AnyConnect-handleiding voor optimale gateway voor probleemoplossing

Inhoud

Inleiding Hoe werkt OGS? **OGS-cache** Locatiebepaling Foutenscenario's Wanneer de connectiviteit op de gateway is verloren Hervat na suspensie TCP uitgestelde-ACK-venstergrootte selecteert een onjuiste gateway Typisch gebruikersvoorbeeld Probleemoplossing OGS Stap 1. Verwijder de OGS-cache om een herevaluatie te forceren Stap 2. Leg de servertests vast tijdens het verbindingsproject Stap 3. Controleer de gateway die door OGS is geselecteerd Stap 4. Vestig de OGS-berekeningen die door AnvConnect zijn uitgevoerd Analyse Vraag en antwoord

Inleiding

Dit document beschrijft hoe u problemen met uw probleemoplossing kunt oplossen met OGS (Optimal Gateway Selection). OGS is een functie die kan worden gebruikt om te bepalen welke gateway de laagste Ronde Trip Time (RTT) heeft en die poort aan te sluiten. U kunt de OGS-functie gebruiken om de latentie voor internetverkeer tot een minimum te beperken zonder tussenkomst van de gebruiker. Met OGS identificeert Cisco AnyConnect Secure Mobility Client (AnyConnect) en selecteert u welke beveiligde gateway het beste is voor verbinding of opnieuw aansluiten. De OGS begint bij de eerste aansluiting of op een heraansluiting ten minste vier uur na de vorige ontkoppeling. U vindt meer informatie in de <u>Administrator's guide</u>.

Tip: OGS werkt het beste met de nieuwste AnyConnect-client en ASA-software versie $9.1(3)^*_{-}$ of hoger.

Hoe werkt OGS?

Een eenvoudig ICMP-**ping** (Internet Control Message Protocol)-verzoek (ICMP) werkt niet omdat veel firewalls van Cisco Adaptieve security applicatie (ASA) zijn ingesteld om ICMP-pakketten te blokkeren om ontdekkingen te voorkomen. In plaats daarvan stuurt de client drie HTTP/443-verzoeken naar elk head-end die verschijnt in een **fusie** van alle profielen. Deze HTTP-tests worden OGS-pings in de stammen genoemd, maar, zoals eerder uitgelegd, zijn het geen ICMP-pings. Om ervoor te zorgen dat een (her)verbinding niet te lang duurt, selecteert OGS de vorige

gateway standaard als deze geen OGS ping-resultaten binnen zeven seconden ontvangt. (Bekijk de **resultaten van OGS** in het logbestand.)

Opmerking: AnyConnect moet een HTTP-aanvraag naar 443 sturen, omdat de reactie zelf belangrijk is en geen succesvol antwoord. Helaas wordt alle verzoeken als HTTPS door de regeling voor de behandeling van volmachten verzonden. Zie Cisco bug-ID <u>CSCtg38672</u> - OGS moeten met HTTP-aanvragen worden geping.

Opmerking: Als er geen head-ends in de cache zijn, stuurt AnyConnect eerst één HTTPaanvraag om te bepalen of er een authenticatieproxy is en of deze het verzoek kan verwerken. Pas na dit eerste verzoek begint het met de OGS-pings om de server te testen.

- OGS bepaalt de gebruikerslocatie op basis van de netwerkinformatie, zoals het Domain Name System (DNS)-achtervoegsel en het DNS-server-IP-adres. De RTT - resultaten worden samen met deze locatie opgeslagen in de OGS - cache.
- OGS-locatiegegevens worden gedurende 14 dagen opgeslagen. Cisco bug-ID <u>CSCtk6531</u> is gedeponeerd om deze instellingen door de gebruiker te configureren.
- OGS wordt pas 14 dagen nadat de locatie voor het eerst is gecachaliseerd, vanuit deze locatie opnieuw uitgevoerd. Gedurende deze tijd gebruikt het de gecachede ingang en de voor die locatie bepaalde RTT's. Dit betekent dat wanneer AnyConnect opnieuw wordt opgestart, deze geen OGS opnieuw uitvoert; in plaats daarvan gebruikt het de optimale gateway order in het cache voor die locatie. In de DART-logbestanden (Diagnostic AnyConnect Reporting Tool) wordt dit bericht gezien:

• RTT wordt bepaald met een TCP-uitwisseling naar de Secure Socket Layer (SSL) poort van de gateway waarnaar de gebruiker zal proberen te verbinden zoals gespecificeerd door de host-ingang in het AnyConnect-profiel.

Opmerking: In tegenstelling tot HTTP-ping, dat een simpel HTTP-bericht doet en dan de RTT en het resultaat weergeeft, zijn OGS-berekeningen iets ingewikkelder. AnyConnect stuurt drie probes voor elke server en berekent de vertraging tussen het HTTP-SYN dat wordt verzonden en de FIN/ACK voor elk van deze problemen. Daarna gebruikt het de laagste delta's om de servers te vergelijken en zijn selectie te maken. Dus hoewel HTTP-pings een redelijk goede indicatie zijn van welke server de AnyConnect zal kiezen, zullen ze niet per se overeenkomen. In de rest van het document is daar meer informatie over te vinden.

- Op dit moment voert OGS alleen controles uit als de gebruiker een schorsing heeft opgelopen en de drempel is overschreden. OGS sluit geen verbinding aan met een andere ASA als de ASA-gebruiker op crashes is aangesloten of niet beschikbaar wordt. OGS contacteert alleen de primaire servers in het profiel om de optimale te bepalen.
- Nadat het OGS-clientprofiel is gedownload, wanneer de gebruiker de AnyConnect-client opnieuw start, wordt de optie om andere profielen te selecteren, zoals hieronder wordt weergegeven:

6	Cisco AnyCor	nnect Secure Mobility Client	x		
-		VPN: Please enter your username and password.			
		Automatic Selection Connect			
	\$ (i)		altalta cisco		

Zelfs als de gebruikersmachine meerdere andere profielen heeft, kunnen ze geen van deze profielen selecteren totdat de OGS onevenwichtig is.

OGS-cache

Zodra de berekening is voltooid, worden de resultaten opgeslagen in het **preferent_global** bestand. Er zijn problemen geweest met deze gegevens die niet eerder in het bestand zijn opgeslagen.

Raadpleeg Cisco bug-ID <u>CSCtj84626</u> voor meer informatie.

Locatiebepaling

OGS caching werkt op een combinatie van het DNS-domein en de afzonderlijke DNS-serveradressen. Het werkt als volgt:

- Location A heeft een DNS-domein van locationa.com, en twee DNS server-IP-adressen ip1 en ip2. Elke domein/IP-combinatie creëert een cache-toets die wijst op een OGS-cacheingang. Bijvoorbeeld: locatiea.com/ip1 -> ogscache1locatiea.com/ip2 -> ogscache1
- Als AnyConnect vervolgens op een fysiek ander netwerk wordt aangesloten, wordt dezelfde combinatie van domein/IP-combinaties gecreëerd en gecontroleerd aan de hand van de gecachgeerde lijst. Als er überhaupt enige overeenkomsten zijn, wordt die OGS cache waarde gebruikt, en wordt de client nog steeds beschouwd als locatie A.

Foutenscenario's

Hier zijn een paar mislukkingsscenario's die gebruikers zouden kunnen tegenkomen:

Wanneer de connectiviteit op de gateway is verloren

Als OGS wordt gebruikt, als de aansluitingen op de gateway naar welke de gebruikers zijn verbonden, verloren gaan, sluit AnyConnect zich aan op de servers in de **reserveserverlijstenniet** naar de volgende OGS-host. De volgorde van de werkzaamheden is als volgt:

- 1. OGS contacteert alleen de primaire servers om de optimale te bepalen.
- 2. Zodra bepaald, is het verbindingsalgoritme:

Probeer verbinding te maken met de optimale server. Als dat mislukt, probeer dan de reserveserverlijst van de optimale server. Als dat mislukt, probeert u elke server die in de OGS-selectielijst blijft staan, geordend door de selectieresultaten.

Opmerking: Wanneer de beheerder de reserveserverlijst vormt, staat de huidige profieleditor alleen de beheerder toe om de Fully Qualified Domain Name (FQDN) voor de reserveserver in te voeren, maar niet de gebruikersgroep zoals mogelijk is voor de primaire server:

FQDN or IP Addr		User Group					
rtpvpnoutbound6.ci	sco.com	/ ogs					
Group URL							
Backup Server List			Load Balancing Server List				
			"Always On" is disabled. Lo	oad Balancing Fields have been d	isabl		
Host Address		Add	Host Address	Add			
		Move Up		Delete			
		Move Down					
		Delete					
Primary Protocol		[SSL ‡]	Automatic SCEP Host				
Standard Auth	entication Only (IOS ga		CAURL		1		
Auth Method	During IKE Negotiation	[IKE-R ≎	Prompt For Challenge Pass	word	_		
IKE Identity			CA Thumbprint				
		ОК	Cancel				

Cisco bug ID <u>CSCud84778</u> is gedeponeerd om dit te corrigeren, maar de volledige URL moet in het veld host-adres voor de reserveserver worden ingevoerd, en deze moet werken: https://<ip-adres/gebruikersgroep.

