

ةيلخادلا ىودعلا ردصم ديدحت

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[DNS ريراقت لاسراب موقى يذلا يلخادلا DNS Server طاشن](#)

[ةيلاتلا تاوطخلا](#)

[Server 2016 جمانربل ةقباسلا ليغشتلا ةمظنأ تارابتعا](#)

[ةيفاضا تاراىخ](#)

ةمدقملا

Cisco Umbrella ي ف ةيلخادلا ةباصإلا ردصم ديدحت ةيفي ك دنتسملا اذه حضوي

ةيساسألا تابلطتملا

تابلطتملا

دنتسملا اذهل ةصاخ تابلطتم دجوت ال

ةمدختسملا تانوكملا

Cisco Umbrella ىلا دنتسملا اذه ي ف ةدراولا تامولعمل دنتست

ةصاخ ةيلمعم ةئيب ي ف ةدوجوملا ةزهجألا نم دنتسملا اذه ي ف ةدراولا تامولعمل عاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دنتسملا اذه ي ف ةمدختسملا ةزهجألا عيمج تأدب رما يأل لمحتملل ريثأتلل كمهف نم دكأتف ،ليغشتلا دي ق ك تكبش

DNS ريراقت لاسراب موقى يذلا يلخادلا DNS Server طاشن

اهدي دحت مت ي تلل رورملا ةكرح وأ ،ةعقوتملل ريغ رورملا ةكرح نم ةريبك ةيمك ىرت تنك اذا ةصاخلا عقاوملا وأ ك تكبش ىدحإ دض اهليجست مت يتلاو تب ةكبش/راض جمانرب ةطساوب هنأل ارظن .يلخاد فيضم ةباصإ ري بك لكشب لمحتملل نم ف ،"ةلظملا تامولعم ةحول" ي ف ك ب IP ب بلطلل ردصملا IP لادبتسإ متي ،يلخاد DNS مداخل ربع DNS تابلط رمت نأ لمحتملل نم ةيماح رادج بقعت بعصلل نم لعجي امم DNS مداخل صاخلا

دي دحتل Umbrella تامولعم ةحول مادختساب عيش أب مايقلا كنكمي الف ،لاحلا وه اذه ناك اذا ةكبشلا ةي وه لباقم تابلطلل عيمج ليجست نكمي .ردصملا

ةيلاتلا تاوطخلا

اهنكمي ىرخأ نامأ تاجتنم ياً نودب نكلو، اهب مايقلال كنكمي يتلا عايشالال نم ليلق ددع كانه DNS مداخلىل عةدوجوملالتا جسلال مادختسا وه يساسالال رمالال ناف، كل كولسلال اذه بقعت ردمال فالتا م، تابللالتا يأت نيأ نم ةفرعمل.

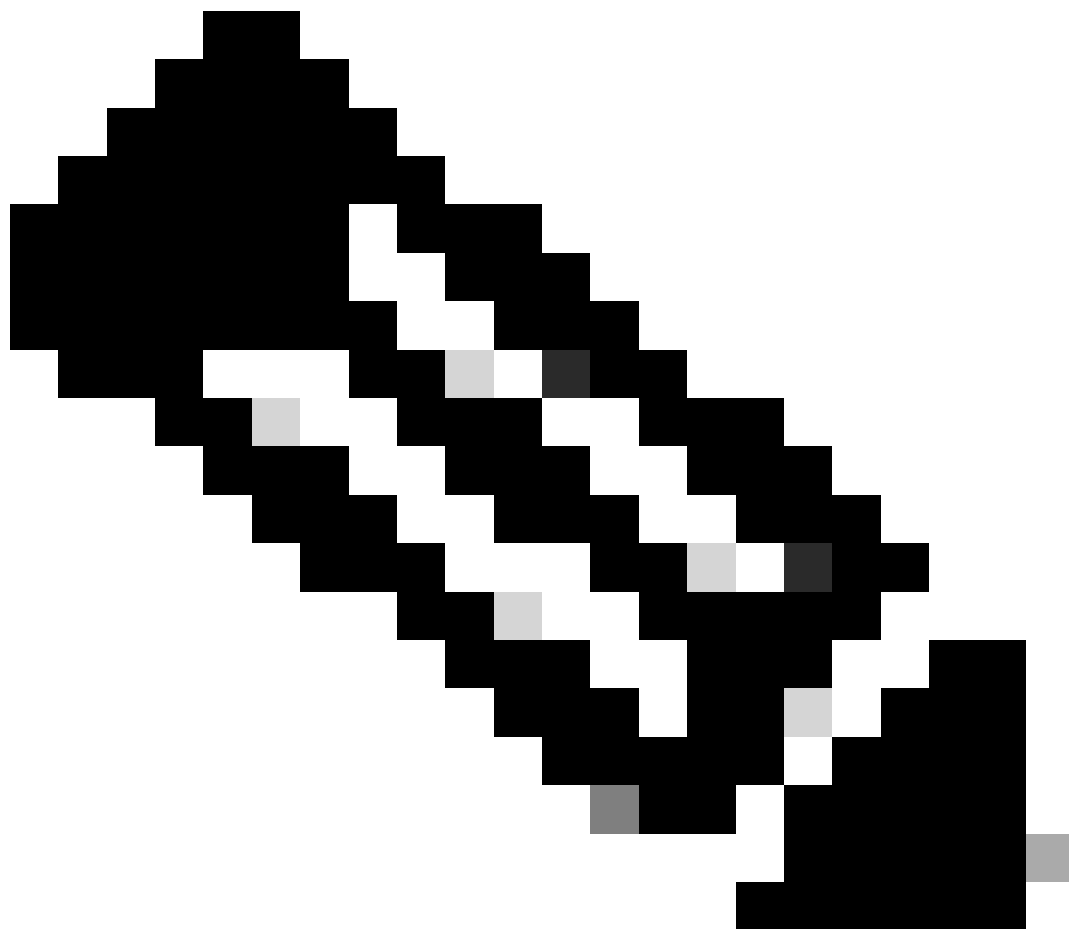
ىوتسم ىل ع [في فور](#) ي طعي نأ نكمي يذلا (VA) يرهظلال زاهجلال ليغشتب ةداع Umbrella ي صوت نم عونلال اذه ةعرسب نيغيو ةيلخادلل ةكبشلال ىل ع DNS رورم ةكرح عيمل ف يضلالم ةلكشمل.

