

عم Umbrella Log تالچسل ةيزكرملا ةرادإلا مهف و MSSP و MSP ءالمعل Amazon نم S3 ةمدخ Multi-org

تايوتحمل

[ةمدقملا](#)

[ةماع ةرظن](#)

[قلظملا لچسل ةرادلا نم ناعون](#)

[ءدبللا يف عورشلا](#)

[ةرادالا يثاذا S3 ولد نيوكت](#)

[ةيساسلا تابلاطتلا](#)

[Amazon S3 ولد دادعا](#)

[Amazon S3 ولد نم ققچتلا](#)

[لچسلا قاىح ةرود ةرادا](#)

[Cisco نم رادمل S3 عدوت سم نيوكت](#)

[رشنلا ةدام نيوكت تاراىخ](#)

[لچسلا ليمحت لشف](#)

[قيسنتلا واهلي ممت يتلا تالچسلا نم ققچتلا](#)

[ليمعل لكل لوخذلا لچست نيوكت](#)

[Splunk / QRadar لمكت وقيسنتلا ىلع فرعتلا، تالچسلا ليزنت](#)

[S3؟ تالچس مچحام](#)

ةمدقملا

و MSP ءالمعل Amazon نم S3 ةمدخ عم Umbrella لچسل ةيزكرملا ةرادإلا دنتسملا اذه فصى
MSSP و Multi-org.

ةماع ةرظن

ةصاخلا IP تالچسو URL و DNS نيزخت Multi-org و MSSP و MSP يف مكحتلا تادحول نكمي
دعبو Amazon S3 يف دوجوم نيزختلا. تاكبشلا ىلع نيزختلا تادحو يف لاصتا نود كئالمع ب
نامألا ليلحتل وأ قفاوتلاب قلعتت بابسأل اهظفحو اهليزنت نكمي، تالچسلا ليمحت

ةدحوو Umbrella تامولعمل احوول نم لك يف اهدادعاو، ةزيملا هذه مهف ىلع قئاثولا هذه كدعاست
يذلا تقولا ةدم كلذ يف امب، نيوكتلا تاراىخ نم ديدعلا ربع اهليغشتو، Amazon S3 مكحتلا
S3. يف هي ف تالچسلا بظافتحالا يف بغرت

ةكرح ةطشنأ تالچس ليمحت ىلع ةردقلا عيمج Multi-Org و MSSP و MSP ل Umbrella كلت مت

ةبألسلا فف ءالأسلا هذف نفلزءو مءءءلأ ءءول ءءبائلأ ءاسسؤملا نم رورملا راشفو؁ ءالأسلا ءفشرا مؤقء فءلأ ءمءلأ فف (طفسبلا نفلزءلأ ءمءلأ) AmazonAWS S3 فف. IS islog retention وأ لصلءملا رفف STORAGE ءف مساب انافأ اءفلا

ضعبل ءبسنلاب .كءاففءلأ بسء؁ بابسا ءءل ءففم ءفشرا ءالأس نوكء نأ نكمف لفلءء ءاوا ءلأ اءفشرا وأ اءرفءصلء مء فءلأ ءالأسلا ءارفءسا نكمف؁ صاأشالأ نوكف نأ نكمف؁ نفلزءلأ ءبسنلابو. SIEMs لءم؁ ففءرشلأ بطلل نامالأ ءاوا وأ ءانافلأ وأ فف نامأ ءءا ءووقو ءلاف فف ءانافلأ بطلل ففءرشلأ بطلل اءففم ءطشنالأ ءالأس فففشرا ءففءرشلأ ءراوملا ءالأس.

مءف هنال ارطن .CSV قفسسناءب (gzip) طوؤضم ففشرا فف ءالأسلا نفلزءب AWS S3 مؤقف رورم ءكرء نفل قفءاقء رشف ءءمل رففءا ءنءا كانف نوكف؁ قفءاقء رشف لك ءالأسلا لفلءءء ءااء مء .Umbrella ءطساوب اءلففءسء مءف فءلأ؁ كفلء ءكبشلأ نم ءمءاقلا ءكبشلأ S3 نم لفلزنءلل

مءءءلأ ءءو نم orgID مقرر

مقرر مااءءسااب؁ فءرف لكشب اءالأس لفلءءب ءالمءلأ ءاسسؤم نم ءسسؤم لك مؤقء اءلفطءء وأ ءزفملا نفلءمء نكمف امك .ءلءم ءلأ لفلءم لك نفلففءل مءءلأ ءءو نم orgID ءسسؤم لكلك / لفلءم لكلك

ءلظملا لأس ءراءا نم ناعون

ءلءم اساسأ) isbuctit وه فمسف ام ءلأ ءالأسلا لفلءء قفرط نع لأسلا ءراءا ذففنا مءف :كب ءصاألأ Umbrella ءالأسل ولء ءفاصلءسا ل نااءقفرط كانف .(AWS ISS S3 ءففب لءا

- ءكرفللأ لوؤسم؁ ءنأ كلبق نم هنمء ءفو ءراءا وهءراءا مءء
- Cisco Umbrella ءطساوب هنمء ءفو ءراءا وهءراءا مءء

كب صاألأ S3 ولء رفءء Cisco لءل ءافبلسو ءافبأفلا كانف

:كبءبفقلأ Cisco ءراءا ءازفم

- نم ءبصف كلء ءعبو طقف قفءاقء ءضب رمالأ قرفءسف .ءاءءلأ فف ءقئاف ءلوهس هءراءا ءفألل لهسلأ
- لءلءف امم؁ Umbrella عم كب ءصاألأ صففءرءلأ ءفلءف فف Cisco ولء ءراءا نفلمصلء مءف ءفللكلأ ف؁ ممئالم رفف كب صاأ ولء كالءما نا نفل ءفو .لءاف لكشب ءفنأم ءمءلأ اءل ءظهاب نوكء نا نكمف ففءلأ ءرءاف ءراءل ءفللمألأ

