Como a conexão do parvoíce trabalha para a presença da área de trabalho do agente da fineza

Índice

Introdução

Este original descreve a arquitetura atrás das conexões da fineza que usa Bidirecional-córregos sobre HTTP síncrono (PARVOÍCE) e como as edições se relacionaram a esta pode ser diagnosticado.

Que é PARVOÍCE?

O protocolo elástico da Mensagem e da presença (XMPP) é protocolo stateful em um client-server model. Se um aplicativo precisa de trabalhar com XMPP, as edições múltiplas elevaram. Os navegadores não apoiam XMPP nativamente, assim que todo o tráfego XMPP deve ser segurado por um programa que seja executado dentro do navegador.

O primeiro problema é que o HTTP é protocolo apátrida. Isto significa que cada pedido do HTTP não está relacionado a nenhum outro pedido. Contudo, este problema pode ser endereçado por aplicável significa--por exemplo usando Cookie/dados do cargo.

O segundo problema é o comportamento unidirecional do HTTP. Somente o cliente envia pedidos, e o server pode somente responder. A incapacidade do server empurrar dados faz não natural executar XMPP sobre o HTTP.

Este problema é eliminado se o cliente pode fazer pedidos diretos TCP (assim eliminando a necessidade de HTTP). Contudo, se você quer endereçar o problema dentro do domínio HTTP (por exemplo porque o Javascript pode enviar pedidos do HTTP), há duas soluções possíveis. Ambos exigem uma ponte entre o HTTP e o XMPP. As soluções estão votando (os pedidos do HTTP repetidos que pedem dados novos) e as votações longas, igualmente conhecidas como o PARVOÍCE.

A finalidade de usar o PARVOÍCE é cobrir acima o fato de que o server não tem que responder porque logo há um pedido. A resposta está atrasada (uma votação longa) até que o server tenha

dados para o cliente, e está enviado então como a resposta. Assim que o cliente o obtiver faz um pedido novo (mesmo se não não tem nada enviar) e assim por diante.

O PARVOÍCE é bastante eficiente do ponto de vista da carga do servidor e tráfego-sábio.

O cliente de desktop da fineza (aplicativo de web) estabelece uma conexão velha do PARVOÍCE cada 30 segundos. Após 30 segundos, se não há nenhuma atualização do serviço de Notificaiton da fineza, o serviço de notificação envia uma resposta HTTP com uma APROVAÇÃO 200 e (quase) um corpo vazio da resposta. Se o serviço de notificação tem uma atualização na presença de um agente ou um evento do diálogo (atendimento), por exemplo, os dados são enviados imediatamente ao cliente web da fineza.

Para resumir:

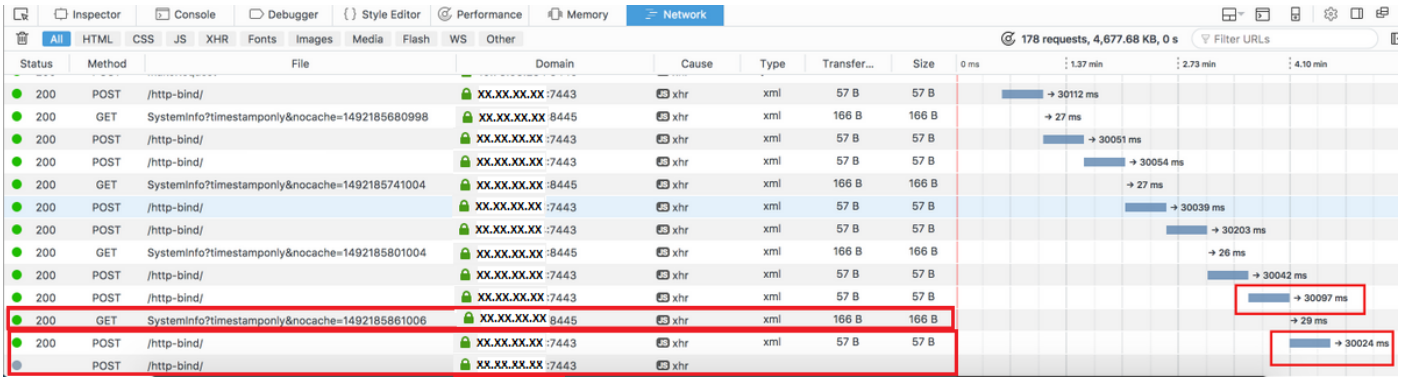
1. O cliente web da fineza terá sempre uma conexão de HTTP velha (HTTP-ligamento) estabelecida ao server da fineza através da porta TCP 7443. Isto é sabido como uma votação longa do PARVOÍCE.