Hervat na suspensie

De OGS kunnen pas worden uitgevoerd nadat de computer is hervat als de stekker is aangesloten. OGS nadat een cv is gestart wordt alleen uitgevoerd nadat de netomgeving is getest, wat bedoeld is om te bevestigen dat de netwerkconnectiviteit beschikbaar is. Deze test bevat een DNS-connectiviteit-subtest.

Als de DNS-server echter laat vallen typt A-verzoeken met een IP-adres in het query-veld, in plaats van te reageren met "name niet gevonden" (het meest gebruikelijke geval, altijd aangetroffen tijdens testen), dan Cisco bug-ID <u>Cti20768</u> "DNS query van type A voor IP adres

moet PTR zijn om timeout te vermijden" van toepassing.

TCP uitgestelde-ACK-venstergrootte selecteert een onjuiste gateway

Wanneer ASA-versies eerder dan versie 9.1(3) gebruikt worden, tonen de opnamen op de client een aanhoudende vertraging in de SSL-handdruk. Wat opgemerkt wordt is dat de cliënt zijn CliëntHallo verstuurt, dan verstuurt de ASA zijn ServerHallo. Dit wordt normaal gevolgd door een certificaatbericht (optioneel certificaatverzoek) en een bericht van de ServerHelloReady. De anomalie is tweevoudig:

- 1. De ASA stuurt het certificaatbericht niet onmiddellijk na de ServerHallo. De grootte van het clientvenster is 64.860 bytes, die meer dan genoeg zijn om de gehele respons van de ASA te behouden.
- 2. De client ACK the ServerHello niet direct, dus geeft de ASA de ServerHello terug na ~120ms, op welk punt de client ACKs de gegevens doorgeeft. Het certificaatbericht wordt vervolgens verzonden. Het is bijna alsof de klant op meer data wacht.

Dit gebeurt vanwege de interactie tussen TCP langzaam-start en TCP vertraagde-ACK. Voorafgaand aan ASA versie 9.1(3), gebruikt de ASA een langzaam-start venstergrootte van 1, terwijl de Windows client een vertraagde-ACK waarde van 2 gebruikt. Dit betekent dat de ASA slechts één datapakket stuurt tot het een ACK krijgt, maar het betekent ook dat de client geen ACK verstuurt tot hij twee datapakketten ontvangt. De ASA keer uit na 120ms en geeft de ServerHello terug, waarna de client ACKs de gegevens doorzet. Dit gedrag werd gewijzigd door Cisco bug ID <u>CSCug98113</u> zodat de ASA een langzaam begin venster grootte van 2 standaard in plaats van 1 gebruikt.

Dit kan invloed hebben op de OGS-berekening wanneer:

- Verschillende gateways runnen verschillende ASA versies.
- Clients hebben verschillende vertraagde-ACK venstergrootte.

In dergelijke situaties kan de door de vertraagde ACK geïntroduceerde vertraging volstaan om de klant ertoe te brengen de verkeerde ASA te selecteren. Als deze waarde verschilt tussen de klant en de ASA, zouden er nog problemen kunnen zijn. In dergelijke situaties moet het tijdelijke beeld worden aangepast.

Windows

- 1. Start de griffier.
- 2. Identificeer de okring van de interface waarop u de vertraagde-ACK wilt uitschakelen. Om dit

te doen, navigeer aan: HKEY_LOCAL_MACHINE > SOFTWARE > Microsoft > WindowsNT > Huidige versie > Netwerkkaarten > (nummer). Kijk naar elk nummer dat staat onder NetworkCards. Aan de rechterkant zou de Description een lijst moeten geven van de interface (bijvoorbeeld Intel(R) Wireless WiFi Link 5100AGN) on de ConviceName zou oon lijst moeten maken van de corresponderende GUID. en de ServiceName zou een lijst moeten maken van de corrésponderende GUID.