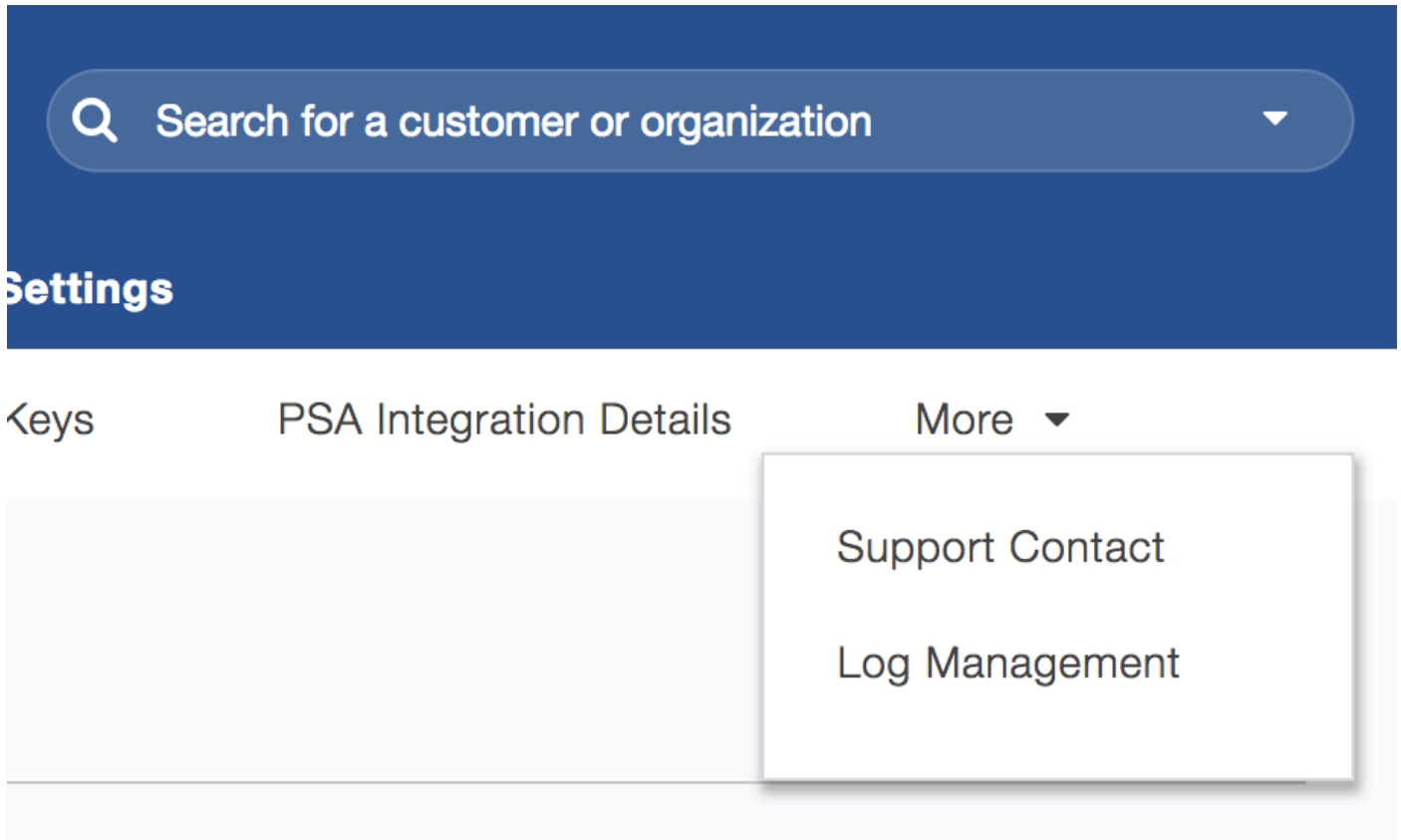
:كسفناب S3 لفلءم ءراءا ءافبأفلا

- نفلزءلأ Cisco ءءء .لأصلءا نوء ءانافلأ نفلزء اءف نكمف فءلأ ءءملل ءل ءلوفف ال ففصقأ ءلأ اموف 30 ب لأصلءا نوء
- Umbrella نم لأسلأ ءافللم كلذف فف امب؁ كب صاألأ ولءلأ ءلأ ءفففأ ءفاصلأ كنكمف ففصفأ ففءلأ ءطساوب ولءلأ مااءءسا نكمف ءففء
- فف ءءءاسم ءلأ لوصءلل Amazon ءقوم نم ءرשאبم مءءلأ ءلأ لوصءلل كنكمف رطس مااءءسااب ءءءاسملا وأ ففءاقلللأ لفلءشءلأ لءم؁ ءمءقءملا نفلوكءلأ ءافلمء رمالأ

نوكت دق اهنكلو، ةيغلل ةضفخنم ولدلا ةنايص ةفلكت إف، ءالمعل مظم ىل ةبسنباب ةقاش.

ءدبل ي ف عورشلا

كنكمي) لچسلا ةرادا > تادادعل نمض مكحتلا ةدحو ي ف "لچسلا ةرادا" ةزيم ىل ع روثعل كنكمي (لدسنملا مهسلا ىل ع طغضلا).



