

عيطب LDAP ةقداصم عاداً

قيبطتلا ةيلباق

Splunk ةسسؤم

فصولا

ةقداصم ةقيرطك LDAP مادختسا دنع ادج ائيطب ني مدختسملا عاداً ناك

ءالجتسا

LDAP:

مدختسي حوتفم لوكوتورب وه، نزولا فيفخ ليلدللا ىلا لوصول لوكوتورب وأ، LDAP، ةداع مدختسي يذلا، نوناقلا اذه دعيو. ةيمره ليلد ةينب نم اءادرتساو تانايبلا نيختل تانايبلا نم عون ياً ديدحتل انرم الح، اهي مدختسمو اهلوصأو ةمظنملا نع تامولعمل نيختل اهصئاصغو.

ليلدللا ةمدخ:

ةمقي عون قيسنن تب اهميدقتو اهميظنتو تانايبلا نيختل ليلدللا ةمدخ مدختست تايلمع ىلع ةءارقلاو ثحبلاو ثحبلا تايلمعل ةلدال نيستحت متي، ةءاعلا يف. حاتفملا هنكلو ابلاغ اهيل ةراشلا متت يتلا تانايبلا ةياغلل ديج لكشب لمعت ثحب، ةباتكلا رركتم لكشب ريغتت.

قرطالا ددحي تالاصت لوكوتورب وه، نزولا فيفخ ليلدللا ىلا لوصول لوكوتورب وأ، LDAP، ةقيرطالا ليكشت ىلع LDAP لمعي، معاً لكشبو. ليلدللا ةمدخ ىلا اهي لوصول نكمي يتلا ددحي امك، ني مدختسملل ليلدللا ةمدخ يف ةدوجوملا تانايبلا ليثمت اهب متي نأ بجي يتلا ةقيرطالا صخليو، ليلد ةمدخ لخاد تانايب تالاخدا ءاشنإل ةمدختسملا تانوكملا تابلطتم تامسلا. تالاخدال نيوكتل ةفلتخم ةيئادب رصانع مادختسا اهب متي يتلا تامس ىمست رصانع يف يسيري لكشب LDAP ماظن يف اهسفن تانايبلا نيخت متي. ةساسا ميق جاوزا اساسا يه تامسلا.

تالاخدال:

نمض. عيشب نرتقت نا بجي، ىنعم اهل نوكي يكلو. ادج ةديفم تسيل اهتاذ دحب تامسلا تحت تامسلا نم ةعومجم ساسالا يف وه لخدملا. لخدم نمض صئاصخ مدختست تاناً LDAP، ام عيش فصول مدختسي مسا.

يف فنص لكل وأ كمماظن يف مدختسملا لخدال كي دل نوكي نأ نكمي، لاثملا ليبس ىلع

لخاد ةدحاو ةحفصل وأ ةيقيئال ع تانايب ةدعاق ماظن يف فصل ابيرقت لثامم اذهو .نوزخم ددحت امنيب .(جذامنلا هذه نم لك يف ةفلتخمل لوقحلا لثمت انه صئاصخلا) نيوان ع رتفد كلت عيمجتب ةطاسبب هسفن رصنعلا لخدملا فص ي ،ام عيشل ةفص وأ ةدوج ةمسلا مسا تحت تامسلا

تامولعم راجشأ ىمست يتلا راجشألا ىلع عورفك LDAP ماظن ىلإ تالخدإلا عيمج ةفاضإ متت ITs. وأ ،تانايبلا

لخدإ فالخب) لخدإ لك يوتحي ثيح تافلمل ماظنل ةهباشم ةيمىظنت ةينب DIT لثمي ةيعرفلا تالخدإلا نم ددع يأ ىلع يوتحي دقوامامت دحاو لصأ لخدإ ىلع (ىلعألا يوتسملا تالخدإلا ضعب نإف ،ابيرقت عيش ي لثمت نأ نكمي LDAP ةرجش يف تالخدإلا نأ امب .هتحت ماظن يف ةدوجوملا ةلدألل ةلثامم ،ةيمىظنت ضارغأل يسئير لكشب اهمادختسا متيس تافلمل

لثاملا ليبس ىلع:

```
dn: sn=Ellingwood,ou=people,dc=digitalocean,dc=com
```

This line is called the entry's distinguished name (more on this later) and is used to identify the entry. It functions like a full

LDAP authentication in Splunk in the end is querying a database and this query could be very broad if you don't set the right authentication.conf In the authentication.conf specification you can find out the following:

```
userBaseFilter = <string>
* OPTIONAL
* This is the LDAP search filter you wish to use when searching for users.
* Highly recommended, especially when there are many entries in your LDAP
  user subtrees
* When used properly, search filters can significantly speed up LDAP queries
* Example that matches users in the IT or HR department:
  * userBaseFilter = (&(|(department=IT)(department=HR)))
  * See RFC 2254 for more detailed information on search filter syntax
* This defaults to no filtering.
```

This in turn allows to narrow down the amount of entries that the query needs to search on because it filters allows to look only into certain e

رارق

يـلـالـلـ لـثـمـ UserBaseFilter مـدخـتـسـمـلـا يـدـلـ نـاـكـ:

```
userBaseFilter = (|(department=VP30)(department=VPIN)(department=VA02))
```

مـاسـقـأـلـا ةـفـاـكـ يـلـا نـومـتـنـي ءـيـطـبـلـا ءـاـدـأـلـا اـذـه نـوـظـحـالـي نـيـذـلـا نـومـدخـتـسـمـلـا نـكـي مـل مـبـر
ثـحـبـلـا تـايـلـمـع نـوكـت تـيـحـب نـيـمـسـق وـأ مـسـق ةـلـاـزـاب مـق .يـلـصـأـلـا UserBaseFilter يـف ةـجـرـدـمـلـا
يـلـا طـوقـف جـاـتـحـيـس LDAP مـداخـ نـأـل كـلـذـو ةـقـداصـمـلـا اـهـيـف ثـدـحـت ةـرمـلـك يـف اـعـاسـتـا لـقـأ
دـحـاو مـسـق تـالـاـخـدـا نـم قـقـحـتـلـا .

ةـلـصـ تـاـذـ طـبـاـور

ةـيـسـيـئـرـلـا تـاـبـاـجـاـلـا:

Windows 6.2 Splunk مـادخـتـسـاب "مـجـحـلـا دـح زـواجـت" ءـاطـخـأ مـ LDAP ةـقـداصـم لـشـفـت اـذا مـل
2008 R2؟

<https://answers.splunk.com/answers/179797/why-is-ldap-authentication-failing-with-size-limit.html>

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