

نمضت يتلا Umbrella ةسايس دي دحت مهف ةددعت م تاسسؤم

تايوت حمل

[ةمدقملا](#)

[ةماع قرطن](#)

[ةدحاو ةسسؤم لالخ نم جهنلا دي دحت](#)

[ةددعت م تاسسؤم عم ةسايسلا دي دحت](#)

[ةددعت م تاسسؤم عم غالبلا](#)

[يلاحلا ةسايسلا رايخا كولس يلغ ةبترت ملا راثلا](#)

[ةددعت م تاسسؤم نمضت يتلا تاهوي راني سلال ةصصخم تاعومجم تاحفص](#)

[ةددعت م تاسسؤم نمضت يتلا ةسايسلا رايخا ةططخملا تاريي غتلا](#)

[ةسايسلا دي دحت كولس](#)

[ةكراش ملا تامظن ملا عي مج يلا ريراقتلا مي دقت](#)

ةمدقملا

يف اهيف رظنلا يرجي يتلا ةددعت ملا ةلظملا تامظنم تاسايس ةقيثولا هذه فرصت
ةني عم تاهوي راني س.

ةماع قرطن

كلذ يلغ لاثم .ةددعت م ةعماج تامظنم تاسايس يف رظنلا نكمي ،تاهوي راني سلا ضعب يفو
هذه حضوت .يرخا ةسسؤم ةكبش ةلصت م ةدحاو ةسسؤم لومحم زاهج وأ لاوحتلا ليمع وه
يونت يتلا تاريي غتلا يه امو ،ةلاحلا هذه يف ايلاح ةسايسلا رايخا ةيفي ةلاقملا
كولسلا اذه نيسحتل اهؤارج Umbrella.

ةدحاو ةسسؤم لالخ نم جهنلا دي دحت

مالعتسالااب ةددعت م تايوه نرتقت نأ نكمملا نم ،Umbrella يلا DNS مالعتسا لاسرا دنع
فرعم ةيمحم ةكبش فلخ (RC) لوچتم ليمع نم مالعتسالا نمضتي دق ،لاثملا لابس يلغ
فرعم يرهاظ زاهج نم مالعتسا نمضتي ،لثامم وحن يلغو .ةكبشلل IP ناونع كلذك و RC زاهج
AD ةعومجم و AD مدختسمو ةيلخادلا ةكبشل او عقوملا .

نإف ،ةلاحلا هذه يف .ةدحاو ةسسؤم ةطبترم مالعتسالا يف ةنمضت ملا تايوهلا نوكت ،ةداع
انقئاثو يف ةلصفملا ةسايسلا ةيقبسأ دعاوق مدختست اهضرف متي يتلا ةسايسلا

<https://docs.umbrella.com/deployment-umbrella/docs/policy-precedence>

عم ،تامولعمل ءحول يف اهبيترت يلا اذانتسا ةيولوا ةسايس لك Umbrella نيغت ،راصتخابو
يلغ قبطني يذلا يلغالا ةيولوالا جهن Umbrella وللحم راتخي .جهنلل ايلعلا ةيولوالا ءاطعا

للقال إلى عل مالعتسال في ءءوءومل اايلول.

A: ءسسؤمل لاسالسل هءه فيرعت مءل ءق، لاللم ليلسل عل

Subscription Properties - Login Events

Subscription name:

Login Events

Description:

Destination log:

Forwarded Events

Subscription type and source computers

☒ Collector initiated

Select Computers...

This computer contacts the selected source computers and provides the subscription.

☐ Source computer initiated

Select Computer Groups...

Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

Events to collect:

Select Events...

User account (the selected account must have read access to the source logs):

Machine Account

Change user account or configure advanced settings:

Advanced...

OK

Cancel

mceclip0.png

ءاا اءا، لالءل 1. ءيلولأ هل ءكبشلل ءهن امنيل 2، ءيلولأ هل لولءلم رلويلبمكلل ءهن، لالءل ءم و 2. ءهنلل قيببلم مءل سف، ءلءراخ ءكبش بلمبلم لولءلم رلويلبمكلل نم مالعللسال ءهنلل قيببلم مءل سف، A ءسسؤمل لالءبش لءل لولءلم رلويلبمكلل مامضلنا مل اءا لعلأ ءيلولأ هل ءكبشلل ءهن نأ شلء، 1.

ءءءلم لاسالسل ءم ءسالسل لءلءل

فيل ءنمضللم ءءءلم لاملظنم نم لالولل ءلءل نوكلم ءءنل قطنلمل اءه سفن قيببلم مءل لال ءلبسلل ءيلولأ نل ف، ءلءنم ءءءلم لاملظنم ءول ارظن، لالءل ءم و. مالعللسال ءسسؤمل لك لاسالسل ءمئللق لعلءل مفل رابلل ءلءل ءمئل ءسالسل.

هءه لعل (ب) ءسسؤملل و (أ) ءسسؤملل نم لك لمءشءل. لصفل وءن لعل لالءل ءضول لاللم ءمءل و

امهوب ةصاخلا ةلظملا ب ةصاخلا تامولعمل تاحول يف ةددحمل تاسايسلا

- **Minimize Latency**

- Makes sure that events are delivered by having minimal delay.
- The appropriate choice if you collect alerts or critical events.
- Uses push delivery mode, and sets a batch time-out of 30 seconds.

mceclip2.png

B. ةسسؤملا ىلإ يمتنت ةكبش ىلإ كلذ دعب A ةسسؤملا نم لوجتم رتويبمك مضمني A'RC زاهج فرعم ىلإ Umbrella ىلإ هلاسرا مت يذلا DNS مالعئسا يوتحي يلاتلابو ةسسؤملا B ةكبش ل IP ناونعو ةسسؤملا.