115012963103

ةرادلا ي تاذا S3 ولد نيوكت

ةيساسالا تابلطتملا

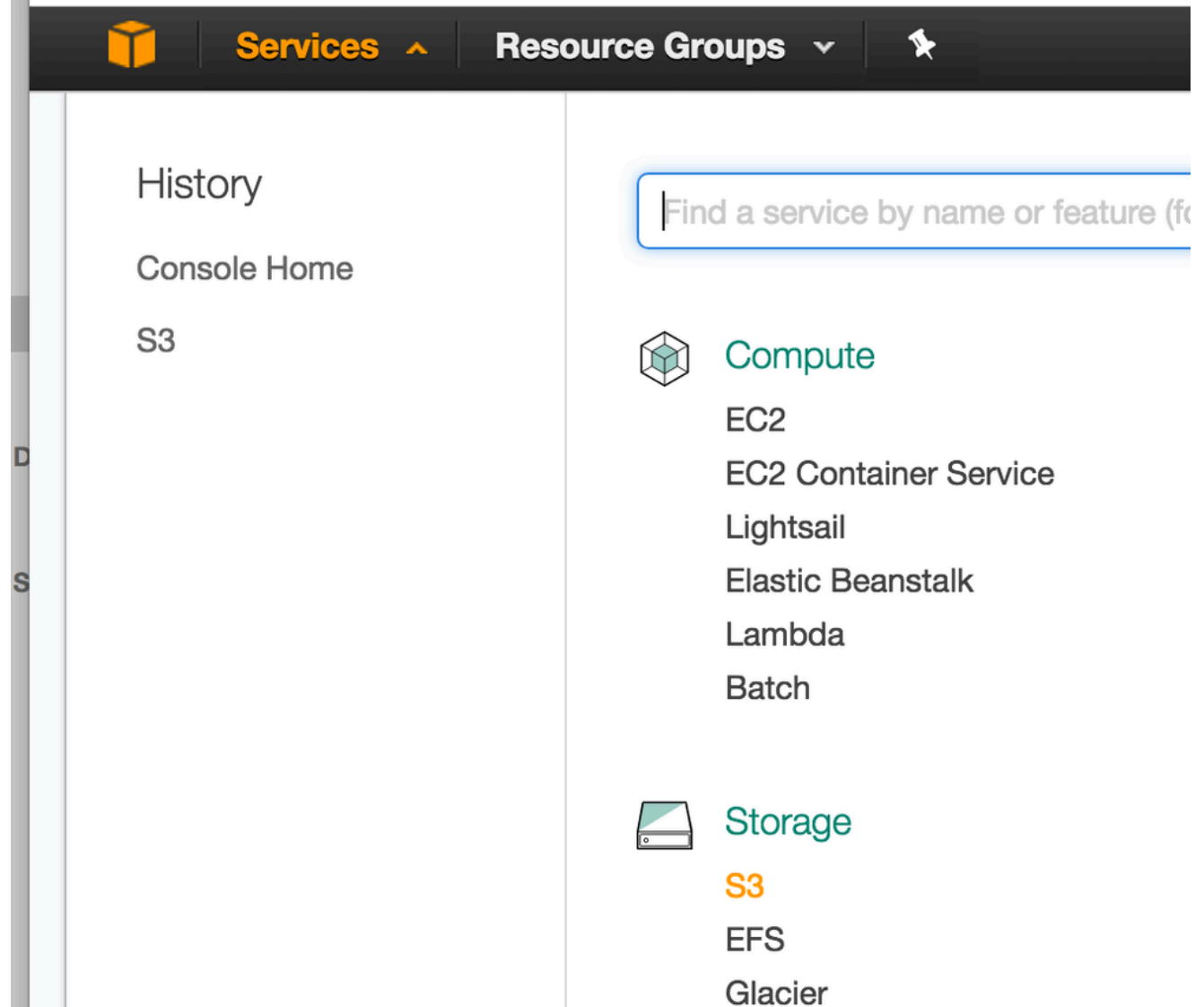
ببلطتم اذه تي فو تسايغبني تنأ، لچس ةفشرا in order to

- تاسسؤملا ةددعتم مكحتلا ةدحو وأ MSSP وأ Cisco Umbrella MSP ىل لماك يرادا لوصو.
- ديرت تنك اذا (<https://aws.amazon.com/console/>) Amazon AWS ةمدخ ىل لوخد ليچست ببلطت اهنإف، كلذ عمو. S3 ل ينام ل وخذ ليچست Amazon رفوت، باسح ىل ع لوصحلل ةطخلل ينام لامادختسالا مادختسالا زواجت لاح ي ف نامتئا ةقاطب ىل ع لوصحلل يلاتلا مسقلا عجار. تالچسلا نيختل Amazon S3 ي ف أيهم ولد Amazon. نم S3 ولد دادعإو نيوكت لوح تاميلعت

Amazon S3 ولد دادعإ

1. تحت ةدوجوملا تاراخيلا ةمئاق نم "S3 ديحتو، [AWS مكحت ةدحو](#) ىل لوخدلا ليچستب ادبا.

نيزختال.



115012842106

2. Amazon طيسبلا نيزختال ماظن في كب بحرت ةمدقم ةشاش ةدهاشم كنكمي

3. ولد عاشن رقا. ولد عاشن ديتر تنأف، لعفلااب ولد كي دل نكي مل اذا، كلذ دعب



Amazon S3



Search for buckets

+ Create bucket

Dele

115012842326

4. عدوتسم مسا لاخداپ أدبا .

ةلظمال وأكب صاخال AWS ل طقف سيل - هعون نم اديرف ولدلا مسا نوكي نأ بجي
لثم ،يصخش عيش مادختساف Amazon في AWS لكل نكلو ،كب ةصاخال
ديرفال ولدلا مسا بلطم يطخت ىلع مكدعاسي نا نكمي "My-Organization-name-log-bucket"
تافاسم ىلع يوتحي نأ نكمي الو طقف ةريغص فرحأ ولدلا مسا مدختسي نأ بجي .امومع
دويق لوح تامولعمل نم ديزمل .DNS ةيمست تايقافاتال لثتم نأ بجي و ،تارتف وأ
[انه](#) أرقا ،ةيمستال كلذ في امب ،ولدلا عاشنإ لوح تامولعمل نم ديزمل .[انه](#) أرقا ،عامسألا

Create bucket

1

Name and region

2

Set properties

3

Set permissions

4

Review

Name and region

Bucket name 1

my-msp-organization-name-log-bucket

Region

US West (N. California) ▼

Copy settings from an existing bucket

Select bucket (optional)

2 Buckets ▼

Create

Cancel

Next

115013010503

- تادادعإلأخسنمدع.عاشنإقوفرقناوكعقومللضفألكشبلمعتيتلاةقطنملاددح.
رخأولدنم
- اقحالرضانعالهذهليدعتنكمي.يلالاتلقوفرقنا،"صئاصخالنييت"ةوطخلإي
- اقحالنانوذألاةعجارمةداعإبموقنس.يلالاتلقوفرقنا،"نانوذأالنييت"ةوطخلإي
هليمحتلولدلدادعإل
- ولدعاشنإقوفرقناوةعجارملةيلمعءاهنإ.

Create bucket

✓ Name and region

✓ Set properties

✓ Set permissions

4 Review

Name and region

Bucket name

my-msp-organization-name-log-bucket-2

Region

US West (N. California)

Edit

Properties

Versioning

Disabled

Logging

Disabled

Tagging

0 Tags

Edit

Permissions

Users

1

Public permissions

Disabled

System permissions

Disabled

Edit

Previous

Create bucket

115012842686

9. في S3، Umbrella ممدخ نم لي محتات ايل لمع لوبقل ولدل نيوكت الى جاتحت، كلذ دع ب. ددح م ث اتي دح هنيوكت مت يذل عدوتسم الم مسا قوف رقنا. ولد ةسايسك اذه الى راشي ةهجاوالا الى عأ في نوذا بيوبتلا ةمالع

Amazon S3

> my-msp-organization-name-log-bucket

Overview

Properties

Permissions

Management

Q

Type a prefix and press Enter to search. Press ESC to clear.

115012842906

10. عدوتسملا يف قصللاب كتبلاطم متت مٹ Bucket جهن ددح

Access Control List

Bucket Policy

CORS configuration

Bucket policy editor ARN: arn:aws:s3::my-msp-organization-name-log-bucket

Type to add a new policy or edit an existing policy in the text area below.

```
1 {
2   "Version": "2008-10-17",
3   "Statement": [
4     {
5       "Sid": "",
6       "Effect": "Allow",
7       "Principal": {
8         "AWS": "arn:aws:iam::568526795995:user/logs"
9       },
10      "Action": "s3:PutObject"
```

115012843006

11. وأصوصن ررحم ىلإ، ولدلا جهن ىلع يوتحت يتلاو، اهقصلو هاندأ JSON ةلسلس خسنأ. ديدحت متي شيح ددحمل ولدلا مسالادبتسإ. ةذفانلا يف ةطاسبب اهقصلب مق أطخ ةلسر روهظ ىلإ كلذب مايقلا يف لشفلا يدي. هاندأ BucketName

```
{
  "رادصإلا": "2008-10-17",
  "نايب": [
    {
      "ديس": "",
      "ريثأتلا": "حامسلا",
      "ريدملا": {
        "AWS": "arn:aws:iam::568526795995:user/log"
      },
      "لمعلا": "s3:PutObject",
      "دروملا": "arn:aws:s3::bucketname/*"
    },
    {
      "ديس": "",
      "ريثأتلا": "ضفر",
      "ريدملا": {
        "AWS": "arn:aws:iam::568526795995:user/log"
      },
      "لمعلا": "s3:GetObject",
      "دروملا": "arn:aws:s3::bucketname/*"
    }
  ],
  "ريدملا": {
    "AWS": "arn:aws:iam::568526795995:user/log"
  }
}
```



```

،
"لمعلا": "S3:GetBucketLocation"،
"لروملا": "arn:aws:s3:::bucketname"
}،

{
"س": ""،
"لثألا": "لحامل"،
"لرلما": {
"AWS": "arn:aws:iam::568526795995:user/log"
}،
"لمعلا": "S3:ListBucket"،
"لروملا": "arn:aws:s3:::bucketname"
}
]
}

```

لرلغلل اذله لثألا "لفل قوف رلنا 12.

Amazon S3 ولد نم ققحتلا

1: ةوطخل

1. لجلسلا ةرادا > تادادعلا لىل لقتناو Umbrella Console مكلحتلا ةدحو لىل عجرا
2. ةذفانل علسوتل "Amazon S3" قوف رلنا
3. رلناو S3 ف هتأشنأ لذل عدوتسملا مسال قصلأ وأ بلكا، "عدوتسملا مسا" لقل ف ةحصل نم ققحتلا قوف عدوتسملا نم ققحتلا مت هنأ لىل لرلشت كتامولعم ةحول ف لثألا ةلاسرى ققلت حاجنب

Log Management

Amazon S3

STATUS

LAST SYNC

☒ Not Configured

Never

AWS S3 Bucket

my-msp-organization-name-log-bucket

VERIFY

✓ Verification Successful

For security, we need to confirm that we're sending logs to your bucket. Navigate to your AWS account, copy your unique token from the README file from your bucket, paste it below, and click save.

Unique Token

CANCEL

SAVE

115012847146

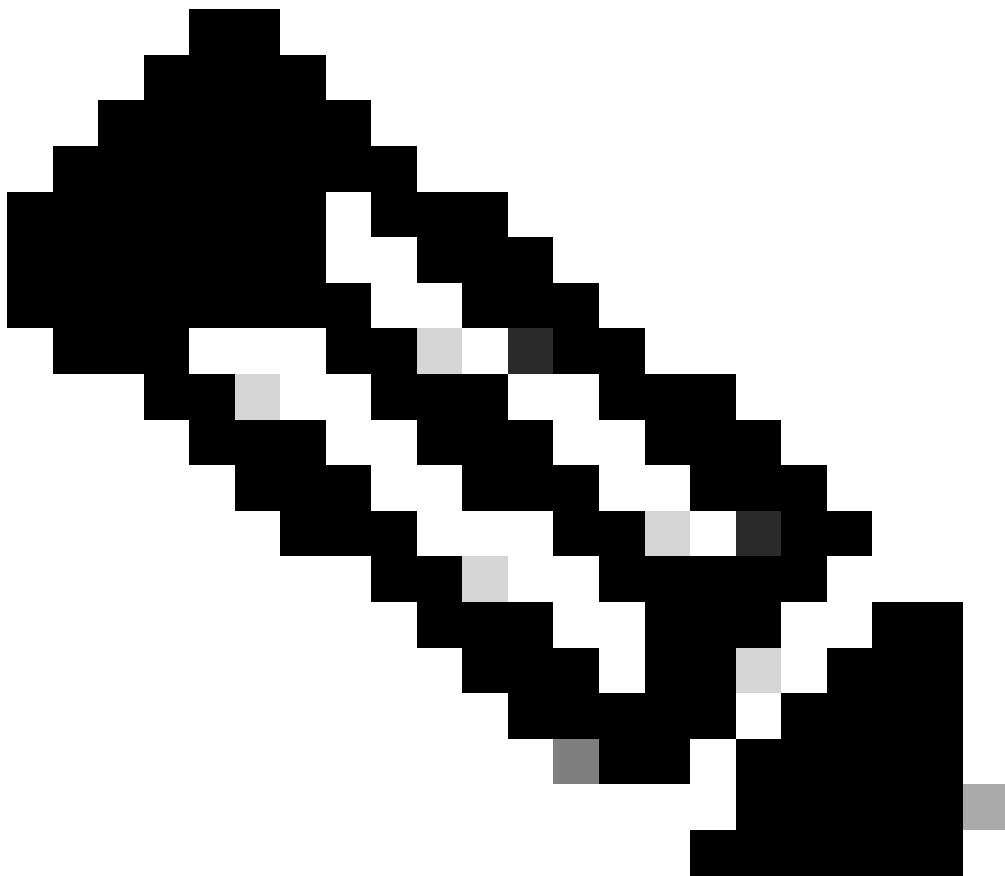
ةلمج ءانب نم ققحتلا دءاف، كب صاخلا ولد نم ققحتلا رذعت هنأ لىل لرلش لءط تىقلت اذلا عباتلا معدلا مسق لءلا لءل ءل ف لءل، تالكلشمل ترمتسا اذلا. نلوكلا عجارو ولءلا مسا

