The on-screen keyboard allows typing of key combinations that may otherwise be impossible (such as Ctrl-Alt-Del).

DEFAULT MOUSE EMULATION MODE

The default mouse emulation mode determines how the remote mouse will behave in new connections with respect to touches. This setting can be overridden on a per-connection basis within the Guacamole menu.



Tap to click. The click occurs at the location of the touch.



Drag to move the mouse pointer and tap to click. The click occurs at the location of the pointer.

Suporte a IPv6

- Apache Guacamole configurado para acesso IPv6 até a estação de trabalho do usuário.
- Usuário com IPv6 em suas casas conseguiram obter uma maior estabilidade no acesso. Sem tradução CGNAT.
- Maior controle de acesso, auditoria e facilidade no troubleshooting.
- Tendência natural na adoção do protocolo IPv6 em todos os serviços da Universidade.

Conclusão

- Solução segura e viável para um grande número de máquinas.
- Os computadores remotos podem ser acessados também com tablets e smartphones através dos navegadores.
- Sem necessidade de instalação de clientes (clientless).
- Acesso remoto controlado e centralizado através de um gateway.
- Fornece um relatório dos usuários para auditoria.
- Dispensa a configuração de túneis SSH, liberações de portas nos firewalls.
- Devido a boa aceitação, a solução continua sendo muito utilizado mesmo com o retorno presencial as atividades.

Referências

- Projeto Guacamole

https://guacamole.apache.org/

- Tomcat Apache

https://tomcat.apache.org/

- Wiki BPF

https://wiki.brasilpeeringforum.org/w/Configurando_um_gateway_de_acesso_remoto_com_Guacamole

Muito Obrigado !!

Henri A. Godoy

henri@unicamp.br

/henri-alves-godoy/

Perguntas ?