- Zoek en klik vervolgens op deze registratiesubkey: HKEY LOCAL MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interface s\<interface-GUIT>
- 4. Klik in het menu Bewerken op Nieuw en vervolgens op Waarde WOORD.
- 5. Geef de nieuwe waarde TcpAckFrequency een naam en geef deze een waarde van 1 toe.

- 6. Verstop de griffier.
- 7. Start Windows nogmaals om deze wijziging in werking te stellen.

Opmerking: Cisco bug-ID <u>CSCum19065</u> is gedeponeerd om TCP-tuningparameters configureerbaar te maken in de ASA.

Typisch gebruikersvoorbeeld

Het meest gebruikelijke gebruikcase is wanneer een gebruiker thuis OGS voor het eerst gebruikt, registreert het de DNS-instellingen en de OGS ping-resultaten in het cache (standaard een tijdelijke oplossing van 14 dagen). Wanneer de gebruiker de volgende avond naar huis terugkeert, detecteert OGS dezelfde DNS instellingen, vindt het in het cache en slaat de OGS ping-test over. Later, wanneer de gebruiker naar een hotel of restaurant gaat dat internetservice aanbiedt, detecteert OGS verschillende DNS instellingen, voert de OGS ping-tests uit, selecteert de beste gateway en registreert de resultaten in het cache.

De verwerking is identiek wanneer deze hervat wordt vanuit een geschorste of gehiberde toestand, als de OGS en AnyConnect dit mogelijk maken.

Probleemoplossing OGS

Stap 1. Verwijder de OGS-cache om een herevaluatie te forceren

Om het OGS cache te wissen en de RTT voor beschikbare gateways opnieuw te evalueren, dient u het Global AnyConnect-bestand van de PC te verwijderen. De locatie van het bestand varieert op basis van het besturingssysteem:

• Windows Vista en Windows 7

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\preferences_global.xml Note: in older client versions it used to be stored in C:\ProgramData\Cisco\Cisco AnyConnect VPN Client

Windows XP

C:\Documents and Settings\AllUsers\Application Data\Cisco\Cisco AnyConnect VPN Client\preferences_global.xml

Mac OS X

/opt/cisco/anyconnect/.anyconnect_global Note: with older versions of the client it used to be /opt/cisco/vpn..

Linux

/opt/cisco/anyconnect/.anyconnect_global Note: with older versions of the client it used to be /opt/cisco/vpn..

Stap 2. Leg de servertests vast tijdens het verbindingsproject

1. Start draadloos op de testmachine.

- 2. Start een verbindingspoging op AnyConnect.
- 3. Stop de draadloze vangst zodra de verbinding is voltooid. Tip: Aangezien de opname alleen wordt gebruikt om OGS te testen, is het het beste om de opname te stoppen zodra AnyConnect een gateway selecteert. Het is het beste om geen volledige verbindingspoging te doen, omdat dat de pakketvastlegging kan cloud maken.

Stap 3. Controleer de gateway die door OGS is geselecteerd

Voltooi de volgende stappen om te controleren waarom OGS een bepaalde gateway heeft geselecteerd:

- 1. Start een nieuwe verbinding.
- Start AnyConnect DART: Start AnyConnect en klik op Advanced.Klik op Diagnostiek.Klik op Volgende.Klik op Volgende.
- 3. Bekijk de DART-resultaten die in het nieuwe **DartBundle_XXXX_XXX.zip-**bestand op het bureaublad zijn gevonden.

Navigeer naar Cisco AnyConnect Secure Mobility Client > AnyConnect.txt.

Let op de tijd dat de OGS-spelden voor een bepaalde server vanaf dit DART-logbestand zijn gestart:

Meestal moeten ze rond dezelfde tijd zijn, maar voor het geval dat de opnamen groot zijn, helpt de tijdstempel vernauwen welke pakketten de HTTP-sondes zijn en welke de eigenlijke verbindingspogingen zijn.