انل

2: ةوطخال

طيشنت زمر لاخل Umbrella بطلت ،ححصلا ولدلا ديدحت نامضل يوناث يطايتح اءاركا نم ءزكا S3 ولد ةرايز ةءاع لالخال نم طيشنتلل زيمملا زمرلا ىلع لوصحلا نكمي .ديرف نم README_FROM_UMBRELLA.txt مساب فلم ليمحت مت ،ءحصلا نم ققحتلا ةيلمع .كانه رهظي و Amazon نم S3 ولد ىل Umbrella .

1. دجوي .يصن ررحم ي ف هحتف م ءه لعل جودزمل رقنلاب يديهمتلا فلملا ليزنتب مق .
كب ةصاخلا Umbrella تامولعم ءحول و S3 ولد ني ب طبري زيمم زمر فلملا لءاد
-



ءعب README فلم ضرعل ضرعتسملا ي ف S3 ولد شيءحت ىل اءاتحت دق :ءطءالم هليمحت .

2. زيمملا زمرلا "ىمسمل لقحلا ي ف زيمملا زمرلا قصل او Umbrella تامولعم ءحول ىل عءرا وه نيوكتلا نإف ،ءطقنلا هءه دنع .ظفح قوف رقنا مء ،"ديرفلا ةراءا مسق ي ف Amazon S3 مسا قوف طقف رقنا ،كب صاخلا نيوكتلا ءعءارمل .لماك لءسل

Log Management

Amazon S3

STATUS

LAST SYNC



Configured

August 2nd 2017, 11:43:21 am

AWS S3 Bucket: my-msp-organization-name-log-bucket

Last Sync: August 2nd 2017, 11:43:21 am



By default all customers are logged to this Amazon S3 Bucket. Logging can be manually turned off for customers individually from the [Customer Management](#) page.

STOP LOGGING

CLOSE

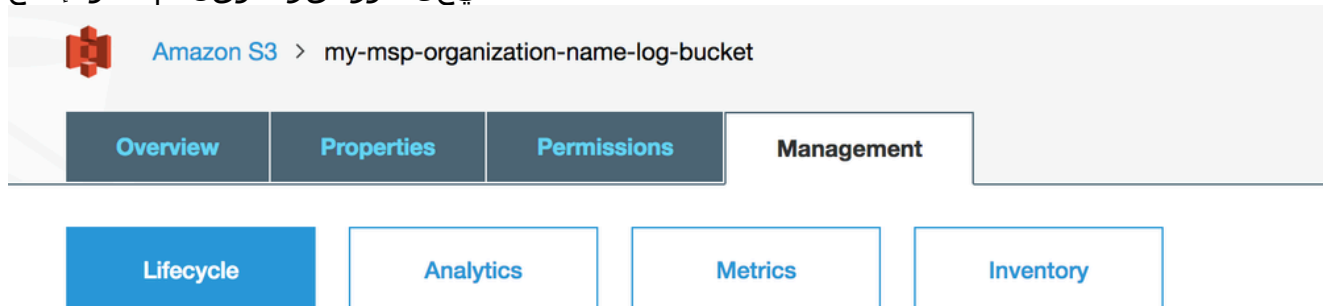
115012848126

لجسلا ةايح ةرود ةرادإ

ةينمزللا ةرتفل ديدمتل عدوتسملا لخاد تانايبلا ةايح ةرود ةرادإ كنكمي، S3 مادختسا دنن اقفو ادج ةليوط وأ ادج ةريصق ةدملا نوكت دق. اهب ةصاخلا تالجسلاب ظافتحالا ديرت يتلا ليزنت ةطاسبب كنكمي، لاثملا ليبس ىلع. يجرالخا لجسلا ةرادإل همذختست يذلا ببسلل ريغ لجأ ىلا تالجسلاب ظافتحالا وأ لاصتا نود انه نيختو ةعاس 24 دعب S3 ولد نم تالجسلال كنكولوىمسم ريغ لجأ ىلا ولد ي تانايبلا Amazon نيخت، ايضارتفا. ةباحسلا يف ىمسم S3، ةايح تارود لوح تامولعمل نم ديزمل. ولدلا ةنايص ةفلكت عفرى دودحمل ريغ نيختلا [انه](#) أرقا.

كب صاخلا ولد ةايح ةرود ةئيهتل:

1. ةايحلا ةرود قوف رقنا مث ةرادإ دح



115012848246

- إذا يعرف دلجم وأ) هلمكأب ولدلا ىلع ةدعاقلا قيبطتب مق مث، ةدعاق ةفاضل قوف رقنا (وحنلا اذه ىلع هنيوكتب تمق).
- بغرت تنك إذا امو ةينمزللا ةرتفل دح مث، ةفشرأ وأ فذح لثم، تانئكلا ىلع ءارج دح. ةيديلجال راهاألا). Amazon فيلاكت ليلقت يف ةدعاسملل Glacier نيخت مادختسا يف أطبأ هنوك نم مغلرلا ىلع يذلاو، طخال جراخ نيخت نع ةرابع تيذوكساللا ةينقت نأ يه (ةفلكت لقأ هنا إلا، هيلإ لوصولل).
- (يلخادلا يطايتحاللا خسنلا لح لثم) ىرخأ ةقيرطب تالجسلا ةرادإ لصف تنك إذا، تقو نييعت مث، ىرخأ ةقيرطب اهب ظافتحالاو S3 نم تالجسلا ليزنت ةطاسبب كنكمي ميايأ ةعضب ىلع ءاقبتسالا.