2. O serviço de notificação da fineza é um serviço da presença que afixe atualizações em relação ao estado de um agente, de um atendimento, etc.

3. Se o serviço de Notiication tem uma atualização, responderá ao pedido do HTTP-ligamento com a atualização do estado como uma mensagem XML no corpo da resposta HTTP.

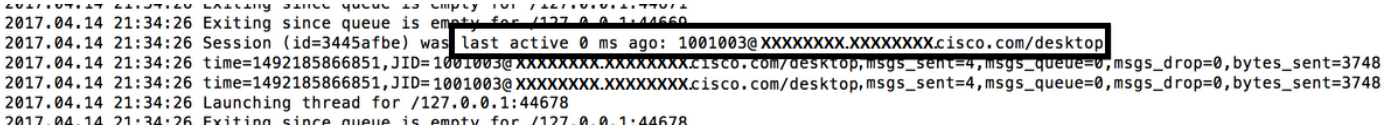
4. Se há nenhum estado atualiza 30 segundos após ter recebido o pedido do HTTP-ligamento, o serviço de Notificaiton responde sem nenhumas atualizações do estado para permitir que o cliente web da fineza envie um outro pedido do HTTP-ligamento. Isto serve como uma maneira para o serviço de notificação de saber que o cliente web da fineza pode ainda conectar ao serviço de notificação e que o agente não fechou seu navegador nem pôs seu computador para dormir, etc.

Também, o cliente web da fineza envia um pedido de SystemInfo que verifique o estado de Tomcat da fineza cada minuto, segundo as indicações da imagem:



Segundo as indicações da imagem, o serviço de notificação (Openfire) debuga o log mostra o HTTP que liga com o desktop junto com o endereço IP de Um ou Mais Servidores Cisco ICM NT e a porta do agente PC.

Segundo as indicações da imagem, o **último active 0 Senhoras** mostra que a sessão é ainda ativa.



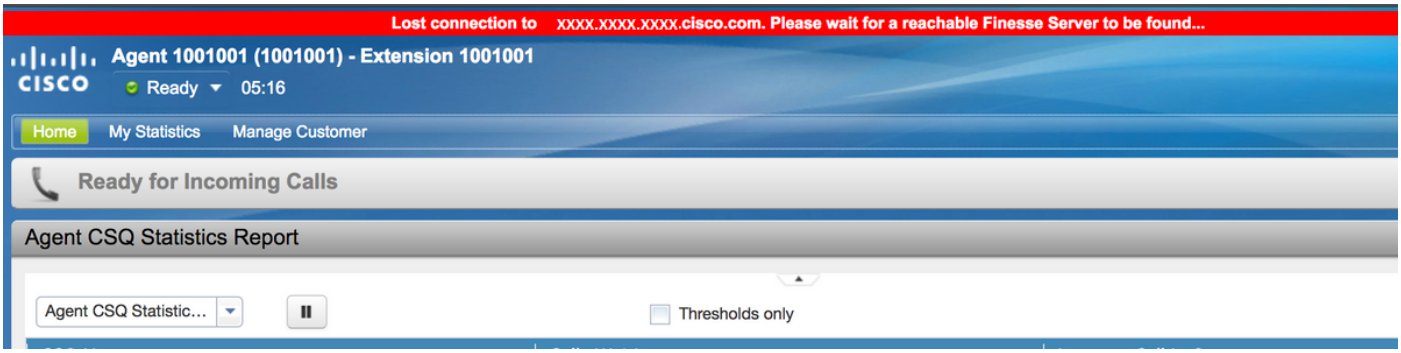
Permita o serviço de notificação debugam logs do centro de contato unificado expresso (UCCX), segundo as indicações da imagem:

```
admin:utils uccx notification-service log enable

WARNING! Enabling Cisco Unified CCX Notification Service logging can affect system performance
and should be disabled when logging is not required.

Do you want to proceed (yes/no)? yes

Cisco Unified CCX Notification Service logging enabled successfully.

NOTE: Logging will be disabled automatically if Cisco Unified CCX Notification Service is restarted.
admin:
```