Zodra AnyConnect drie speldenprikken naar de server stuurt, wordt dit bericht met de resultaten van elk van de speldenprikken gegenereerd:

 $\texttt{Description} : \texttt{Function}: \texttt{CHeadendSelection}::\texttt{CSelectionThread}::\texttt{logThreadPingResults} : \texttt{CSelectionThread}::\texttt{logThreadPingResults} : \texttt{CSelectionThread}::\texttt{logThreadPingResults} : \texttt{CSelectionThread}::\texttt{logThreadPingResults} : \texttt{CSelectionThread}::\texttt{logThreadPingResults} : \texttt{CSelectionThread}::\texttt{logThreadPingResults} : \texttt{CSelectionThread}::\texttt{logThreadPingResults} : \texttt{CSelectionThread} : \texttt{logThreadPingResults} : \texttt{CSelectionThread} : \texttt{CSelectionThread} : \texttt{logThreadPingResults} : \texttt{logThreadPingResults} : \texttt{CSelectionThread} : \texttt{CSelectionThread} : \texttt{logThreadPingResults} : \texttt{logTh$

File: .\AHS\HeadendSelection.cpp
Line: 1137
OGS ping results for gw2.cisco.com: (219 218 132)

Het is belangrijk om aandacht te besteden aan deze drie waarden, omdat ze moeten overeenkomen met de opnamesultaten.

Raadpleeg het bericht met "*** OGS Selectieresultaten***" om de beoordeelde RTT te zien en of de meest recente verbindingspoging het resultaat was van een gecachdeerde RTT of een nieuwe berekening.

Hierna volgt een voorbeeld:

Date : 10/04/2013 Time : 12:29:38 : Information Source Туре : vpnui Description : Function: CHeadendSelection::logPingResults File: .\AHS\HeadendSelection.cpp Line: 589 *** OGS Selection Results *** OGS performed for connection attempt. Last server: 'gw2.cisco.com' Results obtained from OGS cache. No ping tests were performed. Server Address RTT (ms) 302 gwl.cisco.com gw2.cisco.com 132 <======= As seen, 132 was the lowest delay of the three probes from the previous DART log gw3.cisco.com 506 gw4.cisco.com 877 Selected 'gw2.cisco.com' as the optimal server. *****

Stap 4. Vestig de OGS-berekeningen die door AnyConnect zijn uitgevoerd

Inspecteer de opname voor de TCP/SSL-sondes die gebruikt worden om RTT te berekenen. Zie hoe lang de HTTPS-aanvraag één TCP-verbinding overneemt. Elk sonde verzoek zou een andere TCP verbinding moeten gebruiken. Om dit te doen, opent u de opname in Wireshark en herhaalt u deze stappen voor elk van de servers:

 Gebruik het filter ip.addr om de pakketten die naar elk van de servers worden verzonden in hun eigen opname te isoleren. Om dit te doen, navigeer om te bewerken en selecteer Alle weergegeven pakketten markeren. Vervolgens navigeer u naar Bestand > Opslaan als, selecteer de optie alleen gemarkeerde pakketten en klik op Opslaan:

000 50 627494747,pcapeg Wiresh	urk 1.6.2 (SVN Rev 38931 from /trunk-1.6)
Elle Eak Yiew Co Capture Analyze Statistics Telephony Tools Internals Belp	m 🖬 M 🎫 🛠 1 🕅
Filter In addr == 10 100 154	UI 🖷 🗠 🖬 🖉 🖉 I 🗃
No. Time Source Destination Protocol Length Info	
677. 1301161063.040 🖲 🔿 🔿	Voried5535 Laned MSS=1460 SACK_PERM=1
dep 1301101000.104 dep 1301101003.104 Marrie:	40/00 A0/01 WERNOLDS CARNO POSHL350
690 1381161063.165 766 1381161063.288 Save in folder: Phy.Eller	Ack=114 Win=32768 Len=0
709 1381191083 288 Save in Torder.	CK1 Seg+1 4Ck+114 Min+52768 Len+0 14 Ack+2 Min+65595 Len+0
P Browse for other folders P Browse for other folders	egulli Ackuz Monufősői tenuð Monufősői tenuð Mosiládo SACK PERPLI
729 1381161063.412 220 1381161063.412	Arkellis Minespine Lenso Lenso Arkellis Minespine Lenso
721 1291 (61002.422) 721 1291 (61002.422) 0 All extern	egro Ackr3 Warnalsa Lano MSS1360
O Selected point only O Selected point only I 1	Ashe) kin-ssiss Lano
Frame 677: 62 bytes on Marked packets only 61 61	Annel
Internet Protocol Versi O Specify a packet garge: D O	
P Transcesson Control Pr	
Remove Ignored packets 0 0	
File type: Wireshark – pcaprig 💌	
Zancel Save	
	2
0000 00 24 14 95 30 46 10 44 f) 12 c6 49 09 00 45 00	
0010 00 20 Hd 1d 40 00 90 05 00 00 0a 0a 00 9a c1 5a .0	
0030 // 11 66 00 00 02 04 05 64 01 01 04 02	
File: "/Users/atbasu/Desktop/X-Files/627494747 Packets: 1538 Displayed: 61 Marked: 61 Los	d time: 0:10.992 Profile: Default