ةيوه لك ةسايسب ةصاخلا تايولوالا ىلإ لصحن، ةدحاو ةمظنمب صاخلا قطنملا مادختساب ةكبشلا لصحت امنيب، 2 ةيولوا هل يتلاو، A2 ةسايسلا ىلإ A ةسسؤملا نم RC لصحي ةسايس قيبطت متي، يلاتلابو 1. ةيولوا هل يتلاو، B1 ةسايسلا ىلإ B ةسسؤملا نم B1 ةسايسلا، B ةسسؤملا ةكبش.

ةددعتم تاسسؤم عم غالبإلا

يف طقف مالعئسالا رهظي، ةددعتم تاسسؤم نم تايوه ىلإ مالعئسالا يوتحي ام دنع ةمظنملا كلت ريراقت ضرعت. اهتسايس ديدحت مت يتلا ةسسؤملا ب ةصاخلا ريراقتلا ىلإ تايوهلا يف ةيؤر ةيناكم ةسسؤملا سئل. طقف ةمظنملا كلب ةصاخلا تايوهلا ىلإ تاسسؤم ىلإ يمتنت يتلا مالعئسالا يف.

يلالحا ةسايسلا رايتخا كولس ىلإ ةبترتملا راثآلا

ةيوه ىرخأ ةمظنم ةسايس ىغلث نأ نكمملا نم، فوصوملا ةسايسلا رايتخا كولسل ارظنو يوتحمل رطحو نامألا كلذ يف امب، جهنلا تازيم ةفاك كلذ نمضتي. ةدحاو ةمظنم ىلإ يمتنت ىلإ ةضورفملا دويقلا ةطحال (ليجستلا تاداعإو رطخلا تاحفص ميماصتو ةهجول مئاوقو رطخلا ءحفص هيجوت ةداعإ تايلمع ءانثتساب، (ريراقتلا دادعإ).

ةددعتم تاسسؤم نمضتت يتلا تاهوي رانيسلل ةصصخم تاعومجم تاحفص

ىلإ يوتحي مالعئسالا نأ Umbrella وللم فشكتي ام دنع، 2021 زومت/ويلوي 16 نم ارباعا لتك ءحفص ىلإ ةروطحم تامالعئسا يأ هيجوت ديعي هنإف، ةددعتم تاسسؤم نم تايوه ةسسؤم نم رثكأ فاشتكأ مت هنأب مدختسملا مالعاب هذه رطخلا ءحفص موقت. ةصصخم ىلإ ةسسؤم جهن ببسب مالعئسالا رطخ مت نوكتي دق يلاتلابو، ةدحاو

نمضتت يتلا ةسايسلا رايتخال ةططخملا تاريغيغثلا ةددعتم تاسسؤم

ةدحاو ةمظنم نم رثكأ ءكراشم دنع ةسايسلا رايتخا كولس ريغيغت ىلإ Umbrella لمعت

ييلي ام ةيلبقتسملا تارييغتلا نمضتتو

ةسايسلا ديدحت كولس

ايلعللا ةيولوالا ةسايس ديدحت متي شح ب ةسايسلا ديدحت كولس ليديعتب Umbrella موقت رطح متي ،مالعتسال رطح جهنلا هذه نم ي ا مايق ةلاح ي ف ،م ث .اهذافن او ةسسؤم لكل نكميو .اهتاسايس زواجت مدع نامضب ةينعمل تامظنملا عيملج حمسي اذهو .مالعتسال سايقلا مادختساب وحن لصف اىلع كولسلا اذه ريسفت

نأ سيلأل اهومسم سيل .تيبلل دعاوق نم ةيمهأ رثكأ ةيدرفلا دعاوقلا نأ سيلأل ادلاو لوقي ناكم ي ا يفو تقو ي ا ي ف ،تاجلثمل لكأت

لوخدب نوحمسي ال .ةيدرفلا نيناوقلا نم ةيمهأ رثكأ لزنملا نيناوق نأ بوب ادلاو لوقي ادبأ مهلزنم لىل ا زتيبلل

يلاحلا جذوملل

سيلأل .ةيدرفلا سلأل دعاوق سيلو بوب تي ب دعاوق قبطت .بوب تي ب لىل ا بهذت سيلأل نأ لوقي ريرقت لىلع الصح بوب ي دلاو .ازتيبلل سيل نكلو ،تاجلثمل لكأت نأ عيطتست .مسالاب سيلأل ناك هنا لوقي ال نكل ،مهلزنم ي ف تاجلثمل لكأ مهذخ

حرتقملا جذوملل

سيلأل .قبطت ةيدرفلا سيلأل نيناوق و ،بوب تي ب دعاوق قبطت .بوب تي ب لىل ا بهذت سيلأل نم هنامرح مت مهذخ نأ لوقي ريرقت لىلع الصح بوب ي دلاو .ازتي ب وأ ميرك سي ا اهي دل سيل .مسالاب سيلأل ناك هنا لوقي ال نكلو ،ميرك سي ا لىل ا او ازتيبلل

ةكراشملا تامظنملا عيملج لىل ا ريراقتلا مديقت

ي ا چاردإ كلذ لىل ا ةفاضل Umbrella لفكت ،امئاق تاسايسلا رايتخا كولس نوكي امدنعو .ةينعمل تامظنملا عيملج ريراقت ي ف ةددعتم تامظنم نم تايوه نمضتت تاراسفتسا ىرت ال ةينعمل ةمظنملاف - ةمظنملا كلت لىل ا يمتنت تايوه طقف نمضتت ريراقتلاف ىرخأ ةمظنم تايوه ادبأ

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