Permita o serviço de notificação debugam logs da empresa unificada do centro de contato (UCCE) (fineza autônoma), segundo as indicações da imagem:

```
admin:utils finesse notification logging enable

Checking that the Cisco Finesse Notification Service is started...
The Cisco Finesse Notification Service is started.

Cisco Finesse Notification Service logging is now enabled.

WARNING! Cisco Finesse Notification Service logging can affect system performance
and should be disabled when logging is not required.

Note: Logging will be disabled automatically if you restart the Cisco Finesse Notification Service.
```

Problema comum devido à disconexão do PARVOÍCE



Para UCCX, o temporizador da saída é 60 segundos depois que disconexão do navegador. O agente pode estar no pronto ou não no estado pronto para que a saída aconteça.

Para UCCE, a fineza toma até 120 segundos para detectar quando um agente fecha o navegador ou o navegador causa um crash e a fineza espera 60 segundos antes de enviar um pedido forçado da saída ao CTI Server. Sob estas condições, a fineza pode tomar até 180 segundos para assinar para fora o agente.

Para obter mais informações sobre do comportamento do Desktop da fineza UCCE, refira a seção do *comportamento do Desktop do* capítulo dos *mecanismos do Failover da fineza de Cisco no* Guia de Administração da fineza de Cisco.

Registre a análise

Os log de serviço da fineza e do Notificaiton podem ser recolhidos através de RTMT ou através do CLI:

o arquivo obtém o activelog /desktop retorna compressa

Debugar logs

Estes logs estão no dobrador de /desktop/logs/openfire e são nomeados debug.log.

```
2017.06.17 00:14:34 Session (id=f382a015) was last active 0 ms ago:
1001003@xxxxx.xxxx.xxx.cisco.com/desktop
2017.06.17 00:15:04 Session (id=f382a015) was last active 13230 ms ago:
1001003@xxxxx.xxxx.xxx.cisco.com/desktop
2017.06.17 00:15:34 Session (id=f382a015) was last active 43230 ms ago:
1001003@xxxxx.xxxx.xxx.cisco.com/desktop
2017.06.17 00:16:04 Session (id=f382a015) was last active 63231 ms ago:
1001003@xxxxx.xxxx.xxx.cisco.com/desktop

2017.06.17 00:17:04 Unable to route packet. No session is available so store offline. <message
from="pubsub. xxxxx.xxxx.xxx.cisco. com" to="1001003@xxxxx.xxxx.xxx.cisco.com.cisco.com"
id="/finesse/api/User/1001003__1001003@xxxxx.xxxx.xxx.cisco.com__o5Aqb"><event
xmlns="http://jabber.org/protocol/pubsub#event"><items node="/finesse/api/User/1001003"><item
id="0d78a283-466d-4477-a07e-6e33a856fce388"><notification
xmlns="http://jabber.org/protocol/pubsub">&lt;Update&gt
```

Logs da informação

Estes logs estão no dobrador de **/desktop/logs/openfire** e são nomeados info.log.

```
2017.06.17 00:16:04 Closing idle session (id=f382a015): 1001003@xxxxx.xxxx.xxx.
cisco.com/desktop after being inactive for more than threshold value of 60
2017.06.17 00:16:04 A session is being closed for 1001003@xxxxx.xxxx.xxx. cisco.com/desktop
```

Openfire fechando a sessão ociosa indica que saída do agente provocará 1 minuto e este aparece como o código de motivo 255 nos relatórios