2. In deze nieuwe opname, navigeer naar Weergave > Weergave van tijd > Notatie > Datum en Tijd van dag:

0 0 (Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6)							
Elle Edit View Co Capture Analyze Statistics Telephony Iools Internals Help							
E 4 4 8	< Main Toolbar		🛶 🛪 🞍 🔲 🖼 ର ସ୍ଥ୍ୟ 🖉 🖬 🖬 🛸	1 22			
	✓ <u>Filter Toolbar</u>						
Filter: ip.	< <u>Statusbar</u>		pression Clear Apply				
No.	< Parket List		Protocol Length Info		i i i i i i i i i i i i i i i i i i i		
677	< Packet Details		CP 62 4542 > https: (SYN) Seq=0 VLn=62525 Len=0 MSS=.	AGO SACI_PERM	1		
560 509	< Packet Bytes		CP 52 https > 4542 [SYN, AOK] Seg=0 Ack+1 Win+9192 ; CP 54 4542 > https [408] Seg=1 Ack=1 Win+95526 Lense	.en=0 MSS=1260			
690		_	Contraction Cata				
700	Time Display Format		Date and Time of Day: 1970-01-01 01:02:03.123456	Ctrl+AR+L			
710	Name Resolution		Time of Day: 01:02:03.123456	Ctrl+Alt+2			
711	< Colorize Packet List		 Seconds Since Epoch (1970–01–01): 1234567890.123456 	Ctrl+AE+3			
713	 Auto Scroll in Lige Capture 		Seconds Since Beginning of Capture: 123.123456	Ctrl+AR+4			
730	Q Zoom In C	rl++	Seconds Since Previous Captured Packet: 1,123456	Ctrl+AR+5			
731	Q. Zoom Qut Q	trl+-	Seconds Since Hevidus Displayed Facket. 1.123456	CUTHAR+6			
134	③, Normal Size C	rl+=	Automatic (File Format Precision)				
b From 67	E Resize All Columns Shift+0	tri+R	Seconds: 0				
> Ethernet	Displayed Columns	•	Deciseconds: 0.1				
Enternet	Expand Subtrees Shift+	Right	Centiseconds: 0.12				
P Transmis	Expand All Ctrl+	Right	Milliseconds: 0.123				
	Collapse All Ctri	+Left	Microseconds: 0.123456				
	Colorian Commention		Nanoseconds: 0.123456789				
	Colorize Conversation		Display Seconds with hours and minutes	Ctrl+At+0			
	Reset Coloring 1–10 Ctri+	space					
	Soloring Rules						
	Show Packet in New Window						
	Beload C	tri+R					
0000 00 24	14 95 30 e5 f0 de f1 12 c5 e9 08 00 45 0 fd 1d 40 00 80 05 00 00 Ca Da 00 94 e1 6		.0E.				
0020 84 bc	XXXXX 94 br 11 br 01 bb 86 41 20 99 00 00 00 70 70 02						
ousu IT IT	ee us do co uz d4 c6 b4 d1 01 04 d2						
- Contraction		100					

3. Identificeer het eerste HTTP SYN-pakket in deze opname dat werd verzonden toen de OGSsonde werd verzonden op basis van de DART-logbestanden zoals geïdentificeerd in Stap 3.3.2. Het is belangrijk om te onthouden dat, voor de eerste server, het eerste HTTP-verzoek geen serversonde is. Het is gemakkelijk om het eerste verzoek om een server sonde te verwarren en zo te komen tot waarden die volledig anders zijn dan wat OGS rapporteert. Dit probleem wordt hier onder de aandacht gebracht:

	677 2013-10-07 11:51:03.040834 10.10.0.154		1930219ck02x388a	TCP	62 4542 > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
	689 2013-10-07 11:51:03.164885 10.10.0.154	Test HTTP Connection	\$93/636/937/2884×	TCP	54 4542 > https [ACK] Seg=1 Ack=1 Win=65535 Len=0
	690 2013-10-07 11:51:03.165061 10.10.0.154		191110.112.108	551.	167 Continuation Data
	710 2013-10-07 11:51:03.288837 10.10.0.154		1930110/10/1084	TCP	54 4542 > https [ACK] Seg=114 Ack=2 Win=65535 Len=0
	711 2013-10-07 11:51:03.288937 10.10.0.154		1931110113221080	TCP	54 4542 > https (FIN, ACK) Seg=114 Ack=2 Win=65535 Len=0
	713 2013-10-07 11:51:03.297522 10.10.0.154		193111011321188	TCP	62 4543 > https [SYN] Seg=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
	732 2013-10-07 11:51:03.424015 10.10.0.154		1930210:023702884	TCP	54 4543 > https [ACK] Seg=1 Ack=1 Win=65535 Len=0
	734 2013-10-07 11:51:03.424384 10.10.0.154		1991-1101-137-12884s	TLSv1	131 Client Hello
	762 2013-10-07 11:51:03.552735 10.10.0.154	OGS Test 1	193 110 137 188	TCP	54 4543 > https [ACK] Seg=78 Ack=1486 Win=65535 Len=0
	763 2013-10-07 11:51:03.553816 10.10.0.154		19302300582v188+	TLSv1	368 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Mes
	779 2013-10-07 11:51:03.747197 10.10.0.154		293142465232/28844	TLSv1	192 Application Data
	792 2013-10-07 11:51:03.874861 10.10.0.154		19371071377188	TCP	54 4543 > https [ACK] Seq=530 Ack=1850 win=65172 Len=0
	793 2013-10-07 11:51:03.876186 10.10.0.154		1034410-433-588:*	TCP	54 4543 > https [FIN, ACK] 5eq=530 Ack=1850 Win=65172 Len=0
	794 2013-10-07 11:51:03.877037 10.10.0.154		103-120-082/289-11	TCP	62 lanner-lm > https [5YN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
	809 2013-10-07 11:51:04.001356 10.10.0.154		101.110.110.188	TCP	54 lanner-lm > https [ACK] Seg=1 Ack=1 Win=65535 Len=0
	810 2013-10-07 11:51:04.001693 10.10.0.154		193:019:019:01988a	TLSv1	163 Client Hello
	827 2013-10-07 11:51:04.127077 10.10.0.154	OGS Test 2	\$95/636/837/2884×	TLSv1	101 Change Cipher Spec, Encrypted Handshake Message
	828 2013-10-07 11:51:04.129515 10.10.0.154		T997TT0:T927E08	TLSv1	192 Application Data
	844 2013-10-07 11:51:04.254843 10.10.0.154		193obb9ckBlockBlo	TCP	54 lanner-lm > https [ACK] Seg=295 Ack=444 Win=65093 Len=0
	845 2013-10-07 11:51:04.254860 10.10.0.154		193-0104-12-010-12-00-10-10-10-10-10-10-10-10-10-10-10-10-	TCP	54 lanner-lm > https [FIN, ACK] Seq=295 Ack=444 Win=65093 Len=0
	846 2013-10-07 11:51:04.255775 10.10.0.154		1997110:1927108	TCP	62 gds-adppiw-db > https [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_
	856 2013-10-07 11:51:04.382426 10.10.0.154		1981110:137:088=	TCP	54 gds-adppiw-db > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
	857 2013-10-07 11:51:04.382941 10.10.0.154		199 TYON SPIRES	TLSv1	163 Client Hello
	866 2013-10-07 11:51:04.510362 10.10.0.154	OGS Test 8	193.110.132.188	TLSv1	101 Change Cipher Spec, Encrypted Handshake Message
	867 2013-10-07 11:51:04.512581 10.10.0.154		1930230/258202884	TLSv1	192 Application Data
	895 2013-10-07 11:51:04.639659 10.10.0.154		193-1240-1237-1288-11	TCP	54 gds-adppiw-db > https [ACK] Seq=295 Ack=444 Win=65093 Len=0
	896 2013-10-07 11:51:04.640162 10.10.0.154		191.110.137.188	TCP	54 gds-adppiw-db > https [FIN, ACK] Seq=295 Ack=444 Win=65093 Len=0
_					

4. Om elk van de problemen makkelijker te identificeren, klikt u met de rechtermuisknop op het HTTP SYN voor de eerste sonde en vervolgens selecteert u Conversation Coloriseren zoals hier wordt getoond:



Herhaal dit proces voor SYNs op alle sondes. Zoals in de vorige afbeelding wordt getoond, worden de eerste twee spelden in verschillende kleuren weergegeven. Het voordeel van het coderen van de TCP-gesprekken is om gemakkelijk retransmissies of andere dergelijke eigenaardigheden per sonde te detecteren.

5. Als u de tijdweergave wilt wijzigen, navigeer dan naar Weergave > Weergave tijd > seconden sinds Epoch:

0 0 0 Vi 627494747,pcaping (Wireshark 1.6.2 (SVN Rev 38931 from /trunk-1.6))						
Elle Edit View Go Capture Analyze Statistics Telephony Tools Internals Help						
EX 84 8	< Main Toolbar					
	< Eilter Toolbar					
Filter: ip.	< Statusbar	pression Clear Apply				
No.	- Packet List	Yotocol Length Info	<u>.</u>			
677	< Packet Details	OP 62 4542 > https:[StN] Sep-0 M(n=65555 Lef-0 MSS-)460 SAO(99Me).				
689	- Packet Bytes	CP 54 dtg2 > https [4X] 99-1 4X-1 kinet555 [4010				
690	Time Dirolay Format	Mat Continuation Data Data				
708	Name Resolution	Time of Day: 010203 133656 0101010101010101010101010000				
710	< Colorize Packet List	Second Since Enech (1976-01-01): 1234567/800.123456 OrtHAR-43				
711	 ✓ Auto Scroll in Live Capture 	Seconds Since Reginning of Capture: 123.123456 Ctrl+At+4				
729		Seconds Since Previous Captured Packet: 1.123456 Ctrl+At+5				
720	Q Zoom In Ctrl++	Seconds Since Previous Displayed Packet: 1.123456 Ctrl+AR+6				
732	R 200m Qut Ctri+-	Automatic /City Encount Straticion	Ļ			
•	E Pasiza All Columns Solt - Orl-1	Second: 0))+			
D Frame 67	Displayed Columns	Deciserands: 0.1				
Enternet		Certiseconts: 0.12				
Fransmis	Expand Subtrees Shift+Right	Milliseconds: 0.123				
	Expand All Corrections	Microseconos: 0.123456				
	Compseign Complexity	Nanoseconds: 0.123456789				
	Colorize Conversation	Display Seconds with hours and minutes Ctrl+At+0				
	Reset Coloring 1–10 Ctrl+Space					
	Soloring Rules					
	Show Packet in New Window					
	Beload Ctri+i					
0010 00 30	45 00 0 fd 1d 40 00 90 06 00 00 0a 0a 00 9a c1 6e .	E-				
0020 94 bs 0030 ff ff	11 be 00 bb 9c 41 2c 96 00 00 00 00 70 02 . 665 00 00 00 02 04 05 54 01 01 04 02 .	P. f				
-						
Etherne	t (eth), 14 bytes P	ickets: 1538 Displayed: 61 Marked: 0 Load time: 0:10.992	Profile: Default			

Selecteer Milmilliseconden, omdat dit het precisieniveau is dat OGS gebruikt.

 Bereken het tijdsverschil tussen het HTTP-SYN en de FIN/ACK, zoals in het schema van Stap 4. Herhaal dit proces voor elk van de drie sondes en vergelijk de waarden met die in de DART-loggen in Stap 3.3.3.

Analyse

Als na de analyse van de opgenomen waarden de vastgestelde RTT-waarden worden berekend en vergeleken met de waarden in de DART-bestanden en alles op elkaar lijkt te afgestemd, maar het nog steeds lijkt of de verkeerde poort wordt geselecteerd, is dat te wijten aan een van de twee problemen:

- Er is een probleem op het hoogtepunt. Als dit het geval is, kan er te veel terugzending zijn van het ene specifieke head-end, of van enige andere eigenschap zoals gezien in de probes. Een nadere analyse van de uitwisseling is noodzakelijk.
- Er is een probleem met de Internet Service Provider (ISP). Als dat het geval is, kan er voor één bepaald kopstuk sprake zijn van fragmentatie of grote vertragingen.

Vraag en antwoord

V: Werkt OGS met taakverdeling?

A: Ja. OGS is alleen op de hoogte van de clustermaster name en gebruikt dat om het dichtstbijzijnde head-end te beoordelen.

V: Werkt OGS met de proxy-instellingen die in de browser zijn gedefinieerd?

A: OGS ondersteunt geen automatische proxy- of proxy Auto Config (PAC)-bestanden, maar

ondersteunt een harde proxy-server. Als zodanig gebeurt er geen OGS-operatie. Het relevante logbericht is: "OGS zal niet worden uitgevoerd omdat automatische proxy-detectie is ingesteld."