Cisco نم رادمال S3 عدوتسم نيوكت

ةلظملا تامولعم ةحول يف لجسلا ةرادإ > تادادعإلا ىلإ لقتنا

نارايخ كانه:

- ةكرشلل هريدت يذلا Amazon S3 ولد مدختسأ
- Amazon عقوم ىلع Cisco نم هترادإ متت يذلا S3 عدوتسم مادختسإ

Settings

 Log Management

Amazon S3

☒ Use your company-managed Amazon S3 bucket

Amazon S3 bucket

[VERIFY](#)

[Learn more about Amazon S3 bucket verification »](#)

☐ Use a Cisco-managed Amazon S3 bucket

25231151138964

"ةقطنم ددح": ناديدج نارايخ كحنم متي و "Amazon نم Cisco هريدت يذلا S3 ءاعو مادختسإ" رتخأ
".ءاقبتسا ةدم ددح" و



Settings

Log Management

Amazon S3

☐ Use your company-managed Amazon S3 bucket

☒ Use a Cisco-managed Amazon S3 bucket

Cisco will manage your logs in Amazon S3 for you. To learn more [view our guide](#).

Select a Region

US West (N. California)

Select a Retention Duration

Data older than the selected time period will be automatically deleted and cannot be recovered.

30 days

25231151158036

ةقطنم ديدحت

مداوخل اللى اتالجس للليزنت دنع لوصولو نمز ليلققتل ةمهم ةيميلق إل ةياهنل طاقن دعت ال نكلو، S3 نوزامأل في ةحاتم لقطانم ل ةمئاقل في ةجرديم لقطانم لقباطو. كيدل ةمئاقل في ةجرديم ريغ نيلصل، لاثم ليلبس لعل. قطانم لعيمج رفوت

في كتقطنم ريغيغت في بغرت تنك اذا. ةلدسنم ل ةمئاقل نم لكيل برقأل ةقطنم لرتخأ ديدج نم عدبل او ةيلالحل كاتاداعل فذح بجي، لبقتسم ل

ءاقبتسا ةدم ديدحت

عيمج ةلازا متي، ةددحم ل ةنمزل ةرتفل دعب. اموي 30 وأ 14 وأ 7 ةطاسبب يه ءاقبتسال ةدم تناك اذا لقأ ةنمزل ةرتفب يصولن. عيشي أنع رظنل لضغب اهدادرتسا نكمي الو تانايل بل قحال تقوي في ءاقبتسال ةدم ريغيغت نكمي. ةيداع كيدل عالتبأل ةرود

اهتدمو كتقطنم ديكأت كنم بلطوي لالتل قوف رقنا، تاديحتل ءارجاب كماي ق دعب

Do these settings look ok?

If you wish to change your region in the future, you will need to delete your current bucket and start over. Retention duration can be changed at any time.

Storage Region Asia Pacific (Seoul)
Retention Duration 30 Days

CANCEL

CONTINUE

25231181211796

طيشننتلاب مالعإىلع لوصحلا كنكمي،ةعباتملاىلع ةقفاوملا درجمب

We're activating AWS S3 export now...



We're still working to create your AWS S3 bucket...

Once activation is complete, we'll provide you with keys to access your new bucket.

25231181218708

تقولا هنأل ("!هإىلع لوصحلا" قوف رقنا) بچي.ي رسلحاتفم ولوصوحتافم ملتست مث
لوصولا حيتافم رفوت مزلي.حيتافملا نم يأةدهاشم إىلع هيف لصحت يذلا ديحول
كتالچس لي زنتو ولدلا إىل لوصولل ةيرسل حيتافملاو

كب صاخلا ولدلا مسا،مهألاو،نيوكتلا ضرعت يتلا ةصخلمللا ةشاشلا ىرتس،ارىخأ

Amazon S3

Status

● Active (Managed)

Last Sync

Sep 28, 2017 at 10:19 AM

✔

We're sending data to your managed S3 bucket

Storage Region

us-west-1

Retention Duration

30 days

EDIT

Bucket Name

s3://umbrella-managed-

Last Sync

Sep 28, 2017 at 10:19 AM

⚠

Forget your keys?

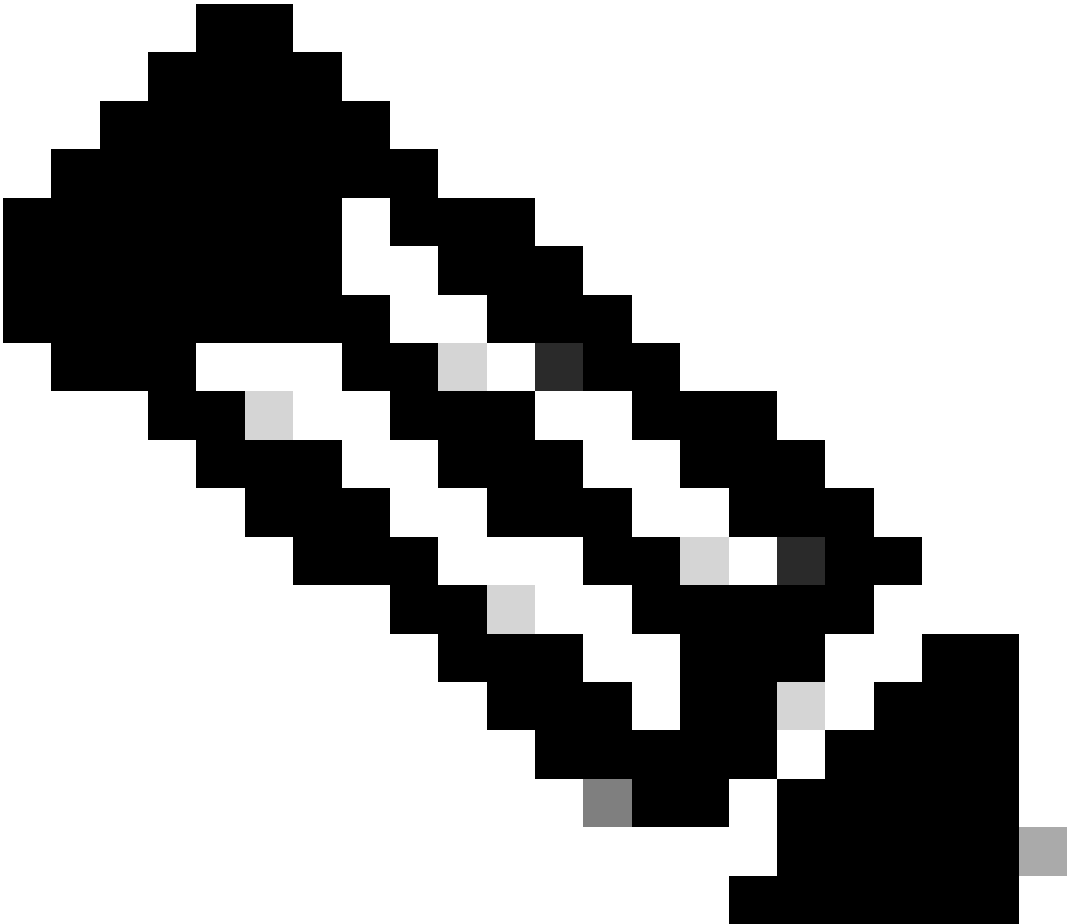
You can regenerate them below. Note that this will invalidate any existing keys.

STOP LOGGING

REGENERATE KEYS

25231181228180

كڭايتحال اق فو هلي غشت فاقيا و ا لي ج ست لا لي غشت كن كم ي



يتيح، ةددحمل ءاقبتسالا ةدم ىلإ اءانتسا تالءسالا ةلازا في Cisco رمتست :ةظءالم
لجسستالا لىغشت فاقى مت اءا

رشننل ةءام نىوكت تارايء

لجسالا لىمءت لشف

اهءدم ءامس ةرتف ءانه S3 ءءوتسم ىلإ Cisco Umbrella نم تالءسالا لىمءت لشف ةلاء في
ءتف مءى ،تاعاس عبرا ءعب .ةقىقء 20 ل ءلواءملا ءءاعب ءمءءالا اءلالء موقت تاعاس عبرا
لءشب لصاوتىو ءلءشملا ببس فى قىقءءالا اءبى ءءلا ،انىءل مءءلا قىرف عم ءىضقلا
ءلءشملا ءمءالا ءعم قىقءتسا

قىسنننل او اءلىمءت مءى تالا ءسالا نم ققءءالا

Umbrella لجس راطننا ءمءاق نم قىقءاقء رشن اهءدم ءىنمز لصاوف فى تالءسالا لىمءت مءى
نوضغ فى S3 ءءوتسم ىلإ لوالا لجسالا لىمءت مءى ،نىوكتالا لامءا ءعب .S3 ءالا ىلإ
لىمءت بلطءى ،ءلء عمو .ةىروفالا نم ءبىرق واءةىروف ءءاع نوكء ءىلمءالا نأ مءر ،نىءتءاس
ةئب فى ءلء لواءء نءا ءلءل ،اىءء اهؤاشن مءى تالا لجسالا تاناىب ءوءو ءىش
طاشننل نع ءءبال فى ءءبشالا تاناىب لىءسء نم ءءأءف ،رابءءا

ءامولعم ءءول ءاىءء فى ءنمزم ءقو رءا اءبى ،لمءى ءىش لء ناءا ءا م ققءءالا
S3 ءءوتسم فى روءظلال اهءالءسو Umbrella

هء صاءالا ءسسؤملا فرعمب ءسسؤم واءلىمء لء ىلء ءمءالء ءضو مء ،ءب صاءالا ولءلا لءءا
ىه ءلمءالا ءىننل فء ءلءل

Amazon S3/<bucket-name>/<orgID>/<subfolder>

<subfolder> وء ،ءب صاءالا ءمظنملا فرعم وء orgID وء ،ءب صاءالا ولءلا مسا وء <bucket-name>
لءاء ءءوءملا تالءسالا ءاونأ بسء ،IPLOGS وء ProxyLog وء DNSLOG اما

لء نمض "للمءالا ءاءاءءا" فى ءوءوملا مقرلا orgID قباطى ،MSSP و MSP ءالمءل ءبسننل
ءىمءء ءاسسؤملا ءءءءم ءالمءلل نءمى .رشننل ءاملمء مءسقى فى للمءالا لىصافء
فرعم ءظءالمو ءىءرف ءسسؤم لء ىلإ لوءءلا لىءسء قىرطنع ءسسؤملا فرعم
(). (https://dashboard.umbrella.com/o/#####/):ضرءءسملا ب صاءالا URL ناونع فى ءسسؤملا

S3 LOGS

Centralized Log Management

To enable centralized log management, a centralized bucket needs to be set up in the [Log Management](#) page.

Individual Log Management

[Configure individual log management](#)
This enables logging dedicated to this customer.

DEPLOYMENT PARAMETERS

Org ID	Fingerprint	User ID	Show install command	Resource
1918	1300a53676a576151b1c37	8955		How to set up RMM scripts

[DELETE THIS ORGANIZATION](#)
[CANCEL](#)
[SAVE](#)

360002271623

رهظتو 1.1 رادصلإل Multi-org و MSSP و MSP ءالمعل لجسلال قيسنت رادصلإ نوكي، ايلاح بسانملا يعرفلا دلجملا في S3 تالاد إلهل محت متي و GZIP قيسنتب تالجلال اذه ةيمستلا قيسنتب:

<subfolder>/<YYYY>-<MM>-<DD>/<YYYY>-<MM>-<DD>-<hh>-<mm>-<xxxx>.csv.gz

لخاد ةدوجوملا تالجلال ءاونأ بسح، IPLOGS، ProxyLog، DNSLOGS، ام وه <subfolder>. ةباتكلا عنمي امم، ةيمقر ةيدجأ فرأ ةعبرأ نم ةنوكم ةيئاوشع ةلسلس نع ةرابع <xxxx> ةرركملا تافلما ءامسأ قوف.

لثالملا لبس ىلع:

dnslogs/2019-01-01/2019-01-01-00-00-e4e1.csv.gz

يتلا تاوطخلا اءضوم معدلاب لاصتالا ىجرفي، قئاقد 10 لالخال ولدلا في تالجلال دءاشت مل اذا نآالا ىتح اءذختا.

تايللمع تايتوتحم طغض ءاغلل قيرط نع تانايبلا ةءجارمب يءون، تالجلال روظ درجمب تانايبلا ضرع ةيناكمإ نم دكأتلل اءلابقتسا متي يتلا ىلوالا ةلئللال تالجلال ليمحت ىلع ءالطالل (.csv. ل يءارتفالا دادءال وه، Microsoft Excel في ىتح وأ) صوصن ررحم في انه أرقا، لجلال في لقح لك لثم يتيلا تامولعمل.

ءبرأ اءدم ءامس ةرتف كانهف، S3 ءدوتسم ىلإ Cisco Umbrella نم لجلال ليمحت لشف اذا ةيضع حتف متي، تاعاس ءبرأ ءعب. ةقيقد 20 لك ةلواءملا ءءاعب ءمدخل اءلالء موقت تاعاس لكشب كب لصتيو ةلكشملا ببس في اققيقحت أدبي يذلا انيدل معدلا قيرف لخاد ةلكشملا نع كربءيل يقابقتسا.

ليجمع لكل لوخدلا ليچست نيكم

نكمي. كلذ فالخ ديدحت متي مل ام عالعملل عيچل ةزيملا هذه نيكم متي، عبرملا جراخ ةفلتخم ةمدخ تايوتسم كيذل ناك اذا ديفم رمأ وهو، دارفألا عالعملل ةزيملا ليغشت فاقيا حضوت. مكحتلا ةدحو في ليجمع لكب ةصاخ تادادعإ لك نمض اذه. ةزيملا مهيدل نيذل عالعملل اهلغشت فاقيا ل ليديتلا قباصلل مسقلا في ةشاشلا ةقول

ىلإ ءالؤه IAM يمدختسم نييعتو Amazon في IAM يمدختسم عاشنإ اضيأ نكمملا نمو ممدختسملل حامسلل كنكمي، كلذب ماقلا لالخ نم. ولدلا في نئاكلاب ةصاخ ةيعرف تادلجم طقف هتالچس نكلو، هتالچس ىلإ لوصولاب يئاهنلا

Splunk / لماكنتو قيسنتلا ىلع فرعتلا، تالچسلا ليذنت QRadar

نم DNS تالچس ليذنتل جهنلا ضعب كانه، اهكاهتسا واهب ظافتحالل تالچسلا ليذنتل انه ةلكشملا هذهل جهنلا ضعب حضوت ةلاقم عاشنإ مت دقل S3.

نع اليلق فلتخي فيكولچسلا قيسنت لوح ةلئسلال ضعب اضيأ كيذل نوكي دق قيسنت لوح تامولعملل نم ديزمل Umbrella تامولعمل ةحول في اهضرع متي يتلا تالچسلا ةلاقملا هذه أرقا، ردمملا لچسلا

SIEM تاودأ عم لماكللا في DNS تالچس ريصدتل ةيساسألا تامادختسال دحأ لثمتي، اريخأو دحأ ىلإ هلوزن متي ام ابلاغ هذه لثم تالچس عم لماعتلا دنع SIEM نيوكت نا نم مغرلا ىلع رثكألا SIEM ب ةصاخلا تاداشرالا ضعب انيدل، ةيصخشلا هتاليفت وه نيولوؤسملا اعويش

انه أرقا، Umbrella و Amazon AWS S3 ل Splunk يفاضلا نوكملا دادعإ لوح تامولعملل نم ديزمل

اهصخلتو Amazon S3 نم تالچسلا بچسل IBM QRadar نيوكت لوح تامولعملل نم ديزمل انه أرقا

S3 تالچس مچح ام

DNS رورم ةكرح مچح ىلع دمتعت يتلاو، ثدحت يتلا ثادحألا ددع ىلع S3 تالچس مچح دمتعي

انه S3 ليچستل لچسلا قيسنت ىلع روثعلا كنكمي

لوط) رصانعلا نم ددع ىلع ءانب لچس دنب لك مچح فلتخي نكلو، تياب 220 وه لاثملا لاخدا نوكيس، تياب 220 وه لچس رطس لك نأ ضارثفاب. (كلذ ىلإ امو، تائفلا ددع، لاجملا مسا تياباچيم 220 بلط نويلم

موي لك اهتيؤر متي يتلا DNS تامالعتسا ددعل ريذقت ىلع لوصحلل

1. Reporting > Activity Search ىلإ لقتنا، Umbrella تامولعمل ةحول في
2. ةنوقيأ قوف رقنا مث ةعاس 24 رخآل ريرقت ليغشتب مق، ةيفصتلا لماعو تحت. CSV ريصدت

تامالعتسا ددع وه (سأرلل دحاو صقان) فوفصلا ددع .هليزنت مت يذلا csv فلم حتفا 3. دحاو مويلا ري دقتلا ىلع لوصحلل تياب 220 ب كلذب رضا ؛مويلا في DNS

نوقفني ةماخض انئالمع رثكأ ىتح هنا دجن ،ةتوافتم اهنأ نم مغرلا ىلع ،ةفلكتلا ثيح نم طبترت وني زختلا تقوب فيلكتلا ىدحإ طبترت .ةمدخل ىلع ايرهش طقف تارالود ةعضب ديزم ىلع لوصحلل Amazon عقوم عجار .كتئي ب ىلإ S3 نم تانايبلا لي زنتب ىرخأ ةفلكت لي صافتلا نم

قلعتي امي ف اميس ال ،هدقتعت ام فرعن نأ دون ،انب ةصاخلا تامسلا نم ي أ عم لالحا وه امك ناك اذا .قئاثولا هذه اهي طغت يتلا ةئيبل نوكت ةيفاضا ةلئسأ ي أ أو SIEM لمكت تاي لمعب !كلذب انما لعإ عاجرلا ،تاظحالم ي أ كيدل

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 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