Logs de Webservices

Estes logs estão no dobrador de /desktop/logs/webservices e são nomeados Desktop-webservices.YYYY-MM-DDTHH-MM-SS.sss.log.

```
0000001043: XX.XX.XX.XXX: Jun 17 2017 00:16:04.630 +0530: %CCBU_Smack Listener Processor (1)-6-
PRESENCE_NOTIFICATION_RECIEVED: %[FROM
JID=1001003@xxxxx.xxxx.xxx.cisco.com/desktop][PRESENCE_TYPE=unavailable]:Finesse received a
presence notifcation
0000000417: XX.XX.XX.XXX: Jun 17 2017 00:16:04.631 +0530: %CCBU_Smack Listener Processor (1)-6-
UNSUBSCRIBE_REQUEST_SUCCESS:
%[NodeId=/finesse/api/User/1001003/ClientLog][user_id=1001003@xxxxx.xxxx.xxx.cisco.com]:
Sucessfully unsubscribed from a node on the XMPP server
0000001044: XX.XX.XX.XXX:  Jun 17 2017 00:16:04.631 +0530: %CCBU_Smack Listener Processor (1)-6-
AGENT_PRESENCE_MONITOR: %[message_string=Adding agent 1001003 into the expiry hash.]:
0000001051: XX.XX.XX.XXX:  Jun 17 2017 00:16:35.384 +0530: %CCBU_pool-8-thread-1-6-
AGENT_PRESENCE_MONITOR: %[message_string=[Expired] Removed agent from cache 1001003]:
0000001060: XX.XX.XX.XXX:: Jun 17 2017 00:17:04.632 +0530: %CCBU_CoreImpl-worker12-6-PRESENCE
DRIVEN LOGOUT: %[agent_id=1001003]: Performing CTI Logout on basis of the agents unavailable
presence
0000001061: XX.XX.XX.XXX:: Jun 17 2017 00:17:04.633 +0530: %CCBU_CoreImpl-worker12-6-
MESSAGE_TO_CTI_SERVER: %[cti_message=Invoke id :39 , agentstate : 1, workmode : 0, reason code:
255, forceflag :1, agentcapacity: 1, agentext: 1001003, agentid: 1001003, supervisorid: null,
ssoFlag=false][cti_message_name=SetAgentStateReq]: Message going to the backend cti server
0000001066:  XX.XX.XX.XXX:: Jun 17 2017 00:17:04.643 +0530: %CCBU_CTIMessageEventExecutor-0-6-
DECODED_MESSAGE_FROM_CTI_SERVER: %[cti_message=CTIAgentStateEvent [skillGroupState=1 (LOGOUT),
stateDuration=0, skillGroupNumber=-1, skillGroupPriority=0, agentState=1 (LOGOUT),
eventReasonCode=255, numFltSkillGroups=0, CTIClientSignature=null, agentID=1001003,
agentExtension=1001003, agentInstrument=null, agentID_Long=1001003, duration=null,
nextAgentState=null, fltSkillGroupNumberList=[], fltSkillGroupIDList=[],
fltSkillGroupPriorityList=[], fltSkillGroupStateList=[], MRDId=1, agentMode=0]CTIMessageBean
[invokeID=null, cti_sequence_id=105, msgID=30,
timeTracker={"id":"AgentStateEvent","CTI_MSG_RECEIVED":1497638824642,"CTI_MSG_DISPATCH":14976388
24643}, msgName=AgentStateEvent, deploymentType=CCX]][cti_response_time=1][dispatch_phase=DnD-
CHECKPOINT-3B]: Decoded Message to Finesse from backend cti server
```

Motivos comuns para a disconexão do PARVOÍCE

- Questão de rede
- Navegador e/ou versão Unsupported.
- Condição travada do navegador devido a satisfazer da outra aba/indicador.
- Computador posto para dormir.
- Edição da alta utilização da CPU ou da memória alta no server.
- Dispositivos da 3ª parte que fazem a atividade dos shenanigans no fundo.
- Conexão perdedora do motor CTI Server/CCX com o server da fineza.
- Edição NTP no server ou no cliente.

Ações da sugestão

- Use o navegador suportado/versão e os ajustes conforme os guias.
- Teste o comportamento com todos os dispositivos da 3ª parte removidos.

- Compreenda o comportamento e o fluxo de trabalho do agente.
- Reinicie a fineza Tomcat de Cisco e o serviço de notificação.
- Execute **utils diagnosticam o teste no** server, e validam-no para a frente e pesquisa de DNS reversa do server e do cliente ambos.
- Verifique o **estado NTP dos utils no** server.
- Nos logs do cliente, verifique a tração e a latência da rede. Os logs do cliente podem ser considerados dos logs do console de web do navegador ou pressionando os **relatórios de erro da emissão na** página da fineza e recolhendo os logs da fineza. Os logs são ficados situados em **/desktop/logs/clientlogs**.

  Note: Os valores de temporizador puderam mudar no futuro conforme o requerimento do produto.