ال يذلا يلخادلل فيضملال اهي ف ضرعتي يتلا لكاشملال انايحأ "Umbrella معد" ددحي، كلذ عمو نم ال دب Windows DNS مداخلال نم DNS تابللط لسريو ةباصلال VAs ىل DNS ىل ريشي DNS بلط VA ىرت نأل ةقيرط دجوت ال هنأ ويرانيسلال اذه ي ف حضاولال نم هنأل. كلذ ربع رمت يتلا DNS تامالعتسا عيمل لي جست نكمي، (هب صاخلال ردمال IP ناوئع يلاتلابو) عقومال وأ ةكبشلال لباقم DNS مداخل.

Server 2016 جمانربل ةقباسلال ليغشتلال ةمظنأ تارابتعا

تامولعملال هذه لي جست متي ال، Server 2016 ل ةقباسلال ليغشتلال ةمظنأ ي ف، كلذ عمو لكشب. تانايبلال طاقتلال نم نكمتت ىتح ايودي اهنكمت ىل جاتحت. يضارتفا لكشب اذه ىل ع لوصلل [Microsoft نم لجاعلال حالصالا](#) تي بثت كنكمي، 2012r2 ل ةبسنلاب، صاخ كل رفوتمال لي جستلال نم ىوتسمال.

لي جست لي جست دادعإ لوح تامولعملال نم ديزملو، ىرخالال ليغشتلال ةمظنأل ةبسنلاب تارايلال ىل ع ةماع ةرطن هذه [Microsoft ةلاقم](#) ي طعت، DNS مداخلىل ع ءاطخالل حيحصت مادختسالالو.



ەي فاضل تاراڭ

(192.168.168.129) لي م عمل DNS م داخ ىل ع اذه طاقت لال لي غشت ره ظي ، لاثم ل لې بس ىل ع اراج اب DNS م داخ موق ي م ث ، (192.168.168.228) DNS م داخ ىل ب لطل ا اراج اب موق ي ذل اذه م دخ وة باجت س ا ىل ع ل و ص ح ل او ، (208.67.222.222) Umbrella AnyCast م داو خ ىل م ا ل ع ت س ا ل ل . م عمل ىل ىر خ ا ق ر م

لېږلې اذه نم ائىش نوکىس حشرملا حارتقا

dns.gry.name contains examplebotnetdomain

dns.qry.name eq "examplebotnetdomain.com"

Capturing from Ethernet0							
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help							
dns.qry.name eq *examplebotnetdomain.com*							
No.	Time	Source	Destination	Protocol	Length	Info	
149	7.603774	192.168.168.129	192.168.168.228	DNS	83	Standard query 0x0009 A examplebotnetdomain.com	
150	7.604031	192.168.168.228	208.67.222.222	DNS	94	Standard query 0x4839 A examplebotnetdomain.com OPT	
151	7.604776	208.67.222.222	192.168.168.228	DNS	110	Standard query response 0x4839 A examplebotnetdomain.com A 67.215...	
152	7.605110	192.168.168.228	192.168.168.129	DNS	99	Standard query response 0x0009 A examplebotnetdomain.com A 67.215...	
153	7.606018	192.168.168.129	192.168.168.228	DNS	83	Standard query 0x000a AAAA examplebotnetdomain.com	
154	7.606153	192.168.168.228	192.168.168.129	DNS	144	Standard query response 0x000a AAAA examplebotnetdomain.com SOA au...	

exampleBotnetdomain.png

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا