Question #1 *Topic 1*

Which setting in indexes.conf allows data retention to be controlled by time?

A. maxDaysToKeep

B. moveToFrozenAfter

C. maxDataRetentionTime

D. frozenTimePeriodInSecs

Suggested Answer: *D*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/SmartStoredataretention

Community vote distribution
D (100%)

DeltaPotato Highly Voted 3 years ago
D - Sys Admin slide 131 for me (indexes.conf options listed on slide 126).
upvoted 7 times

pcksplunk 6 months, 4 weeks ago
D is correct
upvoted 1 times

Prasadthorat333 1 year, 11 months ago
Please help me with the Sys admin PDF.
upvoted 1 times

nanaw770 Most Recent 3 months, 2 weeks ago
Selected Answer: D
D is right answer.
upvoted 1 times

emlch 2 years ago
I did a quickly search and the only option seems to be frozenTimePeriodInSecs (the other options isn't additional configurations of indexes.conf)
upvoted 2 times

Nnatech 2 years, 2 months ago
Answer is D
upvoted 1 times

king1993 2 years, 4 months ago
Answer: D
upvoted 3 times

RedYeti 2 years, 5 months ago
Selected Answer: D
D. frozenTimePeriodInSecs
upvoted 2 times

Apis 2 years, 8 months ago
Selected Answer: D
D is correct
upvoted 1 times

BMO 3 years, 3 months ago
System Admin - Slide 116
upvoted 1 times

ZeusP 3 years, 3 months ago
Ans is D for sure
upvoted 1 times

MrHyde 4 years, 2 months ago

understand better with this link:
https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Setaretirementandarchivingpolicy

upvoted 3 times

ucsdmiami2020 2 years, 11 months ago

Agreed D. Quoting the provided URL reference, "To specify the age at which data freezes, edit the frozenTimePeriodInSecs attribute in indexes.conf. This attribute specifies the number of seconds to elapse before data gets frozen. "

upvoted 1 times

jasytpeiotqxvohxma 4 years, 3 months ago

D is correct

upvoted 2 times

Question #2 *Topic 1*

The universal forwarder has which capabilities when sending data? (Choose all that apply.)

A. Sending alerts

B. Compressing data

C. Obfuscating/hiding data

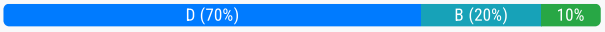
D. Indexer acknowledgement

Suggested Answer: *D*

Reference:

https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders

Community vote distribution



Ashton_98 Highly Voted 4 years, 3 months ago

D AND B Compressing data is the answer.

upvoted 14 times

Princee Highly Voted 4 years, 1 month ago

B and D both: compressed=true This tells the forwarder to compress the data before it forwards the data to receiving indexers in the target groups. If you
raw data.

Splunk doc:

https://docs.splunk.com/Documentation/Forwarder/8.1.1/Forwarder/Configureforwardingwithoutputs.conf#:~:text=compressed%3Dtrue%20This%20tells%

upvoted 6 times

MaryamNesa Most Recent 2 weeks ago

Selected Answer: B

D AND B Compressing data is the answer.

upvoted 1 times

MonicaKarim 1 month, 3 weeks ago

Selected Answer: B

B&D choose all that apply

upvoted 1 times

gatundu_ 5 months, 3 weeks ago

B & D are correct

upvoted 1 times

newrose 7 months, 1 week ago

B D seems correct

upvoted 1 times

dohatelo 11 months ago

B and D is correct . C(masking) can be done with the Heavy Forwarder not the Universal. Universal only parses data.

upvoted 1 times

bobixaka 1 year, 4 months ago

Selected Answer: B

B and D are correct

upvoted 1 times

Ibisc 1 year, 8 months ago

Selected Answer: C

I think C is also correct.

https://docs.splunk.com/Documentation/Splunk/latest/Data/Anonymizedata

"To anonymize data with Splunk Enterprise, you must configure a Splunk Enterprise instance as a heavy forwarder and anonymize the incoming data with that instance before sending it to Splunk Enterprise."

upvoted 1 times

Mntman77 1 year, 8 months ago

In this case they are referring to "universal forwarder" not a heavy, so "C" is out.

upvoted 1 times

harrytbb 2 years, 1 month ago

Selected Answer: D

B & D are the answers

upvoted 1 times

emlch 2 years, 6 months ago

UF has the following capabilities:

- Index ack* (useACK=true in outputs.conf)
- Send data over HTTP
- Compressing the feed (compressed = true on both input.conf (indexer) and outputs.conf (uf))
- Securing the feed with SSL

So, D and B

C. that would be a HF

A. not sure if Forwarders in general can send alerts

upvoted 3 times

emlch 2 years, 6 months ago

But definetely (a) the UF can't send alerts

upvoted 1 times

Ailen_Man 2 years, 10 months ago

Selected Answer: B

Answer is B

upvoted 1 times

Marco63 2 years, 10 months ago

B AND D !!!

upvoted 2 times

RedYeti 2 years, 11 months ago

Selected Answer: D

B. Compressing data

D. Indexer acknowledgement

System Admin course, page 182

upvoted 4 times

Apis 3 years, 2 months ago

Selected Answer: D

B and D are correct

upvoted 2 times

BMO 3 years, 9 months ago

Data Admin - Slide 65

upvoted 1 times

ZeusP 3 years, 9 months ago

Ans is B&D

upvoted 3 times

Question #3 *Topic 1*

In case of a conflict between a whitelist and a blacklist input setting, which one is used?

A. Blacklist

B. Whitelist

C. They cancel each other out.

D. Whichever is entered into the configuration first.

Suggested Answer: *A*
Reference:
https://www.google.com/url?
sa=t&rct=j&q=&esrc=s&source=web&cd=8&ved=2ahUKEwj0r6Lso6bkAhUqxYUKHbWlDz4QFjAHegQIAxAC&url=http%
3A%2F%2Fsplunk.training%2Fshowpdf.asp%3Fdata%
3D789BB6B10C1B4376B548D711B4377F3F4B511B437805A8EC11B437742EA8F11B43779B6FA211B4376EA657C11B4376FC19B311B4377E
2407E11B437
30AF97411B4377F3F4B511B437742EA8F11B43779B6FA211B43771F822111B437731365811B43730AF97411B437789BB6B11B4376B548D
711B4377F3F4B
511B437805A8EC11B437742EA8F11B43779B6FA211B4376EA657C11B4376FC19B311B4377E2407E11B43732E61E211B4377F3F4B511B43
7742EA8F11B4
3779B6FA211B43771F822111B437731365811B43746D0DC011B4377549EC611B4377BED81011B437789BB6B11B4376D8B14511B4377313
65811B4376B54
8D711B4377F3F4B511B4376FC19B311B43732E61E211B4376D8B14511B4377AD23D911B437789BB6B11B43730AF97411B4373989B2C11B
437386E6F511
B437386E6F511B4373DF6C0811B43737532BE11B4373BC039A11B437351CA5011B43737532BE11B43730AF97411B4375BD6DD511B43730
AF97411B4375
64E8C211B43730AF97411B437%257C2318D1%257C11649A&usg=AOvVaw2e9s-JweivuCkqTb4-Y9uW

Community vote distribution

A (100%)

newrose Highly Voted 3 years, 9 months ago
"It is not necessary to define both an allow list and a deny list in a configuration stanza. The settings are independent. If you do define both filters and a file matches them both, Splunk Enterprise does not index that file, as the blacklist filter overrides the whitelist filter."
Source: https://docs.splunk.com/Documentation/Splunk/8.1.0/Data/Whitelistorblacklistspecificincomingdata
upvoted 5 times

yybbb Most Recent 7 months, 2 weeks ago
Selected Answer: A
A. blacklist
upvoted 1 times

emlch 2 years ago
In case of a conflict the blacklist prevails
upvoted 3 times

Apis 2 years, 8 months ago
Selected Answer: A
A is correct
upvoted 4 times

BengieQuesada 3 years ago
A is correct Data Admin slide 123
upvoted 4 times

ZeusP 3 years, 3 months ago
Blacklist always overrides Whitelist
upvoted 1 times

Kobi 3 years, 6 months ago

Blacklist Overides Whitelist

upvoted 4 times

Praf7 3 years, 10 months ago

A. Blacklist

upvoted 2 times

Question #4 *Topic 1*

In which Splunk configuration is the SEDCMD used?

A. props.conf

B. inputs.conf

C. indexes.conf

D. transforms.conf

Suggested Answer: *A*
Reference:
https://answers.splunk.com/answers/212128/why-sedcmd-configured-in-propsconf-is-working-duri.html

Community vote distribution
A (100%)

emlch 6 months, 1 week ago
There's two transformation methods: SEDCMD or TRANSFORMS

SEDCMD: uses props.conf (used to mask or truncate raw data)
TRANSFORM: uses props.conf and transforms.conf (transforms matching events based on metadata)
upvoted 3 times

alejohu 6 months, 3 weeks ago
Selected Answer: A
A is correct
upvoted 2 times

Apis 1 year, 2 months ago
Selected Answer: A
A is correct
upvoted 1 times

ZeusP 1 year, 9 months ago
A in props.conf
upvoted 3 times

matsumo 1 year, 9 months ago
A is correct

<https://docs.splunk.com/Documentation/Splunk/8.2.0/Data/Anonymizedata>
Use the SEDCMD setting. This setting exists in the props.conf configuration file, which you configure on the heavy forwarder.
upvoted 2 times

ucsdmiami2020 1 year, 5 months ago
Agreed A. Quoting the Reference URL

"There are two ways to anonymize data with a heavy forwarder:
- Use the SEDCMD setting. This setting exists in the props.conf configuration file, which you configure on the heavy forwarder. It acts like a sed *nix script to do replacements and substitutions."
upvoted 1 times

sargeholik 2 years, 1 month ago
page 182 data admin
upvoted 1 times

ames 2 years, 6 months ago
"You can specify a SEDCMD configuration in props.conf to address data that contains characters that the third-party server cannot process. "
<https://docs.splunk.com/Documentation/Splunk/8.0.5/Forwarding/Forwarddatatothird-partysystemsd>
upvoted 3 times

ames 2 years, 6 months ago

So yea answer is A.

upvoted 1 times

ucsdmiami2020 1 year, 5 months ago

Agreed A. Quoting the Reference URL

"By default, Splunk software does not change the content of an event to make its character set compliant with the third-party server. You can specify a SEDCMD configuration in props.conf to address data that contains characters that the third-part server can't process."

upvoted 1 times

Asami 2 years, 8 months ago

answer is A

upvoted 1 times

Question #5 *Topic 1*

Which of the following are supported configuration methods to add inputs on a forwarder? (Choose all that apply.)

A. CLI

B. Edit inputs.conf

C. Edit forwarder.conf

D. Forwarder Management

Suggested Answer: *AB*
Reference:
https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/HowtoforwarddatatoSplunkEnterprise#Define_inputs_on_the_universal_forwarder_with_configuration_files

Community vote distribution
AB (100%)

AngusBlack Highly Voted 3 years, 8 months ago
It's A and B. On forwarder management you assigned server classes and apps, but adding a new input would be done by editing the inputs.conf on the DS, not using the Forwarder Management web interface.
upvoted 37 times

ucsdmiami2020 3 years, 5 months ago
Agreed A and B. Quoting the Reference URL https://docs.splunk.com/Documentation/Forwarder/7.3.1/Forwarder/HowtoforwarddatatoSplunkEnterprise#Define_inputs_on_the_universal_forwarder_with_configuration_files

"You can collect data on the universal forwarder using several methods. Define inputs on the universal forwarder with the CLI. You can use the CLI to define inputs on the universal forwarder. After you define the inputs, the universal forwarder collects data based on those definitions as long as it has access to the data that you want to monitor.
Define inputs on the universal forwarder with configuration files. If the input you want to configure does not have a CLI argument for it, you can configure inputs with configuration files. Create an inputs.conf file in the directory, $SPLUNK_HOME/etc/system/local
upvoted 1 times

Hamiltonian 3 years, 8 months ago
This needs more upvotes. The main purpose of the forwarder manager is to create server classes and overview the deployment. If you want to change the inputs, you do it via CLI on the forwarder, or change the settings in the inputs.conf file in the associated app on the DS which then will automatically update the settings on the forwarder after some phone home interval.
upvoted 5 times

Hamiltonian 3 years, 8 months ago
This is what the Add Data does on the Web UI, i.e., updates/creates the inputs.conf in the deployable app on the DS. It then automatically deploys/re-deploys the app to the remote forwarder.
upvoted 3 times

toney_mu 2 years ago
Add inputs on forwarders, by either:
- Editing inputs.conf manually
- Using Deployment Server
- Running Splunk commands (CLI)
upvoted 2 times

khyoung7410 Highly Voted 4 years, 3 months ago
My ans is A,B,D
upvoted 17 times

Hamiltonian 3 years, 8 months ago
Wrong. D is not part of the answer.
upvoted 4 times

newrose 4 years, 3 months ago

Agreed. CLI, inputs.conf editing, and via Deployment Server (forwarder maangement).

Source: "Configure the universal forwarder to send data to Splunk Enterprise
" section at https://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/HowtoforwarddatatoSplunkEnterprise
upvoted 5 times

toney_mu 2 years ago
A,B and D, you cna see the below notes in data admin pdf
Add inputs on forwarders, by either:
- Editing inputs.conf manually
- Using Deployment Server
- Running Splunk commands (CLI)
upvoted 1 times

yashgoel Most Recent 4 months, 3 weeks ago
Yes it A AND B
upvoted 1 times

toney_mu 2 years ago
I would say options AB and D
===
Add inputs on forwarders, by either:
- Editing inputs.conf manually
- Using Deployment Server
- Running Splunk commands (CLI)
====
upvoted 1 times

emlch 2 years, 6 months ago
You can add data inputs with: apps and add-ons, splunk web, CLI, editing inputs.conf
upvoted 2 times

cagdaskarabag 2 years, 7 months ago
Selected Answer: AB
ABD
Forwarder Mgmt from a deployment server.
upvoted 1 times

marda 2 years, 9 months ago
A, B, and D - Check page 175 of the SA PDF and you'll see it says:
-Forwarder management
-CLI
-Edit inputs.conf manually
upvoted 4 times

thissiteisgreat 2 years, 10 months ago
Selected Answer: AB
agreed for AB
upvoted 2 times

RichieL 2 years, 11 months ago
If you already have an input set up for a different forwarder then you can add that same input to a different forwarder using Forwarder Management. My answer is A, B and D
upvoted 1 times

Apis 3 years, 2 months ago
Selected Answer: AB
A and B for sure, maybe D as well, however D is not configured **on a forwarder**
upvoted 1 times

aallpp 3 years, 2 months ago
Hi ,
I'm stuck between a,b or a,b,d but the answer is a,b,d
upvoted 2 times

M9201715 3 years, 3 months ago

I think it's A, B and D. That's what Forwarder Management is for - to set up the inputs.conf file on the Deployment Server to push out to your Forwarders. Forwarder Management lets you set the apps (what this question is talking about), set the clients, and define the server classes that connect them together

upvoted 3 times

Sunny38 3 years, 6 months ago

A,B and D, check data admin slide 53

upvoted 6 times

BengieQuesada 3 years, 7 months ago

Forwarder Management is no right, answer is A and B. This is because we can add a forward via Deployment Manager but it is no the same that the Forwarder Manager that is used to create server classes and send apps.

upvoted 2 times

hesbee 3 years, 7 months ago

The correct answer is A & B. Please see the reference for clarification - https://docs.splunk.com/Documentation/Forwarder/8.2.1/Forwarder/HowtoforwarddatatoSplunkEnterprise

upvoted 1 times

navotfk 3 years, 8 months ago

answer is A & D...page 46 Data Admin

upvoted 2 times

ZeusP 3 years, 9 months ago

A, B & D

upvoted 4 times

Question #6 *Topic 1*

Which parent directory contains the configuration files in Splunk?

A. $SPLUNK_HOME/etc

B. $SPLUNK_HOME/var

C. $SPLUNK_HOME/conf

D. $SPLUNK_HOME/default

Suggested Answer: *A*

Reference:

https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Configurationfiledirectories

Community vote distribution

A (100%)

Apis Highly Voted 8 months, 2 weeks ago

Selected Answer: A

A is correct

upvoted 6 times

Asami Highly Voted 2 years, 1 month ago

A. $SPLUNK_HOME/etc

upvoted 5 times

ZeusP Most Recent 1 year, 3 months ago

Ans is A

upvoted 4 times

Question #7 *Topic 1*

Which forwarder type can parse data prior to forwarding?

A. Universal forwarder

B. Heaviest forwarder

C. Hyper forwarder

D. Heavy forwarder

Suggested Answer: *D*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders

Community vote distribution
D (100%)

Asami Highly Voted 3 years, 1 month ago
D. Heavy forwarder
upvoted 12 times

ucsdmiami2020 1 year, 11 months ago
Per the provided Reference URL https://docs.splunk.com/Documentation/Splunk/7.3.1/Forwarding/Typesofforwarders

"A heavy forwarder parses data before forwarding it and can route data based on criteria such as source or type of event."
upvoted 1 times

toney_mu Most Recent 6 months, 3 weeks ago
Option D
Parsing phase: Handled by indexers (or heavy forwarders)
- Data is broken up into events and advanced processing can be performed
upvoted 1 times

nedwons 1 year, 6 months ago
Heavy forwarder
upvoted 1 times

Apis 1 year, 8 months ago
Selected Answer: D
D is correct
upvoted 2 times

sargeholik 2 years, 8 months ago
both indexers and heavy forwarders parse events
upvoted 1 times

newrose 2 years, 9 months ago
"The universal forwarder does not parse data. You cannot use it to route data to different Splunk indexers based on its contents.", so the answer is Heavy Forwarder

Source: https://docs.splunk.com/Documentation/Splunk/latest/Forwarding/Typesofforwarders
upvoted 1 times

Question #8 *Topic 1*

Which Splunk component consolidates the individual results and prepares reports in a distributed environment?

A. Indexers

B. Forwarder

C. Search head

D. Search peers

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Advancedindexingstrategy

Community vote distribution
C (100%)

giubal Highly Voted 4 years, 4 months ago
It is the Search Head role
https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Howuserscancontroldistributedsearches
upvoted 23 times

ucsdmiami2020 2 years, 11 months ago
Agreed C. Quoting the reference URL

"From the user standpoint, specifying and running a distributed search is essentially the same as running any other search. Behind the scenes, the search head distributes the query to its search peers, and consolidates the results when presenting them to the user."
upvoted 7 times

rajpandey1512 Highly Voted 3 years, 3 months ago
PPT (Sys Admin) - Page 189 - "The search head consolidates the individual results and prepares reports."
upvoted 8 times

62d8e4c Most Recent 3 months, 2 weeks ago
C option is the correct one, SH.
upvoted 1 times

yybbb 7 months, 2 weeks ago
Selected Answer: C
Should be C
upvoted 1 times

KiranVM 1 year, 8 months ago
Selected Answer: C
As per the document, The indexers perform the actual searching of their own indexes, but the search heads manage the overall search process across all the indexers and present the consolidated search results to the user.
So answer is C
upvoted 4 times

Brinkster 1 year, 9 months ago
Correct answer is C.

Literally on the page quoted it says it's the search head: "The indexers still perform the actual searching of their own indexes, but the search heads manage the overall search process across all the indexers and present the consolidated search results to the user"
upvoted 2 times

alejohu 2 years ago
Selected Answer: C
C is correct
upvoted 3 times

Skandale 2 years, 1 month ago

Selected Answer: C

C is ans

upvoted 1 times

Yoho_1013 2 years, 6 months ago

Selected Answer: C

C should be the correct answer

upvoted 2 times

Apis 2 years, 8 months ago

Selected Answer: C

C is correct

upvoted 2 times

neledov 2 years, 9 months ago

Selected Answer: C

C - it's a search head

upvoted 2 times

Shiviv 3 years, 4 months ago

C is correct. Search head does it

upvoted 1 times

Sandy_1988 3 years, 7 months ago

C is the correct answer

upvoted 2 times

IDM 3 years, 10 months ago

search heads is the correct answer

upvoted 3 times

oksey 4 years ago

C is the correct Ans

upvoted 3 times

jasytpeiotqxvohxma 4 years, 3 months ago

Search heads is the correct answer

upvoted 4 times

Question #9 *Topic 1*

Which Splunk component distributes apps and certain other configuration updates to search head cluster members?

A. Deployer

B. Cluster master

C. Deployment server

D. Search head cluster master

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/PropagateSHCconfigurationchanges

Community vote distribution
A (100%)

loky0 Highly Voted 1 year ago
A. Deployer handles search heads, Deployment Server handles forwarders.
upvoted 8 times

Apis Most Recent 8 months, 2 weeks ago
Selected Answer: A
A is correct
upvoted 2 times

DeltaPotato 1 year ago
Unable to find any discussion of the deployer in either the sys or data admin class materials, but this page (https://docs.splunk.com/Documentation/Splunk/8.2.2/DistSearch/PropagateSHCconfigurationchanges) mirrors what Tony_123 said below.
upvoted 2 times

Tony_123 1 year, 7 months ago
The deployer is a Splunk Enterprise instance that you use to distribute apps and certain other configuration updates to search head cluster members. The set of updates that the deployer distributes is called the configuration bundle.
upvoted 4 times

ucsdmiami2020 11 months, 1 week ago
Agreed A. Continuing with the quoting of the reference URL provided by @DeltaPotato

"You must use the deployer, not the deployment server, to distribute apps to cluster members. Use of the deployer eliminates the possibility of conflict with the run-time updates that the cluster replicates automatically by means of the mechanism described in Configuration updates that the cluster replicates."
upvoted 1 times

sargeholik 1 year, 8 months ago
A. deployer
upvoted 1 times

Asami 2 years, 1 month ago
A. Deployer
upvoted 4 times

Question #10 *Topic 1*

Where should apps be located on the deployment server that the clients pull from?

A. $SPLUNK_HOME/etc/apps

B. $SPLUNK_HOME/etc/search

C. $SPLUNK_HOME/etc/master-apps

D. $SPLUNK_HOME/etc/deployment-apps

Suggested Answer: *A*
Reference:
https://answers.splunk.com/answers/371099/how-to-configure-deployment-apps-to-push-to-client.html

Community vote distribution
D (100%)

AbuAli Highly Voted 4 years, 11 months ago
The Answer is etc/deployment-apps
upvoted 29 times

ames Highly Voted 4 years, 6 months ago
After an app is downloaded, it resides under $SPLUNK_HOME/etc/apps on the deployment clients. But it resided in the $SPLUNK_HOME/etc/deployment-apps location in the deployment server.

Hence, answer is D.
upvoted 20 times

gatundu_ Most Recent 5 months, 3 weeks ago
On deployment clients, the directory is /etc/apps while on the deployment server the directory is /etc/deployment-apps
upvoted 1 times

62d8e4c 9 months, 3 weeks ago
D option is the correct one.
upvoted 1 times

allahsal 1 year ago
Selected Answer: D
Answer is D
upvoted 2 times

Maha86 1 year, 6 months ago
D is correct
upvoted 2 times

toney_mu 2 years ago
Answer should be D
=====
Configuration files (such as inputs.conf) to be packaged into apps to
be deployed to the deployment clients
Reside in SPLUNK_HOME/etc/deployment-apps/
=====
upvoted 2 times

ayush_1995 2 years, 8 months ago
Selected Answer: D
D is correct
upvoted 3 times

Apis 3 years, 2 months ago
Selected Answer: D
D is correct

upvoted 3 times

neledov 3 years, 3 months ago

Selected Answer: D

answer is D - it's deployment-apps

upvoted 5 times

sachinkiet 3 years, 3 months ago

Selected Answer: D

https://docs.splunk.com/Documentation/Splunk/8.2.3/Updating/Createdeploymentapps

upvoted 4 times

Sandy_1988 4 years, 2 months ago

Ans id D

upvoted 3 times

rj88 4 years, 6 months ago

Answer D is correct

upvoted 4 times

jasytpeiotqxvohxma 4 years, 9 months ago

D is correct

upvoted 3 times

Question #11 *Topic 1*

This file has been manually created on a universal forwarder:
/opt/splunkforwarder/etc/apps/my_TA/local/inputs.conf
[monitor:///var/log/messages]
sourcetype=syslog
index=syslog
A new Splunk admin comes in and connects the universal forwarders to a deployment server and deploys the same app with a new inputs.conf file:
/opt/splunk/etc/deployment-apps/my_TA/local/inputs.conf
[monitor:///var/log/maillog]
sourcetype=maillog
index=syslog
Which file is now monitored?

A. /var/log/messages

B. /var/log/maillog

C. /var/log/maillog and /var/log/messages

D. none of the above

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Exampleaddaninputtoforwarders

Community vote distribution
B (100%)

Stressplein Highly Voted 3 years, 9 months ago
https://answers.splunk.com/answers/728155/what-happens-if-you-deploy-an-inputsconf-from-a-ds.html
B
upvoted 17 times

Apis Highly Voted 2 years, 2 months ago
Selected Answer: B
B is correct. Apps from deployment server will overwrite any existing configuration
upvoted 6 times

bobixaka Most Recent 4 months, 1 week ago
Selected Answer: B
The client phones home to the DS, performs a checksum match on the apps and configs, finds a mismatch in that particular app and conf file, downloads the app from the DS and overwrites the mismatched inputs.conf
upvoted 4 times

InfoSec_RC53 1 year ago
This is a great example of the poorly written questions in a Splunk exam. Notice the path, it is in the "deployment-apps" folder which means it is on the DS, not the forwarder. Once it gets to the forwarder, it will then overwrite the inputs, and be located in the $SPLUNK_HOME/etc/apps folder.
upvoted 1 times

gibla1929 1 year, 9 months ago
Selected Answer: B
deployment client will reinstall the app with the same name that matches its expected hash.
upvoted 1 times

ZeusP 2 years, 9 months ago
B is correct as soon as UF try to connect with DS it will pull updated conf and over write the existing conf.
upvoted 4 times

Tony_123 3 years, 1 month ago

Once UF (DS client) connects DS server, it will pull the /opt/splunk/etc/deployment-apps/my_TA/local/inputs.conf from DS server , so B is the correct answer.
upvoted 5 times

pucca012 3 years, 1 month ago
A is the correct answer, because the local always take precedence.
upvoted 1 times

Hamiltonian 2 years, 8 months ago
This question has nothing to do with precedence. In the first case, the inputs.conf is written locally on the forwarder. In the second case, this original inputs.conf is overwritten by the new inputs.conf settings because the configurations been redeployed from a DS.
upvoted 4 times

Hamiltonian 2 years, 8 months ago
Better to say "deployed" rather than redeployed, because it's the first time a DS is being used with the forwarder.
upvoted 3 times

sargeholik 3 years, 1 month ago
b correct answer
upvoted 4 times

Sandy_1988 3 years, 2 months ago
B is the correct answer
upvoted 5 times

sergito095 3 years, 8 months ago
I think that the C is the correct answer, because inputs.conf file from forwarder is set up to monitor "messages" file and "maillog" file is monitored by Depolyment Server. Files are differents.
upvoted 3 times

Hamiltonian 2 years, 8 months ago
It doesn't matter. The DS is deploying the configuration setting sunder the given app name. The forwarder, once cnnected to the DS, will do whatever the DS tells it to do from the app configuration settings.
upvoted 2 times

Ashton_98 3 years, 3 months ago
That would be true if they didn't have the same app name. When you deploy an app with the same name, it will overwrite the inputs.conf file instead of merging.
upvoted 4 times

mker 3 years, 9 months ago
A is the correct answer, becouse the file inputs.conf will by overwrite by deployment
upvoted 2 times

mker 3 years, 9 months ago
sorry B is the correct
upvoted 7 times

Question #12 *Topic 1*

In which phase of the index time process does the license metering occur?

A. Input phase

B. Parsing phase

C. Indexing phase

D. Licensing phase

Suggested Answer: *C*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/HowSplunklicensingworks

Community vote distribution
C (100%)

ames Highly Voted 2 years, 6 months ago
True, its C. Part of the indexing process is to measure the volume of data being ingested, and report that volume to the license master for license volume tracking.
upvoted 6 times

Marco63 Most Recent 10 months, 3 weeks ago
Actually license metering happens AFTER parsing and BEFORE indexing, it's an intermediate phase.
upvoted 2 times

emlch 6 months, 1 week ago
Nah, the indexing phase includes license meter and indexing. The license meter runs as data is initially written to disk
upvoted 2 times

Apis 1 year, 2 months ago
Selected Answer: C
C is correct
upvoted 2 times

BMO 1 year, 9 months ago
Data Admin - Slide 14
C. is the correct answer
upvoted 1 times

splunkuser03 1 year, 2 months ago
Can anyone help sharing the splunk admin pdf.
upvoted 1 times

krishdee 1 year, 10 months ago
C. Indexing Phase
upvoted 1 times

Asami 2 years, 8 months ago
C. Indexing phase
upvoted 3 times

demarko 2 years, 5 months ago
https://docs.splunk.com/Documentation/Splunk/8.0.6/Admin/HowSplunklicensingworks
upvoted 4 times

ucsdmiami2020 1 year, 5 months ago
Agreed C. Quoting the reference URL,

"When ingesting event data, the measured data volume is based on the new raw data that is placed into the indexing pipeline. Because the data is measured at the indexing pipeline, data that is filetered and dropped prior to indexing does not count against the license volume qota."

upvoted 1 times

Question #13 *Topic 1*

You update a props.conf file while Splunk is running. You do not restart Splunk and you run this command: splunk btool props list `"-debug. What will the output be?

A. A list of all the configurations on-disk that Splunk contains.

B. A verbose list of all configurations as they were when splunkd started.

C. A list of props.conf configurations as they are on-disk along with a file path from which the configuration is located.

D. A list of the current running props.conf configurations along with a file path from which the configuration was made.

Suggested Answer: *D*
Reference:
https://answers.splunk.com/answers/494219/need-help-with-what-should-be-a-simple-precedence.html

Community vote distribution
C (100%)

giubal Highly Voted 3 years, 10 months ago
should be C
https://docs.splunk.com/Documentation/Splunk/8.0.1/Troubleshooting/Usebtooltotroubleshootconfigurations
upvoted 21 times

dpharker Highly Voted 3 years, 5 months ago
Answer is C.
See this phrase in the docs -> "The btool command simulates the merging process using the on-disk conf files and creates a report showing the merged settings."
https://docs.splunk.com/Documentation/Splunk/latest/Troubleshooting/Usebtooltotroubleshootconfigurations
upvoted 15 times

newrose 3 years, 3 months ago
Yes, and right after it says "The report does not necessarily represent what's loaded in memory. If a conf file change is made that requires a service restart, the btool report shows the change even though that change isn't active."
upvoted 8 times

bobixaka Most Recent 4 months, 1 week ago
Selected Answer: C
it troubleshoots config on disk not in memory. Answer: C
upvoted 2 times

erick165 1 year, 3 months ago
C is the correct answer
The report does not necessarily represent what's loaded in memory. If a conf file change is made that requires a service restart, the btool report shows the change even though that change isn't active.
upvoted 2 times

RedYeti 1 year, 11 months ago
Selected Answer: C
Answer is C.
upvoted 5 times

Apis 2 years, 2 months ago
Selected Answer: C
C is correct
upvoted 3 times

malice4 2 years, 10 months ago
Correct answer is C because debug displays the exact .conf file location
upvoted 2 times

ArDeKu 2 years, 11 months ago
It should be C as btool is used for ondisk and debug is used for file path..

upvoted 1 times

Jackall 3 years ago

btool key words: btool for on-disk ,and --debug for file location

upvoted 1 times

Tony_123 3 years, 1 month ago

C

splunk btool props list

-- shows on-disk configuration for requested

Use --debug to display the exact .conf file location

upvoted 1 times

Ashton_98 3 years, 3 months ago

btool will only show what is running / in memory, not what's on disk. D is correct.

upvoted 3 times

Ashton_98 3 years, 3 months ago

That's wrong actually, it's dependent on the conf and giubal and dphacker are correct.

upvoted 4 times

Question #14 *Topic 1*

When running the command shown below, what is the default path in which deploymentserver.conf is created? splunk set deploy-poll deployServer:port

A. SPLUNK_HOME/etc/deployment

B. SPLUNK_HOME/etc/system/local

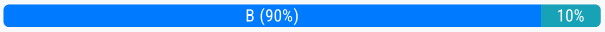
C. SPLUNK_HOME/etc/system/default

D. SPLUNK_HOME/etc/apps/deployment

Suggested Answer: *B*

Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Configuredeploymentclients

Community vote distribution



Jackall Highly Voted 2 years, 6 months ago

question description has a mistake for deploymentclient.conf not depoymentserver.conf

upvoted 13 times

Shafiqul 2 years, 3 months ago

True. Question should have been asking for the client conf since command has deploy poll in there which is normally configured in the client side. Answer should be D while question needs to be updated..

upvoted 3 times

Marco63 1 year, 4 months ago

Answer should be B, but question is wrong, because the file created is "deploymentclient.conf"

upvoted 1 times

RedYeti Highly Voted 1 year, 5 months ago

Selected Answer: B

B. SPLUNK_HOME/etc/system/local

Data Admin course, page 101

upvoted 6 times

toney_mu Most Recent 6 months, 3 weeks ago

deploymentclient.conf si created, option B

upvoted 1 times

BlueRoselia 1 year, 6 months ago

Data Admin pg 108 Creates deploymentclient.conf in SPLUNK_HOME/etc/system/local

upvoted 1 times

Lewist 1 year, 7 months ago

Selected Answer: B

answer is b

upvoted 3 times

Apis 1 year, 8 months ago

Selected Answer: C

C is correct with assumption the question was for deploymentclient.conf

upvoted 1 times

Apis 1 year, 8 months ago

Sorry, I meant B is correct: etc/system/local

upvoted 1 times

M9201715 1 year, 9 months ago

Answer is B, deploymentclient.conf is created in /etc/system/local

upvoted 2 times

furiousjase 2 years ago

In regards to deploymentclient.conf
deploymentclient.conf for connecting to a deployment server.

Configure the universal forwarder to connect to a deployment server
From a shell or command prompt on the forwarder, run the command:
./splunk set deploy-poll <host name or ip address>:<management port>

The forwarder writes configurations for forwarding data to outputs.conf in $SPLUNK_HOME/etc/system/local/). See Configure forwarding with outputs.conf, for information on outputs.conf.

https://docs.splunk.com/Documentation/Forwarder/8.2.2/Forwarder/Configuretheuniversalforwarder
upvoted 5 times

CCSHAO 2 years, 1 month ago

Refer to here. By the way, there is no "depoymentserver.conf", only "deploymentclient.conf"

https://docs.splunk.com/Documentation/Splunk/latest/Updating/Configuredeploymentclients
upvoted 2 times

BMO 2 years, 3 months ago

Despite the issue in the question, the response is C
Data Admin - Slide 103
upvoted 1 times

BMO 2 years, 3 months ago

The answer is B not C. (etc/system/local)
upvoted 5 times

happy_and_lucky 2 years, 7 months ago

https://docs.splunk.com/Documentation/Splunk/8.1.1/Updating/Definedeploymentclasses#Ways_to_define_server_classes
"When you use forwarder management to create a new server class, it saves the server class definition in a copy of serverclass.conf under $SPLUNK_HOME/etc/system/local. If, instead of using forwarder management, you decide to directly edit serverclass.conf, it is recommended that you create the serverclass.conf file in that same directory, $SPLUNK_HOME/etc/system/local."
upvoted 2 times

Asami 3 years, 1 month ago

B. SPLUNK_HOME/etc/system/local
upvoted 3 times

Question #15 *Topic 1*

The priority of layered Splunk configuration files depends on the file's:

A. Owner

B. Weight

C. Context

D. Creation time

Suggested Answer: *C*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfiles

Community vote distribution
C (100%)

RedYeti 5 months, 2 weeks ago
Answer C
Data Admin course, page 43 and 257
upvoted 3 times

Apis 8 months, 2 weeks ago
Selected Answer: C
C is correct
upvoted 2 times

DeltaPotato 1 year ago
C. Page 43, Data Admin pdf (page number as of August 2021 class).

"In case of conflicts, priority is based on context:
- Global context (index time)
- App/User context (search-time)"
upvoted 4 times

ucsdmiami2020 11 months, 1 week ago
Agreed C. Per the Splunk Reference URL
https://docs.splunk.com/Documentation/Splunk/8.2.2/Admin/Wheretofindtheconfigurationfiles

"To determine the order of directories for evaludating configuration file precendence, Splunk software considers each file's context. Configuration files operate in either a global context or in the context of the current app and user"
upvoted 5 times

Question #16 *Topic 1*

When configuring monitor inputs with whitelists or blacklists, what is the supported method of filtering the lists?

A. Slash notation

B. Regular expression

C. Irregular expression

D. Wildcard-only expression

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Filterclients

Community vote distribution
B (100%)

Asami Highly Voted 2 years, 8 months ago
B. Regular expression
upvoted 9 times

erick165 Most Recent 3 months, 2 weeks ago
Correction: D wildcards is incorrect as it says wildcards only so Regular Expressions is correct.
upvoted 2 times

erick165 3 months, 2 weeks ago
D. Wildcards:
clientName is a logical or tag name that can be assigned to a deployment client in deploymentclient.conf.
ipAddress is the IP address of the deployment client. Can use wildcards, such as 10.1.1.*
DNSname is the DNS name of the deployment client. Can use wildcards, such as *.ops.yourcompany.com
hostname is the host name of deployment client. Can use wildcards, such as *.splunk.com
instanceId is the instanceId of the client. This is a GUID string, for example: ffe9fe01-a4fb-425e-9f63-56cc274d7f8b.
upvoted 1 times

RedYeti 11 months, 3 weeks ago
Selected Answer: B
B. Regular expression
Data Admin course, page 123
upvoted 2 times

Apis 1 year, 2 months ago
Selected Answer: B
B is correct
upvoted 2 times

DeltaPotato 1 year, 6 months ago
B. Regular Expression - Page 123 - Data Admin PDF.
upvoted 3 times

newrose 2 years, 3 months ago
https://docs.splunk.com/Documentation/Splunk/latest/Data/Whitelistorblacklistspecificincomingdata#Include_or_exclude_specific_incoming_data is a better reference
upvoted 2 times

ucsdmiami2020 1 year, 5 months ago
Agreed B. Quoting the reference URL

"When you define filter entries, you must use exact regular expression syntax."
upvoted 2 times

Question #17 *Topic 1*

What is required when adding a native user to Splunk? (Choose all that apply.)

A. Password

B. Username

C. Full Name

D. Default app

Suggested Answer: *CD*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/Addandeditusers

Community vote distribution
AB (100%)

Racgud Highly Voted 4 years, 3 months ago
Splunk system admin slides page 144 CLEARLY shows that Name and Password is REQUIRED, while the rest is optional/set by default.
Thus A and B are correct
upvoted 32 times

newrose 4 years, 3 months ago
Agreed
upvoted 6 times

gatundu_ Most Recent 5 months, 3 weeks ago
Answer is username and password (A and B). All other fields are optional when creating a user
upvoted 1 times

Vidomina 1 year ago
Correct are: A and B, a role is required too (not an option here). C Full Name is optional, not required and D is just a default app which is preselected. Doesn't look required.
upvoted 1 times

gatundu_ 1 year, 1 month ago
Full name is optional. Answer is A&B.
upvoted 1 times

Ibisc 1 year, 8 months ago
Selected Answer: AB
Agree with Racgud. The page for version 9.0 is 223
upvoted 1 times

akamit225 1 year, 10 months ago
A B, rest are optional
upvoted 1 times

ALX951 2 years, 5 months ago
Selected Answer: AB
La A y B con correctas
upvoted 4 times

da_stingo 2 years, 10 months ago
Selected Answer: AB
vote for AB
upvoted 2 times

king1993 2 years, 10 months ago
Answer: A and B
upvoted 3 times

RedYeti 2 years, 11 months ago

Selected Answer: AB

A. Password

B. Username

System Admin course, page 154

upvoted 4 times

Apis 3 years, 2 months ago

Selected Answer: AB

A and B are correct

upvoted 2 times

teems5uk 3 years, 2 months ago

This is confusing. https://docs.splunk.com/Documentation/Splunk/8.2.3/Security/Addandeditusers

upvoted 1 times

M9201715 3 years, 3 months ago

You need to define the username, password and role when creating a user. It's not obvious if you do it through the web interface since there are a lot of fields that get filled in with defaults so it's unclear which are required and which are optional. But if you do it with the "add user" command in the CLI, you have to specify username, password and role. Since role is not one of the options in this question, the answer is just A and B.

upvoted 1 times

Powdered_Sugar 3 years, 4 months ago

I just made a new user in Splunk.

Username, Password, and Default App are all required. Full Name is optional.

A, B, and D are correct

upvoted 2 times

[Removed] 3 years, 4 months ago

Username, Password and a Role are required. Everything else the user can make those changes.

upvoted 1 times

malice4 3 years, 10 months ago

Only a password and a username are required, hence A and B.

upvoted 2 times

goal1860 3 years, 11 months ago

A, B are pretty sure. D is vague, as a default app is pre-selected for you anyway.

upvoted 3 times

Question #18 *Topic 1*

What are the minimum required settings when creating a network input in Splunk?

A. Protocol, port number

B. Protocol, port, location

C. Protocol, username, port

D. Protocol, IP, port number

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/UsetheHTTPEventCollector

Community vote distribution
A (100%)

BMO Highly Voted 1 year, 9 months ago
A is correct
Data Admin - Slide 137
upvoted 5 times

ucsdmiami2020 1 year, 5 months ago
Agreed A. Quoting the Reference URL https://docs.splunk.com/Documentation/Splunk/8.0.5/Admin/Inputsconf

[tcp://<remote server>:<port>]
*Configures the input to listen on a specific TCP network port.
*If a <remote server> makes a connection to this instance, the input uses this stanza to configure itself.
*If you do not specify <remote server>, this stanza matches all connections on the specified port.
*Generates events with source set to "tcp:<port>", for example: tcp:514
*If you do not specify a sourcetype, generates events with sourcetype set to "tcp-raw"
upvoted 3 times

emlch Most Recent 6 months, 1 week ago
Selected Answer: A
When you configure a network input you have to specify 4 configurations (only 2 are optional):
- Protocol: TCP or UDP
- Port
- Source name override
- Only Accept Conection from
upvoted 3 times

Apis 1 year, 2 months ago
Selected Answer: A
A is correct
upvoted 4 times

krishdee 1 year, 10 months ago
A. Protocal and Port Number
upvoted 1 times

ames 2 years, 6 months ago
A
[tcp:<port>]
* Configures the input listen on the specified TCP network port.
https://docs.splunk.com/Documentation/Splunk/8.0.5/Admin/Inputsconf
upvoted 1 times

Asami 2 years, 8 months ago
A. Protocol, port number

upvoted 2 times

Question #19 *Topic 1*

Which Splunk component requires a Forwarder license?

A. Search head

B. Heavy forwarder

C. Heaviest forwarder

D. Universal forwarder

Suggested Answer: *B*
Reference:
https://answers.splunk.com/answers/70017/heavy-forwarder-costs-and-licenses.html

Community vote distribution
D (56%) B (44%)

BMO Highly Voted 3 years, 9 months ago
B is correct
Data Admin - Slide 83
System Admin - Slide 42
upvoted 17 times

tjwe 3 years, 4 months ago
I agree, on system admin - slide 44 it says: Forwarder license: Sets the server up as a heavy forwarder.
upvoted 1 times

gatundu_ 4 months ago
Correct, but if the Heavy Forwarder needs to access other Splunk Enterprise instances, parsing and indexing, it requires a forwarder license
upvoted 1 times

dpharker Highly Voted 4 years, 5 months ago
This is a tricky question, because both HF and UF require a license, but the question asks which require a Forwarder License.
The HF uses a Enterprise License to be able to parse or index data.
The UF comes with a built-in license, but it is a license for forwarding.

So when they ask which component requires a Forwarder License, it's the UF
Correct answer is D.
upvoted 16 times

happy_and_lucky 4 years, 1 month ago
I think D too because https://docs.splunk.com/Documentation/Splunk/8.0.1/Admin/Distdeploylicenses
"***Universal forwarders only need a Forwarder license.***

If a heavy forwarder is performing additional functions such as indexing data or managing searches, it requires access to an Enterprise license."
upvoted 5 times

3bd8ac0 Most Recent 1 month ago
Selected Answer: D
D
check official documentation
Universal forwarders only need a Forwarder license. If a heavy forwarder is performing additional functions such as indexing data or managing searches, it requires access to an Enterprise license.
https://docs.splunk.com/Documentation/Splunk/8.0.1/Admin/Distdeploylicenses
upvoted 1 times

Bob_Hob 1 month, 1 week ago
Selected Answer: B

The correct answer is A and D assuming the HF is set up as non-indexing. According to the course for the exam, "sets the server up as a heavy forwarder" probably means they would be looking for the HF as the answer, even though the UF is technically more correct

upvoted 1 times

ljackson 2 months, 2 weeks ago

Selected Answer: B

In both the Ent Admin and Data Admin slide decks, any reference to the phrase "Forwarder License", is attached to comment about the HF not the UF. Answer B.

upvoted 1 times

Alens19 4 months ago

Correct answer seems to be B, a Forwarding License is a license for a forwarder, which is a Splunk Enterprise instance that forwards data to another Splunk Enterprise server or to a third-party system.

In this case the HF is a Splunk Enterprise instance forwarding data, "The heavy forwarder should have access to an Enterprise license stack if you plan to perform indexing on the forwarder or to enable authentication on the forwarder." A "stack" is a collection of licenses, meaning that the forwarding license is required and included in the stack

upvoted 1 times

Alens19 4 months ago

Documentation proving what I said:

https://docs.splunk.com/Splexicon:Forwardinglicense

https://docs.splunk.com/Splexicon:Stack

upvoted 1 times

Alens19 4 months ago

D is correct, as the documentation provided below says, ¨Universal forwarders only need a Forwarder license. If a heavy forwarder is performing addition data or managing searches, it requires access to an Enterprise license.¨

https://docs.splunk.com/Documentation/Splunk/9.3.1/Admin/Distdeploylicenses#:~:text=Universal%20forwarders%20only%20need%20a,access%20to%2(

upvoted 1 times

gatundu_ 4 months, 3 weeks ago

Correct answer is D. A Heavy Forwarder uses an Enterprise license

upvoted 1 times

gabo1969 4 months, 1 week ago

In the question only the UF need just a forwarder license, the HFW can use the forwarder license, but also can use a Enterprise licence, in this case, by the questions , the correct would be "D"

upvoted 1 times

allahsal 1 year ago

Selected Answer: B

Forwarder license

• Sets the server up as a heavy forwarder

• Applies to non-indexing forwarders

• Allows authentication, but no indexing

upvoted 1 times

allahsal 1 year ago

I was wrong, the answer is D

upvoted 1 times

allahsal 1 year ago

Selected Answer: D

https://docs.splunk.com/Documentation/Splunk/8.0.1/Admin/Distdeploylicenses

"***Universal forwarders only need a Forwarder license.***

upvoted 1 times

allahsal 1 year ago

D is the correct answer.

https://docs.splunk.com/Documentation/Splunk/8.0.1/Admin/Distdeploylicenses

"***Universal forwarders only need a Forwarder license.***

upvoted 1 times

Vidomina 1 year ago

Selected Answer: D

I should be D.

The universal forwarder has the Forwarder license applied automatically.

Heavy Forwarder has Enterprise or Forwarder license

upvoted 1 times

bobixaka 1 year, 4 months ago

Selected Answer: D

HF requires Enterprise License

UF comes with a free "Forwarding License"

upvoted 3 times

emlch 2 years, 6 months ago

Selected Answer: B

The HF Requires a Splunk Enterprise Instance with the Forwarder License enabled.

The UF is provided as separate installation with a built-in license

upvoted 2 times

MxQ3 2 years, 7 months ago

Heavy Forwarder for sure

upvoted 1 times

Apis 3 years, 2 months ago

Selected Answer: B

B is correct

upvoted 1 times

gabo1969 3 years, 3 months ago

UF Don´t require licence to work

upvoted 1 times

Question #20 *Topic 1*

Which optional configuration setting in inputs.conf allows you to selectively forward the data to specific indexer(s)?

A. _TCP_ROUTING

B. _INDEXER_LIST

C. _INDEXER_GROUP

D. _INDEXER_ROUTING

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Monitorfilesanddirectorieswithinputs.conf

Community vote distribution
A (100%)

emlch 6 months, 1 week ago
[monitor:<file path>]
_TCP_ROUTING = <index name>

In inputs.conf (UF)
upvoted 3 times

Apis 1 year, 2 months ago
Selected Answer: A
A is correct
upvoted 3 times

loky0 1 year, 6 months ago
A
P66 on Data Admin pdf
upvoted 3 times

ames 2 years, 6 months ago
A.

Extra read: https://docs.splunk.com/Documentation/Splunk/7.0.3/Forwarding/Routeandfilterdatad#Perform_selective_indexing_and_forwarding
upvoted 2 times

ucsdmiami2020 1 year, 5 months ago
Per the provided reference URL

_TCP_ROUTING = <tcpout_group_name>,<tcpout_group_name>,...

Specifies a comma-separated list of tcpout group names. Use this setting to selectively forward your data to specific indexers by specifying the tcpout groups that the forwarder should use when forwarding the data.

Define the tcpout group names in the outputs.conf file in [tcpout:<tcpout_group_name>] stanzas. The groups present in defaultGroup in [tcpout] stanza in the outputs.conf file.
upvoted 2 times

Asami 2 years, 8 months ago
A. _TCP_ROUTING
upvoted 3 times

Question #21 *Topic 1*

To set up a network input in Splunk, what needs to be specified?

A. File path.

B. Username and password.

C. Network protocol and port number.

D. Network protocol and MAC address.

Suggested Answer: *A*
Reference:
http://dev.splunk.com/view/dev-guide/SP-CAAAE3A

Community vote distribution
C (100%)

oksey Highly Voted 2 years, 6 months ago
C is the Ans
upvoted 18 times

AbuAli Highly Voted 2 years, 11 months ago
According to Splunk doc:
https://docs.splunk.com/Documentation/Splunk/8.0.3/Data/Monitornetworkports

Network port and protocol is required
upvoted 11 times

ames 2 years, 6 months ago
So.... C?
upvoted 7 times

emlch Most Recent 6 months, 1 week ago
Check question 18
upvoted 3 times

Helaros 10 months, 2 weeks ago
Selected Answer: C
C is correct
upvoted 4 times

Toffaletti 11 months ago
Selected Answer: C
C is the answ
upvoted 3 times

Apis 1 year, 2 months ago
Selected Answer: C
C is correct
upvoted 3 times

JJJefferson 1 year, 5 months ago
So this is a duplicate question, the previous answer was protocol and port.....now its file path? I don't think so.
upvoted 2 times

gsplunker 2 years ago
C is the answer
upvoted 2 times

happy_and_lucky 2 years, 1 month ago
q said network input, so makes more sense if C = network protocol and port
upvoted 2 times

Sandy_1988 2 years, 2 months ago

C is the answer

upvoted 3 times

Question #22 *Topic 1*

Which Splunk forwarder type allows parsing of data before forwarding to an indexer?

A. Universal forwarder

B. Parsing forwarder

C. Heavy forwarder

D. Advanced forwarder

Suggested Answer: *C*
Reference:
https://docs.splunk.com/Documentation/SplunkCloud/7.2.6/Forwarding/Typesofforwarders

Community vote distribution
C (100%)

Fe01 7 months, 3 weeks ago
That has already been asked in question 7
upvoted 4 times

Apis 8 months, 2 weeks ago
Selected Answer: C
C is correct
upvoted 3 times

thomass 1 year, 5 months ago
Answer : C
upvoted 3 times

ucsdmiami2020 11 months, 1 week ago
Agreed C. Quoting the Splunk reference URL https://docs.splunk.com/Documentation/Splunk/8.2.2/Forwarding/Typesofforwarders

"A heavy forwarder is a full Splunk Enterprise instance that can index, search, and change data as well as forward it. The heavy forwarder has some features disabled to reduce system resource usage."
upvoted 2 times

Asami 2 years, 1 month ago
C. Heavy forwarde
upvoted 3 times

Question #23 *Topic 1*

Which of the following statements describe deployment management? (Choose all that apply.)

A. Requires an Enterprise license.

B. Is responsible for sending apps to forwarders.

C. Once used, is the only way to manage forwarders.

D. Can automatically restart the host OS running the forwarder.

Suggested Answer: *A*

Community vote distribution

Praf7 Highly Voted 4 years, 3 months ago

Option A & B

upvoted 28 times

ucsdmiami2020 3 years, 5 months ago

Agreed A and B. Quoting two Splunk Reference URLs

https://docs.splunk.com/Documentation/Splunk/8.2.2/Admin/Distdeploylicenses#:~:text=License%20requirements,do%20not%20index%20external%2

"All Splunk Enterprise instances functioning as management components needs access to an Enterprise license. Management components include th deployment server, the indexer cluster manager node, the search head cluster deployer, and the monitoring console."

https://docs.splunk.com/Documentation/Splunk/8.2.2/Updating/Aboutdeploymentserver

"The deployment server is the tool for distributing configurations, apps, and content updates to groups of Splunk Enterprise instances."

upvoted 7 times

tommot Highly Voted 4 years, 6 months ago

C is wrong. we can still use CLI and direct editing even after enabling DS.

upvoted 15 times

SasnycoN 3 years, 3 months ago

You can but they will be overwritten by the DS on the nest communication.

upvoted 4 times

EnidV 2 years, 5 months ago

The CLI could be used even on DS.

upvoted 2 times

bobixaka Most Recent 1 year, 4 months ago

Selected Answer: B

A and B

upvoted 1 times

bobixaka 1 year, 4 months ago

Selected Answer: B

A and B are correct

upvoted 1 times

tmmt 2 years ago

Selected Answer: B

Is A and B.

upvoted 1 times

mr56 2 years, 1 month ago

AB not C - For some complex configuration requirements, however, you might need to edit serverclass.conf directly. Important: If you switch from forwarder management to direct editing of serverclass.conf, you might not be able to use forwarder management for any subsequent

configuration. This is because the forwarder management interface can handle only a subset of the configurations possible through serverclass.conf.

upvoted 1 times

PKV27 2 years, 10 months ago

A&B for sure,

C,D - is discussable, by design not applicable

C - is it possible use sys/local/*.conf, DS not overriding this confs with apps

D - what about run ps script Restart-Computer on win OS? so it is possible to restart host OS

upvoted 2 times

BlueRoselia 3 years ago

Data Admin pg 97 A&B

Deployment Server is a built-in tool for managing configuration of Splunk instances

–Allows you to manage remote Splunk instances centrally–Requires an Enterprise License

–Handles the job of sending configurations (inputs.conf, outputs.conf, etc.) packaged as apps

–Can automatically restart remote Splunk instances

•Forwarder management is a graphical interface on top of deployment server

•Monitoring Console Forwarder dashboards help you monitor the deployment

•Best Practice: The Deployment Server should be a dedicated Splunk instance–In this class, you will use your test server as a deployment server

upvoted 2 times

Alusine 3 years, 1 month ago

Its ABCD....page 68 of PDF. Can Automatically restart the remote splunk instances, manages forwarder configurations

upvoted 1 times

kurzer_ 2 years, 11 months ago

Exactly what you said, "It can restart remote SPLUNK INSTANCES" but not the Host OS.

D is wrong!

upvoted 5 times

Mntman77 1 year, 8 months ago

exactly!

upvoted 1 times

Hurshbabe 1 year, 5 months ago

Restarting as instance is equivalent to restarting the OS so D is right

upvoted 1 times

Hurshbabe 1 year, 5 months ago

never mind my answer, its wrong

upvoted 1 times

Apis 3 years, 2 months ago

Selected Answer: A

A and B are correct

upvoted 3 times

ivaanovich 3 years, 6 months ago

Tricky one, but I'd say that C is also correct: once an app is put under Deployment Management, the app's folder (the whole of it) will be overwritten each time the UF detects that there's a mismatch between it's own content and that from the DS. So yes: once used, Deployment Management is the only way to manage THOSE APPS in the forwarders. (apps that are not under Deployment Management can still be managed locally. And of course you can always disable Deployment Management on an app and go back to manual updates, if you so wish).

upvoted 2 times

toney_mu 2 years ago

You cna disable the DS and still push apps or update apps

upvoted 2 times

ckmunich 3 years, 7 months ago

Only A and B are right

C is wrong. You can still use the CLI or edit the .conf files

D is wrong. No Splunk component can cause the underlying OS to reboot.

upvoted 6 times

SasnycoN 3 years, 3 months ago

About C - But even if you made any changes to the files via CLI they will be overwritten by the DS in the next communication.

upvoted 1 times

mjl79 3 years, 8 months ago

A & B. C is wrong because you can still use the CLI or edit the .conf files and D is a sneaky answer designed to catch you out; No Splunk component can cause the underlying OS to reboot.

upvoted 1 times

SasnycoN 3 years, 3 months ago

What will happen if you use CLi to edit the .conf files and in the next communication DS detects that there are changes?!

upvoted 1 times

gsplunker 4 years ago

Guess A,B and D

upvoted 4 times

gatundu_ 4 months, 1 week ago

D is wrong. The DS can only start remote Splunk instances

upvoted 1 times

lollo1234 3 years, 10 months ago

NO! You cant restart fw os

upvoted 1 times

IDM 4 years, 4 months ago

A and B

C is a trick as, it can restart the forwarder on the client NOT the client/HOST OS.

upvoted 5 times

oksey 4 years, 6 months ago

I would go for ABD

upvoted 4 times

ames 4 years, 6 months ago

I would say A, B, D.

https://docs.splunk.com/Splexicon:Deploymentserver

upvoted 4 times

Question #24 *Topic 1*

During search time, which directory of configuration files has the highest precedence?

A. $SPLUNK_HOME/etc/system/local

B. $SPLUNK_HOME/etc/system/default

C. $SPLUNK_HOME/etc/apps/app1/local

D. $SPLUNK_HOME/etc/users/admin/local

Suggested Answer: *C*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfiles

Community vote distribution
C (56%) D (44%)

dwallen41 Highly Voted 4 years, 3 months ago
Very tricky!!! Answer is NOT D as etc/users/admin/local is not a valid directory . it is missing the <user app>.... to be correct it would look like this... etc/users/admin/<app name>/local .. so answer is C. Also reference Data Admin class PDF page 20 search time precedence diagram..
upvoted 31 times

SPLTony 1 year, 6 months ago
What if "admin" in this case was the name of the application?
upvoted 1 times

SCARODJ 10 months ago
Apps don't go in the 'users' folder.
upvoted 1 times

giubal Highly Voted 4 years, 10 months ago
The question is about "search time" no "index time" (Global context) so the App/User context has the highest precedence, the answer is D

https://docs.splunk.com/Documentation/Splunk/7.3.0/Admin/Wheretofindtheconfigurationfiles
upvoted 14 times

ucsdmiami2020 3 years, 5 months ago
Agreed D. Adding further clarity and quoting same Splunk reference URL from @giubal"

"To keep configuration settings consistent across peer nodes, configuration files are managed from the cluster master, which pushes the files to the slave-app directories on the peer nodes. Files in the slave-app directories have the highest precedence in a cluster peer's configuration. Here is the expanded precedence order for cluster peers:
1.Slave-app local directories -- highest priority
2. System local directory
3. App local directories
4. Slave-app default directories
5. App default directories
6. System default directory --lowest priority
upvoted 2 times

AngusBlack 3 years, 8 months ago
It would be, but the directory name isn't valid
upvoted 4 times

hesbee 3 years, 7 months ago
Can you explain better, please? On the documentation, it only says "$SPLUNK_HOME/etc/users/*". How is that invalid?
upvoted 1 times

Marco63 2 years, 10 months ago
In the answer the /app_name/" segment of the path is missing
upvoted 2 times

3bd8ac0 Most Recent 4 weeks, 1 day ago

Selected Answer: D

D, check page 121 os the System Admin official Splunk course.
Search-Time Precedence (App/User Context)
Precedence order where 1 is highest priority:

1. Current user directory for app
etc/users/user/appname/local

2. App directory - running app
etc/apps/appname/local
etc/apps/appname/default

3. App directories - all other apps*
etc/apps/appname/local
etc/apps/appname/default

4. System directories
etc/system/local
etc/system/defaultPrecedence order
upvoted 1 times

3bd8ac0 1 month ago

Selected Answer: D

tricky question, however, if you follow the documentation this is the precedence for search time: Precedence order

1. Current user directory for app
etc/users/user/appname/local

2. App directory - running app
etc/apps/appname/local
etc/apps/appname/default

3. App directories - all other apps*
etc/apps/appname/local
etc/apps/appname/default

4. System directories
etc/system/local
etc/system/default
upvoted 1 times

65aab2c 4 months, 3 weeks ago

Search-Time Precedence (App/User Context)

Current user directory for app
etc/users/user/appname/local
2. App directory - running app
etc/apps/appname/local
etc/apps/appname/default
3. App directories - all other apps*
etc/apps/appname/local
etc/apps/appname/default
4. System directories
etc/system/local
upvoted 2 times

Frank_Rai 11 months ago

It's 'D'.

During search time, the directory of configuration files with the highest precedence is:

D. $SPLUNK_HOME/etc/users/admin/local

The order of precedence for configuration files in Splunk, from highest to lowest, is as follows:

1. **$SPLUNK_HOME/etc/users/<username>/<appname>/local**
2. **$SPLUNK_HOME/etc/users/<username>/<appname>/default**
3. **$SPLUNK_HOME/etc/apps/<appname>/local**
4. **$SPLUNK_HOME/etc/apps/<appname>/default**
5. **$SPLUNK_HOME/etc/system/local**
6. **$SPLUNK_HOME/etc/system/default**

This hierarchy ensures that user-specific settings (which are stored in the `$SPLUNK_HOME/etc/users` directory) take precedence over app-specific settings and system-wide settings.

upvoted 1 times

lance_grown 1 year, 3 months ago

1. Current user directory for app etc/users/user/appname/local
2. App directory -running app etc/apps/appname/local etc/apps/appname/default
3. App directories -all other apps* etc/apps/appname/local etc/apps/appname/default
4. System directories etc/system/localetc/system/default

PDF Page 341

Since the path of D is wrong, I would go with C as the next in line to take precedence and its the highest for this question

upvoted 2 times

bobixaka 1 year, 4 months ago

Selected Answer: C

D is very tricky!
It would have been the correct answer if it was D. $SPLUNK_HOME/etc/users/admin/app_name/local
Since there is no app in the path it doesn't exist.

upvoted 1 times

Splunkor 1 year, 4 months ago

Selected Answer: D

The question is about search-time precedence, answer D is correct.

upvoted 1 times

Splunkor 1 year, 4 months ago

Answer D is correct.

upvoted 1 times

tmmt 2 years ago

Selected Answer: C

If D have a correct dir (/etc/users/app_abcde/local) will be correct, but in this case is C

upvoted 1 times

pro12345 2 years, 5 months ago

Selected Answer: C

Answer C

upvoted 1 times

emlch 2 years, 6 months ago

Selected Answer: D

INDEX time: sys local, app local, app default, sys default
SEARCH time: user app (user directory), running app (local and defautl), other apps (local and default), sys directories (local and default).

so D!

upvoted 3 times

tmmt 2 years ago

very clear, thanks!

upvoted 1 times

king1993 2 years, 10 months ago

Answer: C

upvoted 1 times

BlueRoselia 3 years ago

global/index context

1.etc/system/local

2.etc/apps/app_name/local

3.etc/apps/app_name/default

4.etc/system/default

User/app/search context

1.etc/users/system/local fallow by default

2.etc/apps/currently_running_app/local fallow by default

3.etc/apps/all_other_apps/local fallow by default

4.etc/system/local fallow by default

upvoted 1 times

[Removed] 3 years, 1 month ago

A is correct, page 86-89 in System admin PDF

upvoted 2 times

[Removed] 3 years, 1 month ago

No Sorry, it says search time. Then it is D. Page 90, system admin PDF

upvoted 1 times

[Removed] 3 years, 1 month ago

Ok, don't listen to me. Like people has said. App is missing. Trick question. C all the way here

upvoted 2 times

Apis 3 years, 2 months ago

Selected Answer: C

C is correct

D is incorrect - path is missing app name (assuming local is not an app name)

upvoted 2 times

Question #25 *Topic 1*

Within props.conf, which stanzas are valid for data modification? (Choose all that apply.)

A. Host

B. Server

C. Source

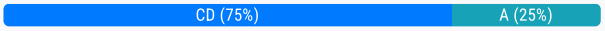
D. Sourcetype

Suggested Answer: *CD*

Reference:

https://answers.splunk.com/answers/3687/host-stanza-in-props-conf-not-being-honored-for-udp-514-data-sources.html

Community vote distribution



Praf7 Highly Voted 4 years, 3 months ago

Option - A,C & D are correct.

upvoted 24 times

happy_and_lucky 4 years, 1 month ago

https://docs.splunk.com/Documentation/Splunk/8.1.1/Admin/Propsconf

upvoted 1 times

sargeholik Highly Voted 4 years, 3 months ago

ACD correct answer, page 151 data admin

upvoted 5 times

liviafarris Most Recent 2 months ago

Selected Answer: AC

3 CORRECT OPTIONS: A + C + D

"Stanzas in PROPS.CONF

All data modifications in props.conf are based on either SOURCE, SOURCETYPES or HOST.

You can use wildcards (*) and regex in the source:: and host:: stanzas" <-- pg 253 Data Admin

upvoted 1 times

65aab2c 4 months, 3 weeks ago

All data modifications in props.conf are based on either source,

sourcetype, or host

Page 253

upvoted 2 times

gatundu_ 5 months, 3 weeks ago

Host, Source and Sourcetype (A,C & D) are all modifiable in props.conf

upvoted 2 times

gatundu_ 1 year, 1 month ago

Host, source and source type.

A, C & D are correct

upvoted 1 times

bobixaka 1 year, 4 months ago

Selected Answer: A

A, C and D

upvoted 1 times

Mando22 2 years, 5 months ago

A,C & D are correct.

https://docs.splunk.com/Documentation/Splunk/8.0.4/Admin/Propsconf#props.conf.spec

https://docs.splunk.com/Documentation/Splunk/8.1.1/Admin/Propsconf

upvoted 1 times

denominator 2 years, 8 months ago

Data Admin pdf, pg 205. A, C, D

upvoted 2 times

Apis 3 years, 2 months ago

Selected Answer: CD

A, C & D are correct

upvoted 3 times

loky0 3 years, 6 months ago

ACD. P206 in the new data admin pdf

upvoted 3 times

gsplunker 4 years ago

A,C,D is the correct answer

upvoted 4 times

Sandy_1988 4 years, 2 months ago

ACD are the options

upvoted 3 times

Praf7 4 years, 3 months ago

I have used source type in my env not sure about the source. Haven't used

upvoted 1 times

Toanbego 4 years, 3 months ago

I would assume it is bad practice to alter the source type at different stages. Not something that often change in my experience, haha. Would stick with A, B and D. I know those can change

upvoted 1 times

Toanbego 4 years, 3 months ago

Nevermind. Seems you are correct. Reviewing the data admin PDF shows that data modification at least has the variables for host, source and sourcetype

upvoted 3 times

Question #26 *Topic 1*

What is the correct order of steps in Duo Multifactor Authentication?

A. 1. Request Login 2. Connect to SAML server 3. Duo MFA 4. Create User session 5. Authentication Granted 6. Log into Splunk

B. 1. Request Login 2. Duo MFA 3. Authentication Granted 4. Connect to SAML server 5. Log into Splunk 6. Create User session

C. 1. Request Login 2. Check authentication / group mapping 3. Authentication Granted 4. Duo MFA 5. Create User session 6. Log into Splunk

D. 1. Request Login 2. Duo MFA 3. Check authentication / group mapping 4. Create User session 5. Authentication Granted 6. Log into Splunk

Suggested Answer: *C*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/ConfigureDuo

Community vote distribution
C (100%)

Asami Highly Voted 2 years, 8 months ago
C. 1. Request Login 2. Check authentication / group mapping 3. Authentication Granted 4. Duo MFA 5. Create User session 6. Log into Splunk
upvoted 7 times

ucsdmiami2020 1 year, 5 months ago
Using the provided DUO/Splunk reference URL https://duo.com/docs/splunk
Scroll down to the Network Diagram section and note the following 6 similar steps
1 - SPlunk connection initiated
2 - Primary authentication
3 - Splunk connection established to Duo Security over TCP port 443
4 - Secondary authentication via Duo Security's service
5 - Splunk receives authentication response
6 - Splunk session logged in
upvoted 6 times

Steve2610 Most Recent 7 months, 2 weeks ago
Selected Answer: C
System Admin - P:230
upvoted 1 times

Apis 1 year, 2 months ago
Selected Answer: C
C is correct
upvoted 1 times

BMO 1 year, 9 months ago
C is correct
System Admin - Slide 225
upvoted 1 times

Sandy_1988 2 years, 1 month ago
Yes C is the ans.
upvoted 1 times

Question #27 *Topic 1*

Where can scripts for scripted inputs reside on the host file system? (Choose all that apply.)

A. $SPLUNK_HOME/bin/scripts

B. $SPLUNK_HOME/etc/apps/bin

C. $SPLUNK_HOME/etc/system/bin

D. $SPLUNK_HOME/etc/apps/<your_app>/bin

Suggested Answer: *ACD*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Getdatafromscriptedinputs#Where_to_place_the_scripts_for_scripted_inputs

Community vote distribution
ACD (100%)

Asami Highly Voted 2 years, 8 months ago
A. $SPLUNK_HOME/bin/scripts
C. $SPLUNK_HOME/etc/system/bin
D. $SPLUNK_HOME/etc/apps/<your_app>/bin
upvoted 8 times

BMO Highly Voted 1 year, 9 months ago
ACD is correct
Data Admin - Slide 143
upvoted 5 times

ucsdmiami2020 1 year, 5 months ago
Agreed A, C, D. Quoting the provided Splunk reference URL
https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Getdatafromscriptedinputs#Where_to_place_the_scripts_for_scripted_inputs

"Where to place the scripts for scripted inputs. The script that you refer to in $SCRIPT can reside in only one of the following places on the host file system:
$SPLUNK_HOME/etc/system/bin
$SPLUNK_HOME/etc/apps/<your_App>/bin
$SPLUNK_HOME/bin/scripts
As a best practice, put your script in the bin/ directory that is nearest to the inputs.conf file that calls your script on the host file system."
upvoted 2 times

Steve2610 Most Recent 7 months, 2 weeks ago
Selected Answer: ACD
Data Admin Slide 154
upvoted 2 times

Nnatech 8 months ago
Selected Answer: ACD
ACD is correct
upvoted 1 times

denominator 8 months, 3 weeks ago
Data Admin Pg 154
upvoted 1 times

Apis 1 year, 2 months ago
Selected Answer: ACD
A, C & D are correct
upvoted 2 times

thomass 1 year, 11 months ago
answer : acd

upvoted 2 times

Question #28 *Topic 1*

How does the Monitoring Console monitor forwarders?

A. By pulling internal logs from forwarders.

B. By using the forwarder monitoring add-on.

C. With internal logs forwarded by forwarders.

D. With internal logs forwarded by deployment server.

Suggested Answer: *A*

Community vote distribution

C (100%)

Josi12 Highly Voted 3 years, 3 months ago

Best answer is C. MC, which is search head of search heads relies on internal logs forwarded by forwarders.

upvoted 17 times

ucsdmiami2020 1 year, 11 months ago

Agreed C. Quoting the following Splunk URL reference https://docs.splunk.com/Documentation/Splunk/8.2.2/DMC/DMCprerequisites

"Monitoring Console setup prerequisites. Forward internal logs (both $SPLUNK_HOME/car/log/splunk and $SPLUNK_HOME/var/log/introspection) to indexers from all other components. Without this step, many dashboards will lack data."

upvoted 2 times

Asami Highly Voted 3 years, 1 month ago

C. With internal logs forwarded by forwarders.

upvoted 6 times

uptightuptight Most Recent 4 months, 2 weeks ago

Selected Answer: C

Uses internal logs from forwarders

upvoted 3 times

Mando22 11 months, 2 weeks ago

The correct answer is C

upvoted 1 times

thissiteisgreat 1 year, 4 months ago

Selected Answer: C

C.....

upvoted 2 times

Marco63 1 year, 4 months ago

Selected Answer: C

uses internal logs from forwarders

upvoted 1 times

Apis 1 year, 8 months ago

Selected Answer: C

C is correct

upvoted 1 times

loky0 2 years ago

C. P109 Data admin pdf

upvoted 2 times

Mimi88 2 years, 11 months ago

Ans. C. See Forwarder Monitoring with Monitoring Console section of Data Administration PDF

upvoted 5 times

Sammy33 3 years, 3 months ago

Correct answer is C, based on the Data Admin Power Point from Splunk Training

upvoted 5 times

giubal 3 years, 4 months ago

I'm not really sure but the answer could be C

"The Monitoring Console dashboards use data from Splunk Enterprise's internal log files"

https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview

upvoted 5 times

Question #29 *Topic 1*

What options are available when creating custom roles? (Choose all that apply.)

A. Restrict search terms.

B. Whitelist search terms.

C. Limit the number of concurrent search jobs.

D. Allow or restrict indexes that can be searched.

Suggested Answer: *AD*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.2.6/Security/Aboutusersandroles

Community vote distribution
AC (100%)

Asami Highly Voted 4 years, 8 months ago
A. Restrict search terms.
C. Limit the number of concurrent search jobs.
D. Allow or restrict indexes that can be searched
upvoted 27 times

ucsdmiami2020 3 years, 5 months ago
Agreed A,C, D. Quoting the Splunk reference URL https://docs.splunk.com/Documentation/SplunkCloud/8.2.2106/Admin/ConcurrentLimits

"Set limits for concurrent scheduled searches. You must have the edit_search_concurrency_all and edit_search_concurrency_scheduled capabilities to configure these settings."
upvoted 4 times

Amith Highly Voted 4 years, 10 months ago
Yes C also
upvoted 9 times

gatundu_ Most Recent 4 months, 1 week ago
A,C and D
1. Restrict - restrict search terms/ limit concurrent search jobs
2. Index - Allow/ restrict indexes

Other options available: inheritance, capabilities and resources
upvoted 1 times

NashP 1 year ago
A,C,D as per sys admin pdf (P 157 158 159)
upvoted 1 times

StevenBzh 1 year, 4 months ago
Selected Answer: AC
Agreed too:
A. Restrict search terms.
C. Limit the number of concurrent search jobs.
D. Allow or restrict indexes that can be searched
upvoted 1 times

tmmt 2 years ago
is ACD
upvoted 3 times

xouu 2 years, 1 month ago
Selected Answer: AC

ACD : https://docs.splunk.com/Documentation/Splunk/latest/Security/Rolesandcapabilities
edit_search_concurrency_all :Lets a user edit settings related to maximum concurrency of searches.
upvoted 1 times

emlch 2 years, 6 months ago
ACD are the correct answer
upvoted 1 times

Apis 3 years, 2 months ago
Selected Answer: AC
A, C & D are correct
upvoted 2 times

loky0 3 years, 6 months ago
ACD. P 157 158 159 in Sys admin pdf
upvoted 2 times

ckmunich 3 years, 7 months ago
A, C, D

C because:
https://docs.splunk.com/Documentation/SplunkCloud/8.2.2106/Admin/ConcurrentLimits
upvoted 1 times

Dejavuu 3 years, 7 months ago
The answers are ACD
upvoted 1 times

hellonair 3 years, 8 months ago
C must be included. So answer is ACD
At the resources tab on creating the user, Role search job limit can be set
upvoted 1 times

Sandy_1988 4 years, 2 months ago
ACD is the options
upvoted 2 times

AbuAli 4 years, 11 months ago
C. Limit the number of concurrent search jobs. >>> is true Also
upvoted 5 times

Question #30 *Topic 1*

Which of the following are supported options when configuring optional network inputs?

A. Metadata override, sender filtering options, network input queues (quantum queues)

B. Metadata override, sender filtering options, network input queues (memory/persistent queues)

C. Filename override, sender filtering options, network output queues (memory/persistent queues)

D. Metadata override, receiver filtering options, network input queues (memory/persistent queues)

Suggested Answer: *D*

Community vote distribution

B (100%)

Asami Highly Voted 2 years, 8 months ago

B. Metadata override, sender filtering options, network input queues (memory/persistent queues)

upvoted 20 times

Steve2610 Most Recent 7 months, 2 weeks ago

Selected Answer: B

Data Admin Slide 143

upvoted 1 times

Marco63 10 months, 3 weeks ago

Selected Answer: B

See Data Admin page 141

upvoted 1 times

Apis 1 year, 2 months ago

Selected Answer: B

B is correct

upvoted 3 times

loky0 1 year, 6 months ago

B. P141 Data admin pdf

upvoted 3 times

Sandy_1988 2 years, 2 months ago

B is the answer

upvoted 2 times

Mimi88 2 years, 5 months ago

Ans. B. See Optional Network Input Settings in the Data Administration PDF

upvoted 4 times

Sapero 2 years, 5 months ago

B is the correct Answer for sure.

upvoted 2 times

ectomorph 2 years, 5 months ago

B is correct:

https://docs.splunk.com/Documentation/Splunk/latest/Data/Monitornetworkports

upvoted 2 times

Sammy33 2 years, 9 months ago

Should be B, according to the Data Admin Course ppx from Splunk

upvoted 2 times

giubal 2 years, 10 months ago

It is trick question, because on forwarder when the queue is full due to latency toward the indexer, persistent queue (writing to a file) is used and is preserves across restarts. So even the answer C could be right.

upvoted 1 times

Amith 2 years, 10 months ago

It should be B, Any one can clarify ?

upvoted 3 times

Question #31 *Topic 1*

What is the default character encoding used by Splunk during the input phase?

A. UTF-8

B. UTF-16

C. EBCDIC

D. ISO 8859

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Configurecharactersetencoding

Community vote distribution
A (100%)

liviafarris 2 months ago

Selected Answer: A
Correct answer: A
Data Admin Slide page 254:
"During the input phase, Splunk sets all input data to UTF-8 encoding
by default.
Can be overridden, if needed, by setting the CHARSET attribute.
Use AUTO to attempt automatic encoding based on language"
upvoted 2 times

emlch 6 months, 1 week ago

UTF-8 and you can change it using the CHARSET attribute
upvoted 2 times

Apis 1 year, 2 months ago

Selected Answer: A
A is correct
upvoted 2 times

loky0 1 year, 6 months ago

A. P207 Data admin pdf
upvoted 2 times

ucsdmiami2020 1 year, 5 months ago

Agreed A. Quoting the Splunk reference URL https://docs.splunk.com/Documentation/Splunk/7.3.1/Data/Configurecharactersetencoding

"Configure character set encoding. Splunk software attempts to apply UTF-8 encoding to your scources by default. If a source foesn't use UTF-8 encoding or is a non-ASCII file, Splunk software tries to convert data from the source to UTF-8 encoding unless you specify a character set to use by setting the CHARSET key in the props.conf file."
upvoted 1 times

amsinha 2 years, 1 month ago

A is True !!
upvoted 1 times

ectomorph 2 years, 5 months ago

A:

https://docs.splunk.com/Splexicon:Charactersetencoding#:~:text=A%20method%20for%20displaying%20and,conf%20configuration%20file.
upvoted 1 times

amporiik 2 years, 7 months ago

A. UTF-8
upvoted 1 times

Question #32 *Topic 1*

Which of the following enables compression for universal forwarders in outputs.conf?

A. [udpout:mysplunk_indexer11] compression=true

B. [tcpout] defaultGroup=my_indexers compressed=true

C. /opt/splunkforwarder/bin/splunk enable compression

D. [tcpount:my_indexers] server=mysplunk_indexer1:9997, mysplunk_indexer2:9997 decompression=false

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Outputsconf

Community vote distribution
B (100%)

amporiik Highly Voted 2 years, 1 month ago
B. [tcpout] defaultGroup=my_indexers compressed=true
to enable compression on UF add option compressed=true in stanza
upvoted 8 times

Apis Most Recent 8 months, 2 weeks ago
Selected Answer: B
B is correct
upvoted 1 times

loky0 1 year ago
B. P73 data admin pdf
upvoted 2 times

ucsdmiami2020 11 months, 1 week ago
Agreed B. Quoting the reference URL https://docs.splunk.com/Documentation/Splunk/latest/Admin/Outputsconf

Compression
#
This example sends compressed events to the remote indexer.
NOTE: Compression can be enabled TCP or SSL outputs only.
The receiver input port should also have compression enabled.
[tcpout]
server = splunkServer.example.com:4433
compressed = true
upvoted 4 times

gsplunker 1 year, 7 months ago
B is the ans
upvoted 1 times

ectomorph 1 year, 12 months ago
this answer = B - formatting is wonky... You could also see for SSL (shown below)
[tcpout]
defaultGroup=my_indexers
compressed=true #HTTP Only
useClientSSLCompression=true #SSL
upvoted 4 times

Question #33 *Topic 1*

User role inheritance allows what to be inherited from the parent role? (Choose all that apply.)

A. Parents

B. Capabilities

C. Index access

D. Search history

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/Aboutusersandroles#How_users_inherit_capabilities

Community vote distribution
B (75%) C (25%)

Shaq007 Highly Voted 4 years, 2 months ago
B and C are correct - checkout the "role inheritance" portion of Sys Admin PDF.
Inheritance:
- Can be based on one or more existing roles
- Provides inherited capabilities and index access
upvoted 15 times

jgab Highly Voted 4 years, 4 months ago
it could be B and C
upvoted 9 times

3bd8ac0 Most Recent 1 month ago
Selected Answer: B
B & C, Creating User Roles: Inheritance in Splunk Admin Course, page 230.
upvoted 1 times

Jactom 1 month, 3 weeks ago
Selected Answer: C
B & C are correct As per sys admin guide "The new role inherits both capabilities and index access"
upvoted 1 times

liviafarris 2 months ago
Selected Answer: C
Correct answer: B and C
System Admin PDF page 230 :
"The Inheritance:
• Can be based on one or more existing roles
• Provides inherited capabilities and index access "
upvoted 1 times

gatundu_ 4 months, 1 week ago
B and C
Inheritance allows you to inherit capabilities, index access, restrictions etc. However, these cannot be modified while using inheritance
upvoted 1 times

bobixaka 1 year, 4 months ago
Selected Answer: C
B and C
upvoted 1 times

Marco63 2 years, 10 months ago
B AND C are correct.
upvoted 2 times

king1993 2 years, 10 months ago

Answer: B and C

upvoted 2 times

Apis 3 years, 2 months ago

Selected Answer: B

B & C are correct

upvoted 3 times

malice4 3 years, 10 months ago

B and C

upvoted 3 times

newrose 4 years, 3 months ago

I think the answer is B and C: https://docs.splunk.com/Documentation/Splunk/latest/Security/Aboutusersandroles#Role_inheritance

upvoted 4 times

Question #34 *Topic 1*

Which of the following statements apply to directory inputs? (Choose all that apply.)

A. All discovered text files are consumed.

B. Compressed files are ignored by default.

C. Splunk recursively traverses through the directory structure.

D. When adding new log files to a monitored directory, the forwarder must be restarted to take them into account.

Suggested Answer: *C*
Reference:
https://answers.splunk.com/answers/133875/recursive-monitoring-of-directories.html

Community vote distribution
A (83%) C (17%)

Eku Highly Voted 4 years, 10 months ago
Answer should be A and C
upvoted 15 times

Mimi88 Highly Voted 4 years, 5 months ago
Ans. A & C. See Monitoring Directories in the Data Administration PDF
upvoted 6 times

gatundu_ Most Recent 5 months, 1 week ago
A & C are correct
upvoted 1 times

HNaka 1 year, 1 month ago
Selected Answer: C
Answer is A and C
upvoted 1 times

bobixaka 1 year, 4 months ago
Selected Answer: A
A and C
upvoted 2 times

emlch 2 years, 6 months ago
Monitoring directories: recursively traverses directory and monitors all discovered text files, unzips compressed files, includes new files added to the directories.
upvoted 1 times

Apis 3 years, 2 months ago
Selected Answer: A
A &C are correct
upvoted 4 times

akkki 4 years, 4 months ago
From where, can I download data administration pdf?
upvoted 2 times

Racgud 4 years, 3 months ago
you can't. You have to sign up and pay for the Data admin course. Then you will receive a PDF which it is illegal to share (watermarked with your name)
upvoted 13 times

Amith 4 years, 10 months ago
A and C are the answers, Most multiple answers are not selected in this site
upvoted 6 times

AbuAli 4 years, 11 months ago

I think A is True Also
upvoted 4 times

Question #35 *Topic 1*

How would you configure your distsearch.conf to allow you to run the search below? sourcetype=access_combined status=200 action=purchase splunk_server_group=HOUSTON

A. [distributedSearch:NYC] default = false servers = nyc1:8089, nyc2:8089 [distributedSearch:HOUSTON] default = false servers = houston1:8089, houston2:8089

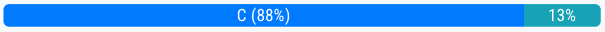
B. [distributedSearch] servers =nyc1, nyc2, houston1, houston2 [distributedSearch:NYC] default = false servers = nyc1, nyc2 [distributedSearch:HOUSTON] default = false servers = houston1, houston2

C. [distributedSearch] servers =nyc1:8089, nyc2:8089, houston1:8089, houston2:8089 [distributedSearch:NYC] default = false servers = nyc1:8089, nyc2:8089 [distributedSearch:HOUSTON] default = false servers = houston1:8089, houston2:8089

D. [distributedSearch] servers =nyc1:8089; nyc2:80893; houston1:8089; houston2:8089 [distributedSearch:NYC] default = false servers = nyc1:8089; nyc2:8089 [distributedSearch:HOUSTON] default = false servers = houston1:80897706; houston2:80898350

Suggested Answer: *B*

Community vote distribution



nottyan Highly Voted 4 years, 3 months ago

I think C is Ans.
https://docs.splunk.com/Documentation/Splunk/8.1.0/DistSearch/Distributedsearchgroups
upvoted 12 times

newrose Highly Voted 4 years, 3 months ago

In my opinion it is C:
Example from https://docs.splunk.com/Documentation/Splunk/8.1.0/DistSearch/Distributedsearchgroups:

[distributedSearch]
# This stanza lists the full set of search peers.
servers = 192.168.1.1:8089, 192.168.1.2:8089, 175.143.1.1:8089, 175.143.1.2:8089, 175.143.1.3:8089

[distributedSearch:NYC]
# This stanza lists the set of search peers in New York.
default = false
servers = 192.168.1.1:8089, 192.168.1.2:8089

[distributedSearch:SF]
# This stanza lists the set of search peers in San Francisco.
default = false
servers = 175.143.1.1:8089, 175.143.1.2:8089, 175.143.1.3:8089

And specifications from distsearch.conf:

servers = <comma-separated list>
* An initial list of servers.
* Each member of this list must be a valid URI in the format of
scheme://hostname:port
upvoted 10 times

NastyNutsu Most Recent 1 month, 2 weeks ago

Selected Answer: C
[distributedSearch]
servers = nyc1:8089, nyc2:8089, houston1:8089, houston2:8089

[distributedSearch:NYC]
default = false

servers = nyc1:8089, nyc2:8089

[distributedSearch:HOUSTON]
default = false
servers = houston1:8089, houston2:8089

B is wrong because the nyc1, nyc2, houston1, and houston2 doesn't have ports associated with them
C is the answer
upvoted 1 times

HR1234 8 months, 1 week ago

Selected Answer: C

C is Ans
upvoted 1 times

tmmt 2 years ago

Selected Answer: C

Is C, others have invalid parameter separator, port and invalid stanza for distsearch
upvoted 2 times

toney_mu 2 years ago

I would choose C
https://docs.splunk.com/Documentation/Splunk/9.0.0/DistSearch/Distributedsearchgroups
upvoted 1 times

Steve2610 2 years, 7 months ago

Selected Answer: B

B I think
upvoted 1 times

Marco63 2 years, 10 months ago

Selected Answer: C

see https://docs.splunk.com/Documentation/Splunk/8.0.3/DistSearch/Distributedsearchgroups
The servers attribute lists groups of search peers by IP address and management port.
The servers list for each search group must be a subset of the list in the general [distributedSearch] stanza.
upvoted 2 times

rafiki31 2 years, 11 months ago

A is also correct to me:
"the full set of search peers in the [distributedSearch] stanza will be queried when the search does not specify a search group."
https://docs.splunk.com/Documentation/Splunk/8.1.0/DistSearch/Distributedsearchgroups

Here the search specifies the search group
upvoted 1 times

Apis 3 years, 2 months ago

Selected Answer: C

C is correct
upvoted 2 times

ArDeKu 3 years, 11 months ago

The answer is C..
Refer link - https://docs.splunk.com/Documentation/Splunk/8.0.3/DistSearch/Distributedsearchgroups
upvoted 3 times

boruilei 4 years, 4 months ago

i think d is ans
upvoted 1 times

Ashton_98 4 years, 3 months ago

100% not D. You can't have ports over 65,535.
upvoted 2 times

AngusBlack 3 years, 8 months ago

Plus they are supposed to be comma separated, not colons

upvoted 1 times

Question #36 *Topic 1*

Which of the following is a valid distributed search group?

A. [distributedSearch:Paris] default = false servers = server1, server2

B. [searchGroup:Paris] default = false servers = server1:8089, server2:8089

C. [searchGroup:Paris] default = false servers = server1:9997, server2:9997

D. [distributedSearch:Paris] default = false servers = server1:8089; server2:8089

Suggested Answer: *D*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/Distributedsearchgroups

Community vote distribution
D (100%)

giubal Highly Voted 3 years, 4 months ago
I'm sorry ... D is wrong separator is ';' (not permitted) instead ','
upvoted 10 times

AngusBlack 2 years, 2 months ago
It's true. They are all wrong.
upvoted 2 times

toney_mu 6 months, 3 weeks ago
I think its a typo, option D would be the closet
upvoted 3 times

Asami Highly Voted 3 years, 1 month ago
D. [distributedSearch:Paris] default = false servers = server1:8089; server2:8089
upvoted 5 times

ames 3 years ago
But the separator is incorrect
upvoted 5 times

nechococo Most Recent 3 weeks, 3 days ago
Selected Answer: D
[distributedSearch:NYC]
# This stanza lists the set of search peers in New York.
default = false
servers = 192.168.1.1:8089, 192.168.1.2:8089
upvoted 1 times

3bd8ac0 4 weeks, 1 day ago
Selected Answer: B
The correct answer is: B. [searchGroup:Paris] default = false servers = server1:8089, server2:8089

Explanation:

In Splunk, to configure distributed search groups, you must use the correct stanza format and port configuration in the distsearch.conf file. The valid configuration follows these rules:

Stanza: [searchGroup:<group_name>]
default: Specifies whether the group is the default search group.
servers: Lists search peers with their management ports (default port is 8089) separated by commas.

Therefore, B correctly follows this format with the stanza [searchGroup:Paris], default set to false, and servers listed with the proper port (8089).
upvoted 1 times

tmmt 6 months, 3 weeks ago

Is D but the separator in incorrect

upvoted 1 times

toney_mu 6 months, 3 weeks ago

as per latest splunk document https://docs.splunk.com/Documentation/Splunk/9.0.0/DistSearch/Distributedsearchgroups

option is D

upvoted 1 times

huu_nguyen 1 year, 7 months ago

Selected Answer: D

D is the answer but there's a typo in the answer. It should be ',' not ';'

upvoted 3 times

huu_nguyen 1 year, 7 months ago

Selected Answer: D

D is the answer

https://docs.splunk.com/Documentation/Splunk/8.2.4/Admin/Distsearchconf

upvoted 2 times

Apis 1 year, 8 months ago

Selected Answer: D

D is the correct answer, however with a typo

I checked and you have to provide port number, otherwise you get the following error:

Failed to parse uri for peer:Paris. This search peer will be ignored.

upvoted 1 times

M9201715 1 year, 9 months ago

B and C are definitely wrong. A is not correct since no port number is given, and that is required. See https://docs.splunk.com/Documentation/Splunk/8.0.6/Admin/Distsearchconf Distributed Search Group Definitions:

servers = <comma-separated list>

* A list of search peers that are members of this group.

* The list must use peer identifiers (i.e. hostname:port)

Answer D must be a typo, and supposed to show a comma and not a semi colon. In that case it is correct.

upvoted 2 times

L4Best 2 years, 2 months ago

It is A, read the documentation : "The servers attribute lists groups of search peers by IP address and management port" , so a server always contains already a port, it is not listed as a seperate attribute.

upvoted 1 times

ArDeKu 2 years, 5 months ago

The answer is B..

Refer link - https://docs.splunk.com/Documentation/Splunk/8.0.3/DistSearch/Distributedsearchgroups

upvoted 1 times

Shaq007 2 years, 8 months ago

I just tested this and a port is required. So, with given choices I would go with D

upvoted 3 times

newrose 2 years, 9 months ago

distsearch.conf specification says:

servers = <comma-separated list>

* An initial list of servers.

* Each member of this list must be a valid URI in the format of

scheme://hostname:port

I haven't tested, but in my understanding the port value is needed, and in that case it couldn't be alternative A. The separator ";" in alternative D makes it wrong too (maybe a test typo?), although it certainly would be the correct one if the separator was a comma.

upvoted 2 times

dpharker 2 years, 11 months ago

A is the correct one

correct stanza name -> [distributedSearch:xxxx]

correct separator -> ,

servers listed don't need to have the port defined, and Splunk will use the default attribute listed in distsearch.conf.spec

https://docs.splunk.com/Documentation/Splunk/8.0.6/Admin/Distsearchconf#distsearch.conf.example

upvoted 4 times

Josi12 3 years, 3 months ago

The correct answer is D. The stanza is <DS1_IP:8089>, <DS2_IP:8089>,....

upvoted 3 times

giubal 3 years, 4 months ago

I think it is "D"

<<The servers attribute lists groups of search peers by IP address and management port>>

upvoted 3 times

Question #37 *Topic 1*

Local user accounts created in Splunk store passwords in which file?

A. $SPLUNK_HOME/etc/passwd

B. $SPLUNK_HOME/etc/authentication

C. $SPLUNK_HOME/etc/users/passwd.conf

D. $SPLUNK_HOME/etc/users/authentication.conf

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/User-seedconf

Community vote distribution
A (100%)

Asami Highly Voted 2 years, 1 month ago
A. $SPLUNK_HOME/etc/passwd
upvoted 10 times

ucsdmiami2020 11 months, 2 weeks ago
Per the provided reference URL https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/User-seedconf
"To set the default username and password, place user-seed.conf in $SPLUNK_HOME/etc/system/local. You must restart Splunk to enable configurations. If the $SPLUNK_HOME/etc/passwd file is present, the settings in this file (user-seed.conf) are not used."
upvoted 1 times

Bob_Hob 1 month, 1 week ago
As a current splunk admin - the answer would be A. But I see where you are coming from with the user-seed. It is just meant to be temporary though
upvoted 1 times

Apis Most Recent 8 months, 2 weeks ago
Selected Answer: A
A is correct
upvoted 3 times

Question #38 *Topic 1*

For single line event sourcetypes, it is most efficient to set SHOULD_LINEMERGE to what value?

A. True

B. False

C. <regex string>

D. Newline Character

Suggested Answer: *B*
Reference:
https://answers.splunk.com/answers/704533/what-are-the-best-practices-for-defining-source-ty.html

Community vote distribution
B (100%)

amporiik Highly Voted 4 years, 7 months ago
B. False
upvoted 6 times

ucsdmiami2020 3 years, 5 months ago
Agreed B. Quoting the Splunk reference URL https://docs.splunk.com/Documentation/Splunk/latest/Data/Configureeventlinebreaking

Attribute : SHOULD_LINEMERGE = [true|false]

Description : When set to true, the Splunk platform combines several input lines into a single event, with configuration based on the settings described in the next section.

Default : true
upvoted 1 times

gatundu_ Most Recent 5 months, 1 week ago
SHOULD_LINEMERGE=false in order to improve efficiency. By deafult it is set to true
upvoted 1 times

Apis 3 years, 2 months ago
Selected Answer: B
B is correct
upvoted 1 times

mikey_76 3 years, 5 months ago
If it's a single line event, then SHOULD_LINEMERGE is set to False
upvoted 2 times

Question #39 *Topic 1*

Which Splunk component does a search head primarily communicate with?

A. Indexer

B. Forwarder

C. Cluster master

D. Deployment server

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/InheritedDeployment/Deploymenttopology

Community vote distribution
A (100%)

amporiik Highly Voted 4 years, 7 months ago
A. Indexer
upvoted 9 times

ucsdmiami2020 3 years, 5 months ago
Per the provided Splunk URL reference https://docs.splunk.com/Documentation/Splunk/7.3.1/InheritedDeployment/Deploymenttopology "Search heads manage searches. They handle search requests from user and distribute the requests across the set of indexers, which search their local data. The search head then consolidates the results from all of the indexers and serves them to the users."
upvoted 2 times

rafiki31 Most Recent 2 years, 11 months ago
Ambiguous, It also could be the Cluster master, depending if we are adding a SH for the first time or we're just running a search...
upvoted 1 times

Bob_Hob 1 month, 1 week ago
Agreed. I only would default to indexer because that is where I see the most errors in the logs lol
upvoted 1 times

b997bd0 4 months, 4 weeks ago
Yes you are correct, but in this case not mention the distributed environment, i think that's why dirrect to indexers
upvoted 1 times

Apis 3 years, 2 months ago
Selected Answer: A
A is correct
upvoted 2 times

Question #40 *Topic 1*

Which layers are involved in Splunk configuration file layering? (Choose all that apply.)

A. App context

B. User context

C. Global context

D. Forwarder context

Suggested Answer: *ABC*

Community vote distribution

ABC (100%)

newrose Highly Voted 2 years, 9 months ago

ABC seems right to me

upvoted 12 times

toney_mu Most Recent 6 months, 3 weeks ago

A,b and C

=====

•In case of conflicts, priority is based on the context:

- Global context (index-time)

-App/User context (search-time)

===

upvoted 2 times

Apis 1 year, 8 months ago

Selected Answer: ABC

A, B & C are correct

upvoted 2 times

ckmunich 2 years ago

A B Cf

C: About configuration file context

To determine the order of directories for evaluating configuration file precedence, Splunk software considers each file's context. Configuration files operate in either a global context or in the context of the current app and user:

Global. Activities like indexing take place in a global context. They are independent of any app or user. For example, configuration files that determine monitoring or indexing behavior occur outside of the app and user context and are global in nature.

App/user. Some activities, like searching, take place in an app or user context. The app and user context is vital to search-time processing, where certain knowledge objects or actions might be valid only for specific users in specific apps.

upvoted 4 times

lona 2 years, 5 months ago

The answer are A B C.

reference link is below

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Wheretofindtheconfigurationfiles

upvoted 3 times

sargeholik 2 years, 5 months ago

AB seems right to me

upvoted 1 times

ucsdmiami2020 1 year, 11 months ago

You forgot C.

upvoted 1 times

Question #41 *Topic 1*

Which of the following are methods for adding inputs in Splunk? (Choose all that apply.)

A. CLI

B. Splunk Web

C. Editing inpits.conf

D. Editing monitor.conf

Suggested Answer: *AB*
Reference:
http://dev.splunk.com/view/dev-guide/SP-CAAAE3A

Community vote distribution
AB (100%)

tmmt 6 months, 3 weeks ago
ABC if C have was inputs.conf
upvoted 3 times

Apis 1 year, 8 months ago
Selected Answer: AB
A & B for sure
C assuming it is a typo
upvoted 4 times

sargeholik 2 years, 8 months ago
A and B
upvoted 4 times

Ashton_98 2 years, 10 months ago
AB and C.
upvoted 1 times

Toanbego 2 years, 9 months ago
Really depends if C is mispelled or not. If it is supposed to be inputs.conf, then i agree. Else i would stay away :P
upvoted 12 times

Ashton_98 2 years, 9 months ago
Good spotting! Attention to detail is the real challenge with these questions.
upvoted 1 times

ucsdmiami2020 1 year, 11 months ago
Agreed A,B,C (assuming its a typo, inputs.conf). Quoting the Splunk Reference URL
https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/Configureyourinputs

Add your data to Splunk Enterprise. With Splunk Enterprise, you can add data using Splunk Web or Splunk Apps. In addition to these methods, you also can use the following methods.
-The Splunk Command Line Interface (CLI)
-The inputs.conf configuration file. When you specify your inputs with Splunk Web or the CLI, the details are saved in a configuartion file on Splunk Enterprise indexer and heavy forwarder instances.
upvoted 2 times

Question #42 *Topic 1*

Which of the following authentication types requires scripting in Splunk?

A. ADFS

B. LDAP

C. SAML

D. RADIUS

Suggested Answer: *D*
Reference:
https://answers.splunk.com/answers/131127/scripted-authentication.html

Community vote distribution
D (100%)

Josi12 Highly Voted 2 years, 3 months ago
RADIUS, PAM, Kerberos, TACACS+ support script authentication
upvoted 6 times

ucsdmiami2020 11 months, 2 weeks ago
Using Splunk Splexicon reference URL https://docs.splunk.com/Splexicon:Scriptedauthentication
Scripted Authentication: An option for Splunk Enterprise authentication. You can use an authentication system that you have in place (such as PAM or RADIUS) by configuring authentication.conf to use a script instead of using LDAP or Splunk Enterprise default authentication.
upvoted 2 times

Galtermedia Most Recent 1 week ago
Selected Answer: D
The question should be reworded to which authentication method supports scripting, not requires.
upvoted 1 times

RedYeti 5 months, 2 weeks ago
D. RADIUS
upvoted 4 times

Apis 8 months, 2 weeks ago
Selected Answer: D
D is correct
upvoted 1 times

haneeka 2 years ago
D should be the answer
Reference: https://answers.splunk.com/answers/131127/scripted-authentication.html
upvoted 4 times

AbuAli 2 years, 5 months ago
Also, PAM using scripted
upvoted 3 times

Question #43 *Topic 1*

Which option accurately describes the purpose of the HTTP Event Collector (HEC)?

A. A token-based HTTP input that is secure and scalable and that requires the use of forwarders.

B. A token-based HTTP input that is secure and scalable and that does not require the use of forwarders.

C. An agent-based HTTP input that is secure and scalable and that does not require the use of forwarders.

D. A token-based HTTP input that is insecure and non-scalable and that does not require the use of forwarders.

Suggested Answer: *B*

Reference:

http://dev.splunk.com/view/event-collector/SP-CAAAE6M

Community vote distribution

B (100%)

Asami Highly Voted 2 years, 1 month ago

B. A token-based HTTP input that is secure and scalable and that does not require the use of forwarders.

upvoted 13 times

ucsdmiami2020 11 months, 1 week ago

Agreed B. Quoting the Splunk Reference URL https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/UsetheHTTPEventCollector

"The HTTP Event Collector (HEC) lets you send data and application events to a Splunk deployment over the HTTP and Secure HTTP (HTTPS) protocols. HEC uses a token-based authentication model. You can generate a token and then configure a logging library or HTTP client with the token to send data to HEC in a specific format. This process eliminates the need for a Splunk forwarder when you send application events."

upvoted 2 times

Apis Most Recent 8 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 2 times

gsplunker 1 year, 7 months ago

I would go with B

upvoted 3 times

Question #44 *Topic 1*

What is the difference between the two wildcards ... and * for the monitor stanza in inputs.conf?

A. ... is not supported in monitor stanzas.

B. There is no difference, they are interchangeable and match anything beyond directory boundaries.

C. * matches anything in that specific directory path segment, whereas ... recurses through subdirectories as well.

D. ... matches anything in that specific directory path segment, whereas * recurses through subdirectories as well.

Suggested Answer: *C*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.0/Data/Specifyinputpathswithwildcards

Community vote distribution
C (100%)

Asami Highly Voted 2 years, 1 month ago
C. * matches anything in that specific directory path segment, whereas ... recurses through subdirectories as well.
upvoted 12 times

ucsdmiami2020 11 months, 2 weeks ago
Per the provided Reference URL https://docs.splunk.com/Documentation/Splunk/7.3.0/Data/Specifyinputpathswithwildcards

... The ellipsis wildcard searches recursively through directories and any number of levels of subdirectories to find matches.
If you specify a folder separator (for example, //var/log/.../file), it does not match the first folder level, only subfolders.

* The asterisk wildcard matches anything in that specific folder path segment.
Unlike ..., * does not recurse through subfolders.
upvoted 3 times

Apis Most Recent 8 months, 2 weeks ago
Selected Answer: C
C is correct
upvoted 2 times

Question #45 *Topic 1*

What type of data is counted against the Enterprise license at a fixed 150 bytes per event?

A. License data

B. Metrics data

C. Internal Splunk data

D. Internal Windows logs

Suggested Answer: *B*
Reference:
https://answers.splunk.com/answers/581441/how-is-the-splunk-license-measured.html

Community vote distribution
B (100%)

amporiik Highly Voted 2 years, 1 month ago
B. Metrics data
upvoted 12 times

Ailen_Man Highly Voted 3 months, 3 weeks ago
For metrics data, each metric event counts as a fixed 150 bytes. Metrics data does not use a separate license. Rather, it draws from the same license quota as event data. So B is correct
upvoted 5 times

3bd8ac0 Most Recent 4 weeks ago
Selected Answer: B
B is correct.
from Splunk data Admin official course, page 99:
"Events are measured as the data (full size) that flows through the parsing pipeline per day. Metrics measurement is capped at 150 bytes per metric event. Both types of data input draw from the same license quota."
upvoted 1 times

Apis 8 months, 2 weeks ago
Selected Answer: B
B is correct
upvoted 3 times

Bianchi 1 year ago
B. Metrics. Pag: 46 from System Admin PDF
upvoted 4 times

Question #46 *Topic 1*

Which valid bucket types are searchable? (Choose all that apply.)

A. Hot buckets

B. Cold buckets

C. Warm buckets

D. Frozen buckets

Suggested Answer: *ABC*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/HowSplunkstoresindexes

Community vote distribution
ABC (100%)

newrose Highly Voted 2 years, 9 months ago
A B C indeed
upvoted 8 times

ucsdmiami2020 1 year, 11 months ago
Agreed A, B, C. Quoting the Splunk reference URL https://docs.splunk.com/Documentation/Splunk/8.2.2/Indexer/Bucketsandclusters?

"A hot bucket is a bucket that's still being written to. When an indexer finishes writing to a hot bucket (for example, because the bucket reaches a maximum size), it rolls the bucket to warm and begins writing to a new hot bucket. Warm buckets are readable (for example, for searching) but the indexer does not write new data to them. Eventually, a bucket rolls to cold and then to frozen, at which point it gets archived or deleted.
Searches occur across hot, warm, and cold buckets.
upvoted 2 times

adamsca Most Recent 5 months ago
Selected Answer: ABC
I agree,ABC
upvoted 2 times

kolaturka 5 months, 1 week ago
Hot, cold, and warm buckets are all searchable in Splunk, whereas frozen buckets are not searchable.

Hot buckets contain recently indexed data and are actively being written to by the indexer. Warm buckets contain data that has been rolled from hot buckets and is no longer being actively written to, but is still available for search. Cold buckets contain data that has been rolled from warm buckets and is not currently in use, but is still available for search. Frozen buckets contain data that has been rolled from cold buckets and is no longer searchable, but is retained for long-term storage or compliance purposes.

In general, only hot and warm buckets are actively queried during typical Splunk searches. Cold and frozen buckets are used for long-term storage and are generally accessed less frequently.
upvoted 2 times

Apis 1 year, 8 months ago
Selected Answer: ABC
A, B & C are correct
upvoted 1 times

mikey_76 1 year, 11 months ago
The frozen bucket cannot be searched it needs to be thawed which places it back into cold. So it's A, B and C
upvoted 3 times

Question #47 *Topic 1*

How do you remove missing forwarders from the Monitoring Console?

A. By restarting Splunk.

B. By rescanning active forwarders.

C. By reloading the deployment server.

D. By rebuilding the forwarder asset table.

Suggested Answer: *D*
Reference:
https://answers.splunk.com/answers/447096/how-to-remove-missing-forwarders-from-the-distribu.html

Community vote distribution
D (100%)

ames Highly Voted 2 years ago
D is correct. More info here
<https://docs.splunk.com/Documentation/Splunk/7.3.1/DMC/Configureforwardermonitoring#Rebuild_the_forwarder_asset_table>
upvoted 7 times

ucsdmiami2020 11 months, 2 weeks ago
Agreed D. Quoting the reference URL

"The data in the forwarder asset table are cumulative. If a forwarder connects to an indexer, its record exists in the table. Then if you later remove the forwarder from your deployment, the forwarder's record is not removed from the asset table. It is instead marked "missing" in the asset table, and it still appears in the DMC forwarder dashboards. To remove a forwarder entirely from the DMC dashboards, click rebuild forwarder assets ...
upvoted 3 times

Apis Most Recent 8 months, 2 weeks ago
Selected Answer: D
D is correct
upvoted 2 times

Question #48 *Topic 1*

Which Splunk indexer operating system platform is supported when sending logs from a Windows universal forwarder?

A. Any OS platform.

B. Linux platform only.

C. Windows platform only.

D. None of the above.

Suggested Answer: *D*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.2/Installation/Systemrequirements#Supported_OSes

Community vote distribution
A (100%)

giubal Highly Voted 4 years, 10 months ago
As per "data administrator" pdf about windows input
"–Data can be forwarded to any Splunk indexer on any OS platform"
upvoted 16 times

Bianchi 3 years, 6 months ago
Yup, Pag: 185
upvoted 3 times

Josi12 Highly Voted 4 years, 9 months ago
The answer is A. Regardless of the OS host the forwarder/indexer; from the forwarder box configure IP address of the indexer(s) and replication port 9997.
upvoted 9 times

samsam5136431 Most Recent 8 months ago
Selected Answer: A
Data can be forwarded to any Splunk indexer on any OS platform
upvoted 1 times

yybbb 1 year, 1 month ago
Selected Answer: A
Data can be forwarded to any Splunk indexer on any OS platform
upvoted 1 times

royjn1981 3 years ago
Selected Answer: A
As per "data administrator" pdf about windows input
"–Data can be forwarded to any Splunk indexer on any OS platform"
upvoted 1 times

Apis 3 years, 2 months ago
Selected Answer: A
A is correct
upvoted 2 times

lollo1234 3 years, 11 months ago
A is correct. Never use a windows deployment-server to manage Linux hosts, it's unsupported
upvoted 3 times

Shaq007 4 years, 2 months ago
A. Any OS platform.
upvoted 3 times

Praf7 4 years, 3 months ago
Option A is correct

upvoted 5 times

ames 4 years, 6 months ago

I think the UF has to be Windows specific for windows events/inputs but indexer can run any OS platform

upvoted 1 times

AbuAli 4 years, 11 months ago

This question is tricky

It's not B & C

A is confusing its support all OS (within the sphere of supported platforms)

So it's could be D but I will go with A

See below link for more details

https://answers.splunk.com/answers/153612/what-is-the-best-way-to-get-data-from-a-linux-forwarder-to-a-windows-indexer.html

upvoted 4 times

ucsdmiami2020 3 years, 5 months ago

Agreed A. Quoting the provided Splunk Reference URL

"The forwarder/indexer relationship can be considered platform agnostic (within the sphere of supported platforms) because they exchange their data handshake (and the data, if you wish) over TCP.

upvoted 1 times

Question #49 *Topic 1*

What are the required stanza attributes when configuring the transforms.conf to manipulate or remove events?

A. REGEX, DEST, FORMAT

B. REGEX, SRC_KEY, FORMAT

C. REGEX, DEST_KEY, FORMAT

D. REGEX, DEST_KEY, FORMATTING

Suggested Answer: *C*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/Transformsconf

Community vote distribution
C (100%)

amporiik Highly Voted 2 years, 1 month ago
C. REGEX, DEST_KEY, FORMAT
upvoted 9 times

ucsdmiami2020 11 months, 1 week ago
Agreed C. Doing a Ctrl+F within the Splunk reference URL https://docs.splunk.com/Documentation/Splunk/latest/Admin/Transformsconf

REGEX = <regular expression>
* Enter a regular expression to operate on your data.

FORMAT = <string>
* NOTE: This option is valid for both index-time and search-time field extraction. Index-time field extraction configuration require the FORMAT settings. The FORMAT settings is optional for search-time field extraction configurations.
* This setting specifies the format of the event, including any field names or values you want to add.

DEST_KEY = <key>
* NOTE: This setting is only valid for index-time field extractions.
* Specifies where SPLUNK software stores the expanded FORMAT results in accordance with the REGEX match.
upvoted 2 times

Apis Most Recent 8 months, 2 weeks ago
Selected Answer: C
C is correct
upvoted 1 times

DeltaPotato 1 year ago
Confirming C. - Data Admin pdf, page 240-241. When SOURCE_KEY is omitted, _raw is used as default.
upvoted 1 times

ames 2 years ago
Latest version https://docs.splunk.com/Documentation/Splunk/latest/Admin/Transformsconf
upvoted 1 times

Question #50 *Topic 1*

Which of the following indexes come pre-configured with Splunk Enterprise? (Choose all that apply.)

A. _licence

B. _internal

C. _external

D. _thefishbucket

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Howindexingworks

Community vote distribution
B (85%) D (15%)

ChantreyC Highly Voted 4 years, 1 month ago
B & D - pg 95 SysAdmin pdf
upvoted 8 times

Sandy_1988 Highly Voted 4 years, 1 month ago
BD are the options
upvoted 6 times

3bd8ac0 Most Recent 4 weeks ago
Selected Answer: B
B&D are correct as per the System Admin official Course:
Preconfigured Indexes list:

Index name Purpose
_internal To index Splunk's own logs and metrics

_audit To store Splunk audit trails and other optional auditing information

_introspection To track system performance, Splunk resource usage data, and provide Monitoring Console (MC) with performance data

_thefishbucket To contain checkpoint information for file monitoring inputs

summary Default index for summary indexing system

main Default index for inputs; located in the defaultdb directory
upvoted 1 times

3bd8ac0 1 month ago
Selected Answer: D
B&D, System admin course, page 171.
Preconfigured Indexes:

_internal To index Splunk's own logs and metrics

_audit To store Splunk audit trails and other optional auditing information

_introspection To track system performance, Splunk resource usage data,
and provide Monitoring Console (MC) with performance data

_thefishbucket To contain checkpoint information for file monitoring inputs
summary Default index for summary indexing system
main Default index for inputs; located in the defaultdb directory

upvoted 1 times

MonicaKarim 1 month, 3 weeks ago

Selected Answer: B

B&D choose all that apply

upvoted 1 times

65aab2c 4 months, 3 weeks ago

Index name Purpose
_internal To index Splunk's own logs and metrics
_audit To store Splunk audit trails and other optional
auditing information
_introspection To track system performance, Splunk resource usage data,
and provide Monitoring Console (MC) with performance data
_thefishbucket To contain checkpoint information for file monitoring inputs
summary Default index for summary indexing system
main Default index for inputs; located in the defaultdb directory

upvoted 2 times

samsam5136431 8 months ago

Selected Answer: D

B and D

upvoted 1 times

allahsal 1 year ago

Selected Answer: B

B and D

upvoted 2 times

HNaka 1 year, 1 month ago

Selected Answer: D

B and D

_internal
To index Splunk's own logs and metrics
_audit
To store Splunk audit trails and other optional auditing information
_introspection
To track system performance, Splunk resource usage data, and provide Monitoring Console (MC) with performance data
_thefishbucket
To contain checkpoint information for file monitoring inputs
summary
Default index for summary indexing system
main
Default index for inputs; located in the defaultdb directory

upvoted 1 times

adamsca 1 year, 11 months ago

B & D are correct

upvoted 1 times

oswaldek 2 years, 2 months ago

Selected Answer: B

_thefishbucket looks decommitted
https://community.splunk.com/t5/Splunk-Search/How-do-I-activate-quot-thefishbucket-quot-index/m-p/410263

upvoted 2 times

Steve2610 2 years, 7 months ago

Selected Answer: B

B and D
System Admin Slide 105

upvoted 3 times

huu_nguyen 3 years ago

B and D are my final answers
upvoted 5 times

Apis 3 years, 2 months ago

Selected Answer: B

B & D are correct
upvoted 4 times

lilsem 3 years, 6 months ago

B, D are the correct answer. After installing Splunk 8.2 on my local machine I checked the default indexes.conf, and there is the fishbucket index configured.
upvoted 3 times

ucsdmiami2020 3 years, 5 months ago

Agreed B and D. Quoting the Splunk Reference URL https://www.splunk.com/en_us/blog/tips-and-tricks/what-is-this-fishbucket-thing.html

"t's time for a little Indexing 101. If you look in the directory where your Splunk datastore resides (default location /opt/splunk/var/lib/splunk) you will find a directory called fishbucket. This index is not really intended for normal humans to investigate, more just Splunk engineers trying to decipher file input issues. It contains seek pointers and CRCs for the files you are indexing, so splunkd can tell if it has read them already. To see what's there, try searching for "index=_thefishbucket". Events look something like this:"
upvoted 1 times

furiousjase 3 years, 6 months ago

I believe the only answer is B.

The other preconfigured indexes are:
main: The default Splunk Enterprise index. All processed external data is stored here unless otherwise specified.
_internal: This index includes Splunk Enterprise internal logs.
_metrics: This index contains Splunk Enterprise internal data, stored in the form of metric data points.
_audit: Events from the file system change monitor, auditing, and all user search history.
_introspection: This index provides data about the Splunk Enterprise instance and environment .

https://docs.splunk.com/Documentation/Splunk/8.2.2/Indexer/Aboutmanagingindexes
upvoted 2 times

SasnycoN 3 years, 3 months ago

_thefishbucket is also preconfigured. Just checked on my installation.
Can confirm B and D
upvoted 1 times

rodrigok 3 years, 11 months ago

B & D sounds better
upvoted 4 times

Question #51 *Topic 1*

How often does Splunk recheck the LDAP server?

A. Every 5 minutes.

B. Each time a user logs in.

C. Each time Splunk is restarted.

D. Varies based on LDAP_refresh setting.

Suggested Answer: *D*
Reference:
http://docshare02.docshare.tips/files/22651/226514302.pdf

Community vote distribution
B (100%)

giubal Highly Voted 4 years, 4 months ago
I think the correct answer is B
upvoted 11 times

Vidomina Most Recent 6 months, 2 weeks ago
Selected Answer: B
The LDAP server is rechecked each time a user logs into Splunk
upvoted 2 times

toney_mu 1 year, 6 months ago
Answer would be B for sure, but if there and multiple choice D is also an option
upvoted 1 times

Marco63 2 years, 4 months ago
Selected Answer: B
See appendix on Data Admin slides
upvoted 3 times

Marco63 2 years, 4 months ago
System Admin, sorry.
upvoted 1 times

Apis 2 years, 8 months ago
Selected Answer: B
B is correct
upvoted 3 times

Pratik18 3 years ago
answer is B Page number 223 sys admin pdf
upvoted 2 times

CCSHAO 3 years, 1 month ago
B is correct. Sys Admin - Appendix A Splunk Authentication Management. Slide 218.
upvoted 4 times

Marco63 2 years, 4 months ago
Confirm. See the appendix.
upvoted 1 times

ArDeKu 3 years, 5 months ago
It will be B..Page 218 of System Admin..
upvoted 3 times

mybox1 3 years, 8 months ago
"– The LDAP server is rechecked each time a user logs into Splunk" (System Administration PDF, page 237), so answer B is correct one
upvoted 2 times

dpharker 3 years, 11 months ago

correct answer is B

this doc describe how it works.

https://docs.splunk.com/Documentation/Splunk/8.0.6/Security/ManageSplunkuserroleswithLDAP

upvoted 2 times

Amith 4 years, 4 months ago

B lah bro this one

upvoted 3 times

japm 4 years, 4 months ago

I've check on Splunk Administrator pdf and you are right giubal

upvoted 2 times

Question #52 *Topic 1*

Where are license files stored?

A. $SPLUNK_HOME/etc/secure

B. $SPLUNK_HOME/etc/system

C. $SPLUNK_HOME/etc/licenses

D. $SPLUNK_HOME/etc/apps/licenses

Suggested Answer: *C*

Reference:

https://docs.splunk.com/Documentation/Splunk/7.3.1/Admin/LicenserCLIcommands

Community vote distribution

C (100%)

amporiik Highly Voted 3 years, 1 month ago

C. $SPLUNK_HOME/etc/licenses

upvoted 11 times

tmmt Most Recent 6 months, 3 weeks ago

Is C, /etc/licenses, because you can have multiple licenses in stack.

upvoted 1 times

Apis 1 year, 8 months ago

Selected Answer: C

C is correct

upvoted 2 times

Question #53 *Topic 1*

In which scenario would a Splunk Administrator want to enable data integrity check when creating an index?

A. To ensure that hot buckets are still open for writers and have not been forced to roll to a cold state.

B. To ensure that configuration files have not been tampered with for auditing and/or legal purposes.

C. To ensure that user passwords have not been tampered with for auditing and/or legal purposes.

D. To ensure that data has not been tampered with for auditing and/or legal purposes.

Suggested Answer: *D*

Reference:

https://www.splunk.com/blog/2015/10/28/data-integrity-is-back-baby.html

Community vote distribution

D (100%)

ames Highly Voted 3 years ago

True D

upvoted 13 times

toney_mu Most Recent 6 months, 3 weeks ago

Option D.

This is mentioned in sysadmin pdf

upvoted 3 times

akrmmar 1 year ago

D is correct

upvoted 1 times

Apis 1 year, 8 months ago

Selected Answer: D

D is correct

upvoted 4 times

Question #54 *Topic 1*

Which Splunk component performs indexing and responds to search requests from the search head?

A. Forwarder

B. Search peer

C. License master

D. Search head cluster

Suggested Answer: *B*
Reference:
https://www.edureka.co/blog/splunk-architecture/

Community vote distribution
B (100%)

ames Highly Voted 4 years ago
True, B. <https://docs.splunk.com/Splexicon:Searchpeer>
upvoted 11 times

ucsdmiami2020 2 years, 11 months ago
Per the Splunk provided URL reference
"A Splunk platform instance that responses to search requests from a search head. The term "Search peer" is usually synonymous with the indexer role in a distributed search topology..."
upvoted 2 times

amporiik Highly Voted 4 years, 1 month ago
B. Search peer
upvoted 5 times

k_alex Most Recent 8 months, 3 weeks ago
Search peer is another name of the indexer
upvoted 3 times

Apis 2 years, 8 months ago
Selected Answer: B
B is correct
upvoted 2 times

1M4hqQ9G 2 years, 12 months ago
search peer a.k.a. indexer
upvoted 1 times

Question #55 *Topic 1*

When deploying apps, which attribute in the forwarder management interface determines the apps that clients install?

A. App Class

B. Client Class

C. Server Class

D. Forwarder Class

Suggested Answer: *C*

Reference:

https://docs.splunk.com/Documentation/Splunk/7.3.1/Updating/Createdeploymentapps

Community vote distribution

C (100%)

ames Highly Voted 3 years ago

True, C.

<https://docs.splunk.com/Documentation/Splunk/8.0.6/Updating/Deploymentserverarchitecture>

<https://docs.splunk.com/Splexicon:Serverclass>

upvoted 9 times

tmmt Most Recent 6 months, 3 weeks ago

Selected Answer: C

C, server class > host list > app list

upvoted 2 times

Apis 1 year, 8 months ago

Selected Answer: C

C is correct

upvoted 1 times

Question #56 *Topic 1*

In this sourcetype definition the MAX_TIMESTAMP_LOOKAHEAD is missing. Which value would fit best?
[sshd_syslog]
TIME_PREFIX = ^
TIME_FORMAT = %Y-%m-%d %H:%M:%S.%3N %z
LINE_BREAKER = ([\r\n]+)\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2}

SHOULD_LINEMERGE = false -

TRUNCATE = 0 -
Event example:
2018-04-13 13:42:41.214 -0500 server sshd[26219]: Connection from 172.0.2.60 port 47366

A. MAX_TIMESTAMP_LOOKAHEAD = 5

B. MAX_TIMESTAMP_LOOKAHEAD = 10

C. MAX_TIMESTAMP_LOOKAHEAD = 20

D. MAX_TIMESTAMP_LOOKAHEAD = 30

Suggested Answer: *B*

Community vote distribution

D (100%)

AbuAli Highly Voted 3 years, 11 months ago
D. MAX_TIMESTAMP_LOOKAHEAD = 30 >>> is right

Please find below link
https://docs.splunk.com/Documentation/Splunk/6.2.0/Data/Configuretimestamprecognition
upvoted 29 times

NastyNutsu Most Recent 1 month, 3 weeks ago
Selected Answer: D
MAX_TIMESTAMP_LOOKAHEAD value determines how many character Splunk should look ahead in the event data to find the timestamp.
in this example, the time stamp is 2018-04-13 13:42:41:214 - 0500, which span the first 30 characters. Therefore, the best value is 30
upvoted 1 times

bobixaka 4 months ago
Selected Answer: D
2018-04-13 13:42:41.214 -0500 is much more than 10 characters long.
30 will catch it.
upvoted 2 times

Marco63 1 year, 10 months ago
Selected Answer: D
MAX_TIMESTAMP_LOOKAHEAD=10 is not enough to catch the whole timestamp
upvoted 3 times

royjn1981 2 years ago
Selected Answer: D
https://docs.splunk.com/Documentation/Splunk/8.1.1/Data/Configuretimestamprecognition
"Specify how far (how many characters) into an event Splunk software should look for a timestamp."
upvoted 3 times

Apis 2 years, 2 months ago
Selected Answer: D
D is correct
upvoted 4 times

leratel 2 years, 12 months ago

Is C a better choice ? Because date + time is 19 characters, 20 is ok or am I wrong ?

upvoted 3 times

leratel 2 years, 11 months ago

sorry for my question, I stupidly look at the format....

30 is good

upvoted 6 times

happy_and_lucky 3 years, 1 month ago

https://docs.splunk.com/Documentation/Splunk/8.1.1/Data/Configuretimestamprecognition

"Specify how far (how many characters) into an event Splunk software should look for a timestamp."

since TIME_PREFIX = ^ and timestamp is from 0-29 position, so D=30 will pick up the WHOLE timestamp correctly.

upvoted 3 times

Question #57 *Topic 1*

Which of the following are required when defining an index in indexes.conf? (Choose all that apply.)

A. coldPath

B. homePath

C. frozenPath

D. thawedPath

Suggested Answer: *ABD*
Reference:
https://answers.splunk.com/answers/558653/indexesconf-and-volume-settings.html

Community vote distribution
ABD (100%)

BlueRoselia Highly Voted 2 years ago
D is wrong frozen bucket are not required thus thawedPath is also not required
upvoted 5 times

Mntman77 Most Recent 8 months, 2 weeks ago
In the GUI these are all listed as optional, but in the documentation for indexes.conf they are required (except frozen)
upvoted 1 times

Apis 2 years, 2 months ago
Selected Answer: ABD
A, B & D are correct
upvoted 4 times

appopay 1 year, 2 months ago
confirmed here: https://docs.splunk.com/Documentation/Splunk/9.0.3/Admin/Indexesconf
upvoted 1 times

islamjy 2 years, 6 months ago
thawed path is optional not required from sys admin page 103
upvoted 3 times

lilsem 2 years, 6 months ago
Check splunk docs on indexes.conf:

thawedPath = <string>
* An absolute path that contains the thawed (resurrected) databases for the
index.
* CANNOT contain a volume reference.
* Path must be writable.
* Required. Splunkd does not start if an index lacks a valid thawedPath. <-----
upvoted 4 times

AxlF 2 years, 5 months ago
Thawed path is REQUIRED.
upvoted 2 times

ucsdmiami2020 2 years, 5 months ago
Answers are A, B, and D. Quoting the Splunk Reference URL https://docs.splunk.com/Documentation/Splunk/6.5.0/Admin/Indexesconf

homePath = <path on index server>
* An absolute path that contains the hotdb and warmdb for the index.

coldPath = <path on index server>
* An absolute path that contains the colddbs for the index.

thawedPath = <path on index server>

* An absolute path that contains the thawed (resurrected) databases for the index.

upvoted 1 times

DeltaPotato 2 years, 6 months ago

ABD - System Admin PDF, page 125. Paths must be specified, even when using the defaults.

upvoted 2 times

hwangho 3 years, 2 months ago

Answer: ABD

https://docs.splunk.com/Documentation/Splunk/8.1.1/Admin/Indexesconf

thawedPath = <string>

* Required. Splunkd does not start if an index lacks a valid thawedPath.

upvoted 3 times

newrose 3 years, 3 months ago

A B D looks correct to me

upvoted 3 times

Question #58 *Topic 1*

Which of the following apply to how distributed search works? (Choose all that apply.)

A. The search head dispatches searches to the peers.

B. The search peers pull the data from the forwarders.

C. Peers run searches in parallel and return their portion of results.

D. The search head consolidates the individual results and prepares reports.

Suggested Answer: *D*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Indexer/Howclusteredsearchworks

Community vote distribution
A (100%)

giubal Highly Voted 3 years, 4 months ago
The correct answer is A, C and D

as reported from system administrato pdf

Users log on to the search head and run reports:
– The search head dispatches searches to the peers
– Peers run searches in parallel and return their portion of results
– The search head consolidates the individual results and prepares reports
upvoted 39 times

Amith Highly Voted 3 years, 4 months ago
A,C and D
upvoted 12 times

FrozenYeti Most Recent 1 month, 2 weeks ago
Selected Answer: A
Correct answer is A, C and D
upvoted 1 times

MonicaKarim 1 month, 3 weeks ago
Selected Answer: C
A,C&D choose all that apply
upvoted 1 times

kolaturka 5 months, 1 week ago
A. The search head dispatches searches to the peers.
C. Peers run searches in parallel and return their portion of results.
D. The search head consolidates the individual results and prepares reports.

In a distributed search architecture, the search head is responsible for dispatching searches to the search peers. The peers then run the searches in parallel and return their portion of the results to the search head. The search head then consolidates the individual results and prepares reports based on the search criteria. The search peers do not pull data from forwarders; they only process search requests from the search head.
upvoted 1 times

ANALYSTBK 1 year ago
Selected Answer: A
A, C & D are correct, as reported from system administrator pdf
upvoted 4 times

Marco63 1 year, 4 months ago
Of course is A,C,D!
upvoted 3 times

Apis 1 year, 8 months ago

Selected Answer: A

A, C & D are correct

upvoted 5 times

Sandy_1988 2 years, 8 months ago

A,C and D are the options correct

upvoted 4 times

oksey 3 years ago

yea, ACD it is

upvoted 6 times

Question #59 *Topic 1*

What hardware attribute would you need to be changed to increase the number of simultaneous searches (ad-hoc and scheduled) on a single search head?

A. Disk

B. CPUs

C. Memory

D. Network interface cards

Suggested Answer: *B*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/SHCarchitecture

mker Highly Voted 3 years, 2 months ago
B is the correct
upvoted 10 times

ucsdmiami2020 1 year, 11 months ago
Per the provided Splunk URL reference https://docs.splunk.com/Documentation/Splunk/7.3.1/DistSearch/SHCarchitecture

Scroll down to section titled, How the cluster handles concurrent search quotas, "Overall search quota. This quota determines the maximum number of historical searches (combined scheduled and ad hoc) that the cluster can run concurrently. This quota is configured with max_Searches_per_cpu and related settings in limits.conf."
upvoted 1 times

kolaturka Most Recent 5 months, 1 week ago
B. CPUs

To increase the number of simultaneous searches (ad-hoc and scheduled) on a single search head, you would need to increase the number of CPUs. This is because searches are a CPU-intensive operation, and adding more CPUs would allow the search head to handle more search requests at the same time. While increasing the disk, memory, or network interface cards could improve other aspects of search performance, they would not directly increase the number of searches that can be run simultaneously.
upvoted 1 times

Apis 1 year, 8 months ago
B is correct
upvoted 1 times

hwangho 2 years, 8 months ago
Answer: B
https://docs.splunk.com/Documentation/Splunk/8.1.1/Capacity/Accommodatemanysimultaneoussearches
upvoted 3 times

Question #60 *Topic 1*

With authentication methods are natively supported within Splunk Enterprise? (Choose all that apply.)

A. LDAP

B. SAML

C. RADIUS

D. Duo Multifactor Authentication

Suggested Answer: *AD*
Reference:
https://docs.splunk.com/Documentation/Splunk/7.3.1/Security/SetupuserauthenticationwithSplunk

Community vote distribution
AB (67%) AD (33%)

newrose Highly Voted 3 years, 9 months ago
A B D I think
upvoted 17 times

hwangho Highly Voted 3 years, 8 months ago
Answer: ABC
https://docs.splunk.com/Documentation/Splunk/8.1.1/Security/SetupuserauthenticationwithSplunk
upvoted 14 times

hwangho 3 years, 8 months ago
also reference this: https://docs.splunk.com/Splexicon:Userauthentication
upvoted 5 times

3bd8ac0 Most Recent 4 weeks ago
Selected Answer: AB
Only A&B are correct. According to Splunk official documentation:
Set up native Splunk authentication
Native Splunk authentication lets you easily configure users to access Splunk platform resources. The native authentication scheme always takes precedence over any external authentication schemes.

The Splunk platform authenticates users in the following order:

Native Splunk authentication:
Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML), or scripted authentication (if you turn it on). For more information, see the following topics:
Set up user authentication with LDAP
Set up user authentication with external systems. Scripted authentication is not available on Splunk Cloud Platform.

Therefore, Radius and DMA are eternal systems.
source: https://docs.splunk.com/Documentation/Splunk/8.1.1/Security/Setupbuilt-inauthentication
upvoted 1 times

FrozenYeti 1 month, 2 weeks ago
Selected Answer: AB
The correct answer is A, B and D. In the Authentication Methods console, the options for natively supported authentication are LDAP, SAML and Duo Security.
upvoted 1 times

Frank_Rai 5 months ago
A, B & C

The authentication methods natively supported within Splunk Enterprise are:

A. LDAP (Lightweight Directory Access Protocol)
B. SAML (Security Assertion Markup Language)
C. RADIUS (Remote Authentication Dial-In User Service)
While Duo Multifactor Authentication can be integrated with Splunk, it is typically done through SAML or another authentication provider and not directly within Splunk Enterprise itself. Therefore, D. Duo Multifactor Authentication is not considered a natively supported authentication method within Splunk.
upvoted 2 times

bobixaka 10 months, 1 week ago
Selected Answer: AD
A B and D.
RADIUS requires scripting to be implemented, which means it's not "natively" supported by Splunk...
upvoted 3 times

BozhidarM 1 year, 1 month ago
A B D

https://docs.splunk.com/Documentation/Splunk/latest/Security/SetupuserauthenticationwithSplunk
upvoted 3 times

jswan382 10 months, 2 weeks ago
ABCD, in the document you referenced it includes "RADIUS":Use scripted authentication to integrate Splunk authentication with an external authentication system, such as Remote Authentication Dial-in User Service (RADIUS) or Pluggable Authentication Module (PAM).
upvoted 1 times

kolaturka 1 year, 5 months ago
A. LDAP
B. SAML
C. RADIUS

Splunk Enterprise natively supports LDAP, SAML, and RADIUS authentication methods. Duo Multifactor Authentication is not natively supported, but it can be integrated with Splunk using third-party plugins or custom scripts.
upvoted 2 times

erick165 1 year, 5 months ago
A & B are correct as we can see https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/Setupbuilt-inauthentication#:~:text=Available%20in%20both%20Splunk%20Cloud,over%20any%20external%20authentication%20schemes.&text=Lightweight%20Dire
upvoted 1 times

shergar 1 year, 9 months ago
I would go for ABCD. In page 239 of System Admin slide deck, it shows the screenshot for Authentication Methods. Internal - Splunk authentication, always on. External: None/LDAP/SAML. Multifactor Authentication: None/DUO Security / RSA Security

Then in the note, it states: Scripted access to PAM, RADIUS or other user account systems are also supported.

The unclear thing here is what exactly they mean with "natively"
upvoted 7 times

Mando22 1 year, 11 months ago
Correct Answer: A,B & C
upvoted 3 times

wts28 2 years, 2 months ago
ABC - https://docs.splunk.com/Documentation/Splunk/latest/Security/Setupbuilt-inauthentication

Set up native Splunk authentication:

Native Splunk authentication lets you easily set up users to access Splunk platform resources. Available in both Splunk Cloud Platform and Splunk Enterprise, the native authentication scheme always takes precedence over any external authentication schemes.

The Splunk platform authenticates users in the following order:

Native Splunk authentication

Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML), or scripted authentication (if enabled). For more information, see the following topics:
Set up user authentication with LDAP
Set up user authentication with external systems. Scripted authentication is not available on Splunk Cloud Platform.
upvoted 1 times

denominator 2 years, 2 months ago
I am still not sure because i see this:

The Splunk platform authenticates users in the following order:
https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/Setupbuilt-inauthentication
1 - Native Splunk authentication
2 - Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML), or scripted authentication (if enabled).

https://docs.splunk.com/Documentation/Splunk/9.0.0/Security/ConfigureSplunkToUsePAMOrRADIUSAuthentication
Native Splunk authentication takes precedence over any other type of authentication scheme. When you configure scripted authentication, the Splunk native authentication scheme still processes logins before passing the request onward to the scripted authentication scheme.
upvoted 1 times

king1993 2 years, 4 months ago
Answer: A and B
Supported: Splunk, LDAP, Scripted, SAML and ProxySSO
upvoted 3 times

Dori77777 2 years, 5 months ago
Selected Answer: AB
A & B
https://docs.splunk.com/Documentation/Splunk/latest/Security/Setupbuilt-inauthentication
Lightweight Directory Access Protocol (LDAP), Security Assertion Markup Language (SAML), or scripted authentication (if enabled). For more information, see the following topics:
upvoted 2 times

BlueRoselia 2 years, 6 months ago
Splunk Authentication Options
–Native Splunk accounts
–LDAP or AD
–SAML
–Scripted access to PAM, RADIUS, or other user account systems
• Saves the settings in authentication.conf
***ALSO Configuration Duo MFA -----AKA---- DUO MULTIFACTOR AUTHOTICATION
upvoted 2 times

huu_nguyen 2 years, 7 months ago
Selected Answer: AB
Only AB
upvoted 2 times

Question #61 *Topic 1*

Which configuration files are used to transform raw data ingested by Splunk? (Choose all that apply.)

A. props.conf

B. inputs.conf

C. rawdata.conf

D. transforms.conf

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.5/Data/Configuretimestamprecognition

Community vote distribution
A (67%) D (33%)

roblaw Highly Voted 3 years, 10 months ago
A & D, From Data Admin pdf, use transformations with props.conf and transforms.conf to:
– Mask or delete raw data as it is being indexed
–Override sourcetype or host based upon event values
– Route events to specific indexes based on event content
– Prevent unwanted events from being indexed
upvoted 25 times

MonicaKarim Most Recent 1 month, 3 weeks ago
Selected Answer: A
A&D Choose all that apply
upvoted 1 times

Frank_Rai 5 months ago
A & D.

The configuration files used to transform raw data ingested by Splunk are:

A. props.conf: This file is used to specify how Splunk formats incoming data, including settings for line breaking, timestamp recognition, character set encoding, and field extraction rules. It works in conjunction with transforms.conf for more advanced data transformation tasks.

D. transforms.conf: This file is used in conjunction with props.conf to define advanced data transformations, such as field extractions, data masking, and data filtering. It allows for the specification of regular expressions and other settings to extract, transform, and manipulate data.

While inputs.conf (B) is indeed a crucial configuration file in Splunk, it's used for specifying the input data settings, such as the type of input, the path for data ingestion, and various parameters for data collection, rather than transforming the data.

rawdata.conf (C) is not a standard configuration file in Splunk.
upvoted 1 times

PKUSER 7 months, 2 weeks ago
A (props.conf) is more about parsing and interpreting data, while D (transforms.conf) is focused on transforming raw data before indexing

So probably D
upvoted 1 times

k_alex 8 months, 3 weeks ago
with SEDCMD, props.conf is ok but using transformation command, props.conf and transforms.conf will be required.
upvoted 1 times

bobixaka 10 months, 1 week ago
Selected Answer: D

Combination of props.conf and transforms.conf is the answer.
Some transformations could be done only within props.conf, but since transforms.conf is in the possible answers, it is also a true answer.
upvoted 1 times

raizen11 1 year, 4 months ago
ABD
for transformation of raw all the three files needed
upvoted 1 times

kirtak 1 year, 4 months ago
inputs.conf is not relevant in the parsing phase
upvoted 1 times

Apis 2 years, 8 months ago
Selected Answer: A
A & D are correct
upvoted 2 times

hwangho 3 years, 8 months ago
Answer: AD
https://docs.splunk.com/Documentation/Splunk/8.1.1/Knowledge/Configureadvancedextractionswithfieldtransforms
upvoted 4 times

Question #62 *Topic 1*

What conf file needs to be edited to set up distributed search groups?

A. props.conf

B. search.conf

C. distsearch.conf

D. distibutedsearch.conf

Suggested Answer: *C*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.5/DistSearch/Distributedsearchgroups

Community vote distribution
C (100%)

newrose Highly Voted 2 years, 9 months ago
C. distsearch.conf
upvoted 8 times

toney_mu Most Recent 6 months, 3 weeks ago
https://docs.splunk.com/Documentation/Splunk/9.0.0/DistSearch/Distributedsearchgroups

Option C
upvoted 1 times

Apis 1 year, 8 months ago
Selected Answer: C
C is correct
upvoted 2 times

DeltaPotato 2 years ago
Confirmed C. https://docs.splunk.com/Documentation/Splunk/8.2.2/DistSearch/Distributedsearchgroups
upvoted 1 times

ucsdmiami2020 1 year, 11 months ago
Agreed C. Using the provided URL reference you read

"You can group your search peers to facilitate searching on a subset of them. Groups of search peers are known as "distributed search groups." You specify distributed search groups in the distsearch.conf file"
upvoted 2 times

Question #63 *Topic 1*

After configuring a universal forwarder to communicate with an indexer, which index can be checked via the Splunk Web UI for a successful connection?

A. index=main

B. index=test

C. index=summary

D. index=_internal

Suggested Answer: *D*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.5/Security/Validateyourconfiguration

Community vote distribution
D (100%)

NS2007 Highly Voted 1 year, 9 months ago
correct answer is D
upvoted 8 times

Apis Most Recent 8 months, 2 weeks ago
Selected Answer: D
D is correct
upvoted 2 times

DeltaPotato 1 year ago
D. index=_internal host=<forwarder_hostname>, page 183, System Admin PDF
upvoted 2 times

Question #64 *Topic 1*

Which of the following are available input methods when adding a file input in Splunk Web? (Choose all that apply.)

A. Index once.

B. Monitor interval.

C. On-demand monitor.

D. Continuously monitor.

Suggested Answer: *D*

Community vote distribution

A (100%)

jgab Highly Voted 4 years, 4 months ago

The correct answers are A & D

upvoted 32 times

ucsdmiami2020 3 years, 5 months ago

Agreed A and D. Quoting the Splunk Reference URL https://docs.splunk.com/Documentation/Splunk/8.2.2/Data/Howdoyouwanttoadddata

The fastest way to add data to your Splunk Cloud instance or Splunk Enterprise deployment is to use Splunk Web. After you access the Add Data page, choose one of three options for getting data into your Splunk platform deployment with Splunk Web: (1) Upload, (2) Monitor, (3) Forward

The Upload option lets you upload a file or archive of files for indexing. When you choose Upload option, Splunk Web opens the upload process page.
Monitor. For Splunk Enterprise installations, the Monitor option lets you monitor one or more files, directories, network streams, scripts, Event Logs (on Windows hosts only), performance metrics, or any other type of machine data that the Splunk Enterprise instance has access to.

upvoted 2 times

toney_mu 2 years ago

I don't see an option to turn on monitor once. Spluk continuasly monitor the file for updates.

upvoted 1 times

FrozenYeti Most Recent 1 month, 2 weeks ago

Selected Answer: A

The correct answer is A and D, those are the only two options in the Add Data > Files & Directories

upvoted 1 times

tje210 1 month, 2 weeks ago

Selected Answer: D

a and d; couldnt only pick one answer on this form, so i picked D to give it some visibility.

upvoted 1 times

65aab2c 4 months, 3 weeks ago

A & D Checked Splunk Live.
If you go to Splunk web > Add Data > Monitor > two options: Continuously Monitor / Index Once

upvoted 1 times

bobixaka 1 year, 4 months ago

Selected Answer: A

A and D

upvoted 1 times

anotherme1013 1 year, 7 months ago

A & D would be the answers

upvoted 1 times

BozhidarM 1 year, 7 months ago

AD is correct

upvoted 1 times

toney_mu 2 years ago

Answer would be D

upvoted 1 times

toney_mu 2 years ago

There is no option to monitor once, as splunk will continusly check for update so A is not valid

upvoted 1 times

erick165 1 year, 11 months ago

But there is an option to index once and that is what the option is so would be A&D

upvoted 1 times

Apis 3 years, 2 months ago

Selected Answer: A

A &D are correct

upvoted 2 times

mosematt 3 years, 9 months ago

ans is AD

upvoted 4 times

Question #65 *Topic 1*

Which is a valid stanza for a network input?

A. [udp://172.16.10.1:9997] connection = dns sourcetype = dns

B. [any://172.16.10.1:10001] connection_host = ip sourcetype = web

C. [tcp://172.16.10.1:9997] connection_host = web sourcetype = web

D. [tcp://172.16.10.1:10001] connection_host = dns sourcetype = dns

Suggested Answer: *C*

Reference:

https://docs.splunk.com/Documentation/SplunkCloud/8.0.2006/Data/Bypassautomaticsourcetypeassignment

Community vote distribution

D (100%)

roblaw Highly Voted 3 years, 3 months ago

D. connection_host attributes: dns (TCP), ip (UDP), none (UI)

upvoted 19 times

Hamiltonian 2 years, 8 months ago

Confirmation in inputs.conf under TCP: connection_host = [ip|dns|none]. Thus, web does not exist as an option and must be answer D.

upvoted 4 times

bobixaka Most Recent 4 months ago

Selected Answer: D

D is the correct answer

upvoted 1 times

Marco63 1 year, 10 months ago

Selected Answer: D

connection_host = web is not supported attribute value, instead connection_host=dns (answer D) is correct.

upvoted 3 times

Apis 2 years, 2 months ago

Selected Answer: D

D is correct

upvoted 1 times

Salman23 2 years, 5 months ago

D is correct.... Option C is incorrect because web is not valid for connection_host,

Data admin page 142

upvoted 2 times

DeltaPotato 2 years, 6 months ago

D - page 142 in Data Admin pdf for options/examples.

upvoted 2 times

ckmunich 2 years, 7 months ago

C is right!

Port 9997 on TCP is in Splunk the standard port for communication between the forwarders and indexers

Port 10001 is a non standard configuration

upvoted 1 times

AngusBlack 2 years, 8 months ago

D is correct. Although in theory you could use 9997 when I tried to configure it Splunk said it was not available.

upvoted 2 times

sargeholik 2 years, 11 months ago

C. PORT 9997 TCP Splunk port for communication between the forwarders and indexers

upvoted 4 times

hwangho 3 years, 2 months ago

Answer: D

https://docs.splunk.com/Documentation/Splunk/8.1.1/Data/Monitornetworkports

upvoted 4 times

Question #66 *Topic 1*

Which additional component is required for a search head cluster?

A. Deployer

B. Cluster Master

C. Monitoring Console

D. Management Console

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.5/DistSearch/SHCdeploymentoverview

Community vote distribution
A (100%)

hwangho Highly Voted 3 years, 8 months ago
A is correct.
https://docs.splunk.com/Documentation/Splunk/8.1.1/DistSearch/SHCdeploymentoverview
upvoted 8 times

ucsdmiami2020 2 years, 11 months ago
Per the provided URL reference
In addition to the set of search head members that constitute the actual cluster, a functioning cluster requires several other components:

The deployer. This is a Splunk Enterprise instance that distributes apps and other configurations to the cluster members. It stands outside the cluster and cannot run on the same instance as a cluster member. It can, however, under some circumstances, reside on the same instance as other Splunk Enterprise components, such as a deployment server or an indexer cluster master node.
upvoted 1 times

Gycu Most Recent 7 months ago
Selected Answer: A
DEPLOYER
upvoted 1 times

kolaturka 1 year, 5 months ago
According to the Splunk documentation on search head clustering, a Deployer is an optional component that can be used to distribute app and configuration updates to the members of a search head cluster. Therefore, Option A is the correct answer to the question, "Which additional component is required for a search head cluster?"
upvoted 2 times

Apis 2 years, 8 months ago
Selected Answer: A
A is correct
upvoted 2 times

Question #67 *Topic 1*

When are knowledge bundles distributed to search peers?

A. After a user logs in.

B. When Splunk is restarted.

C. When adding a new search peer.

D. When a distributed search is initiated.

Suggested Answer: *D*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.5/DistSearch/Whatsearchheadssend

Community vote distribution
D (100%)

hwangho Highly Voted 2 years, 8 months ago
D is correct
https://docs.splunk.com/Documentation/Splunk/8.0.5/DistSearch/Whatsearchheadssend
upvoted 11 times

ucsdmiami2020 1 year, 11 months ago
Agreed D. Quoting the Splunk reference URL...

"The search head replicates the knowledge bundle periodically in the background or when initiating a search. "
"As part of the distributed search process, the search head replicates and distributes its knowledge objects to its search peers, or indexers. Knowledge objects include saved searches, event types, and other entities used in searching accorss indexes. The search head needs to distribute this material to its search peers so that they can properly execute queries on its behalf."
upvoted 2 times

kolaturka Most Recent 5 months, 1 week ago
The correct answer is D. When a distributed search is initiated.

Knowledge bundles are collections of configuration files, saved searches, and other knowledge objects that are used to share knowledge across the distributed environment in Splunk. When a distributed search is initiated, the search head distributes the relevant knowledge bundle to the search peers that are participating in the search.

Option A is incorrect because knowledge bundles are not distributed to search peers after a user logs in.
Option B is incorrect because restarting Splunk does not trigger the distribution of knowledge bundles to search peers.
Option C is also incorrect because knowledge bundles are not distributed to search peers when adding a new search peer. Instead, when a new search peer is added to a search head cluster or a distributed search environment, the knowledge bundle is automatically distributed to the new search peer.
upvoted 3 times

Apis 1 year, 8 months ago
Selected Answer: D
D is correct
upvoted 1 times

Bianchi 2 years ago
D is correct. Pag 193 Sys Adm PDF
upvoted 4 times

Question #68 *Topic 1*

Assume a file is being monitored and the data was incorrectly indexed to an exclusive index. The index is cleaned and now the data must be reindexed. What other index must be cleaned to reset the input checkpoint information for that file?

A. _audit

B. _checkpoint

C. _introspection

D. _thefishbucket

Suggested Answer: *A*
Reference:
http://docshare02.docshare.tips/files/4773/47733589.pdf

Community vote distribution
D (100%)

roblaw Highly Voted 3 years, 3 months ago
D. _thefishbucket, it's purpose is to contain checkpoint information for file monitoring inputs.
upvoted 21 times

bobixaka Most Recent 4 months ago
Selected Answer: D
Absolutely, the answer is D.
upvoted 1 times

BozhidarM 7 months, 3 weeks ago
D is correct
upvoted 1 times

Apis 2 years, 2 months ago
Selected Answer: D
D is correct
upvoted 3 times

rawghav 2 years, 2 months ago
D is the right option
upvoted 2 times

Salman23 2 years, 5 months ago
D is correct, Sysadmin page 105
upvoted 3 times

loky0 2 years, 6 months ago
D. P132 Data admin pdf
upvoted 3 times

hwangho 3 years, 2 months ago
Answer: D
--reset Reset the fishbucket for the given key or file in the btree.
Resetting the checkpoint for an active monitor input reindexes data, resulting in increased license use.
https://docs.splunk.com/Documentation/Splunk/8.1.1/Troubleshooting/CommandlinetoolsforusewithSupport
upvoted 4 times

radskman 3 years, 3 months ago
Shouldn't be D ?
https://community.splunk.com/t5/Getting-Data-In/How-to-reindex-data-from-a-forwarder/m-p/93310
upvoted 4 times

Question #69 *Topic 1*

If an update is made to an attribute in inputs.conf on a universal forwarder, on which Splunk component would the fishbucket need to be reset in order to reindex the data?

A. Indexer

B. Forwarder

C. Search head

D. Deployment server

Suggested Answer: *A*
Reference -
https://community.splunk.com/t5/Archive/How-to-reindex-data-from-a-forwarder/td-p/93310

Community vote distribution
B (100%)

newrose Highly Voted 2 years, 9 months ago
Isn't it B? The files checkpoints reside in the UF's fishbucket index, right? So we should reset in the UF
upvoted 16 times

ucsdmiami2020 1 year, 11 months ago
Agreed B. Quoting the Splunk Reference URL https://www.splunk.com/en_us/blog/tips-and-tricks/what-is-this-fishbucket-thing.html

"Every Splunk instance has a fishbucket index, except the lightest of hand-tuned lightweight forwarders, and if you index a lot of files it can get quite large. As any other index, you can change the retention policy to control the size via indexes.conf"
upvoted 1 times

hwangho Highly Voted 2 years, 8 months ago
Answer: B
-change the inputs.conf on the deployment server (or forwarders)
-reset the fishbucket checkpoint on the involved forwarders
upvoted 8 times

FrozenYeti Most Recent 1 month, 1 week ago
Selected Answer: B
Correct Answer is B
1. Delete old data on indexers
2. Change inputs.conf on deployment server (or forwarders)
3. Reset the fishbucket checkpoint on the involved forwarders
4 Restart Splunk forwarders
upvoted 1 times

kolaturka 5 months, 1 week ago
Option A is incorrect because resetting the fishbucket on the indexer would not have any effect on the universal forwarder.

Option C is incorrect because resetting the fishbucket on the search head is not necessary in this scenario.

Option D is incorrect because the deployment server is used to manage and distribute configurations to forwarders, but resetting the fishbucket would need to be done on the forwarder itself.
upvoted 1 times

Fe01 1 year, 7 months ago
Selected Answer: B
https://www.splunk.com/en_us/blog/tips-and-tricks/what-is-this-fishbucket-thing.html
Answer is B
upvoted 2 times

IndicatorDeStafeta 1 year, 9 months ago

B is the correct answer

upvoted 1 times

Powdered_Sugar 1 year, 10 months ago

Answer: B

Data Admin Slide 132: To re-index step 3: Reset the fishbucket checkpoint on the involved forwarders.

upvoted 3 times

Salman23 1 year, 11 months ago

A is Correct, universal forwarders don't index data. Indexing always on indexers.

upvoted 2 times

Lerd15 2 years, 8 months ago

The correct ANS is B.

upvoted 6 times

Question #70 *Topic 1*

How can native authentication be disabled in Splunk?

A. Remove the $SPLUNK_HOME/etc/passwd file

B. Create an empty $SPLUNK_HOME/etc/passwd file

C. Set SPLUNK_AUTHENTICATION=false in splunk-launch.conf

D. Set nativeAuthentication=false in authentication.conf

Suggested Answer: *A*
Reference:
https://docs.splunk.com/Documentation/Splunk/8.0.5/Security/Secureyouradminaccount

Community vote distribution
B (100%)

roblaw Highly Voted 4 years, 3 months ago
B. A blank passwd file disables native authentication.
upvoted 15 times

FrozenYeti Most Recent 1 month, 1 week ago
Selected Answer: B
B is the correct answer. Creating a blank passwds file will disable native authentication.
upvoted 1 times

65aab2c 4 months, 3 weeks ago
Native authentication
Can be disabled with a blank Splunk passwd file
pg 226
upvoted 1 times

kolaturka 1 year, 11 months ago
reating an empty passwd file can disable native authentication in Splunk. This can be achieved by creating an empty file named passwd in the $SPLUNK_HOME/etc directory. This method is useful if you want to use an external authentication provider such as LDAP or SAML for user authentication.

Option D (nativeAuthentication=false in authentication.conf) can also be used to disable native authentication, but it is a more granular option as it only disables certain parts of the native authentication system.
upvoted 1 times

toney_mu 2 years ago
Option B
https://docs.splunk.com/Documentation/Splunk/9.0.3/Security/Usernameprecedence#:~:text=On%20the%20Splunk%20Enterprise%20instance,Restart%2
upvoted 2 times

Lewist 3 years, 1 month ago
Selected Answer: B
Answer is B
upvoted 2 times

loky0 3 years, 6 months ago
B. P151 sys admin pdf
upvoted 3 times

Sandy_1988 4 years, 2 months ago
B is the answer. Refer system admin pdf.
upvoted 4 times

newrose 4 years, 3 months ago
B. Create an empty $SPLUNK_HOME/etc/passwd file
upvoted 3 times

Question #71 *Topic 1*

The volume of data from collecting log files from 50 Linux servers and 200 Windows servers will require multiple indexers. Following best practices, which types of
Splunk component instances are needed?

A. Indexers, search head, universal forwarders, license master

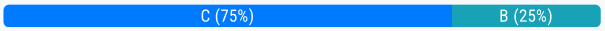
B. Indexers, search head, deployment server, universal forwarders

C. Indexers, search head, deployment server, license master, universal forwarder

D. Indexers, search head, deployment server, license master, universal forwarder, heavy forwarder

Suggested Answer: *B*

Community vote distribution



roblaw Highly Voted 3 years, 10 months ago

C. All search heads and indexers should use a license master

upvoted 17 times

Splunkv Highly Voted 3 years, 4 months ago

Did anybody notice that "s" is missing from "universal forwarder" in option C. whereas all other components are given as plural. so I would go with A.

upvoted 9 times

allahsal Most Recent 6 months, 1 week ago

Selected Answer: C

https://community.splunk.com/t5/Knowledge-Management/The-volume-of-data-from-collecting-log-files-from-50-Linux/m-p/522684

upvoted 1 times

kolaturka 1 year, 5 months ago

Option C is the correct answer.

According to best practices, a distributed deployment architecture is recommended for large-scale data ingestion and search operations. In this scenario, the volume of data from 50 Linux servers and 200 Windows servers requires multiple indexers, a search head, a deployment server, a license master, and universal forwarders.

The indexers are responsible for storing and indexing the data, while the search head is responsible for managing and processing search requests. The deployment server is used to centrally manage configurations across multiple components in the deployment, and the license master is used to centrally manage Splunk licenses. Finally, the universal forwarder is installed on the servers that generate the data to forward the data to the indexers.

upvoted 2 times

erick165 1 year, 5 months ago

Selected Answer: B

B is the correct one because it says needed, the license master and the HF are recomendations for best practice but not needed. also the option B as the UFs in plural and the opcion C doesn't

upvoted 1 times

nupacniyiveli 2 years, 1 month ago

Selected Answer: C

C is correct

upvoted 2 times

cagdaskarabag 2 years, 1 month ago

https://community.splunk.com/t5/Knowledge-Management/The-volume-of-data-from-collecting-log-files-from-50-Linux/m-p/522684
Answer is A.

upvoted 1 times

BlueRoselia 2 years, 6 months ago

C System Admin module 9 pg 196
upvoted 2 times

loky0 3 years ago
I'd say C. License master is definitely recommended with multiple indexers. Since we have multiple servers, we'll likely use a lot of UFs, so deployment servers will be good to monitor UFs.
upvoted 1 times

Hudda 3 years, 2 months ago
what is the final answer here pls confirm friends :)
upvoted 2 times

toney_mu 1 year, 6 months ago
C option
upvoted 1 times

Robo187 3 years, 4 months ago
I would add two heavy forwarders as intermediate forwarders for each linux and unix inputs
upvoted 2 times

toney_mu 1 year, 6 months ago
You may add for better design, but its not necessary
upvoted 1 times

Sandy_1988 3 years, 8 months ago
I think C is the correct answer
upvoted 1 times

hsing 3 years, 9 months ago
B, since the license master can reside on the search head/deployment instance
upvoted 2 times

Ashton_98 3 years, 9 months ago
Because it asks for 'component', it doesn't matter where it sits.
upvoted 2 times

Racgud 3 years, 9 months ago
Wrong, C i correct
upvoted 3 times

Question #72 *Topic 1*

Which of the following configuration files are used with a universal forwarder? (Choose all that apply.)

A. inputs.conf

B. monitor.conf

C. outputs.conf

D. forwarder.conf

Suggested Answer: *AC*

Reference:

https://docs.splunk.com/Documentation/Forwarder/8.0.5/Forwarder/Configuretheuniversalforwarder

Community vote distribution

AC (100%)

thomass Highly Voted 2 years, 5 months ago

answer: a,c

upvoted 9 times

ucsdmiami2020 1 year, 11 months ago

Per the provided URL referencehttps://docs.splunk.com/Documentation/Forwarder/8.0.5/Forwarder/Configuretheuniversalforwarder

--Key configuration files are:

inputs.conf controls how the forwarder collects data.

outputs.conf controls how the forwarder sends data to an indexer or other forwarder

server.conf for connection and performance tuning

deploymentclient.conf for connecting to a deployment server

upvoted 2 times

harrytbb Most Recent 7 months ago

Selected Answer: AC

A & C...

upvoted 1 times

Question #73 *Topic 1*

On the deployment server, administrators can map clients to server classes using client filters. Which of the following statements is accurate?

A. The blacklist takes precedence over the whitelist.

B. The whitelist takes precedence over the blacklist.

C. Wildcards are not supported in any client filters.

D. Machine type filters are applied before the whitelist and blacklist.

Suggested Answer: *A*
Reference:
https://community.splunk.com/t5/Getting-Data-In/Can-I-use-both-the-whitelist-AND-blacklist-for-the-same/td-p/390910

Orion42 Highly Voted 7 months, 2 weeks ago
Only A is correct
Ref: https://docs.splunk.com/Documentation/Splunk/8.2.1/Updating/Filterclients
upvoted 11 times

sam_1215 Most Recent 4 months, 2 weeks ago
Answer is A
A. The blacklist takes precedence over the whitelist.

course "Data Admin" > Forwarder Management > Selecting Clients
- supports wildcards
- in addition ... you can further filter based on machine types

See also :
https://docs.splunk.com/Documentation/Splunk/latest/Updating/Filterclients
upvoted 2 times

Hudda 8 months, 1 week ago
friends, could you please confirm the answer for this Q ?
upvoted 1 times

thomass 11 months, 3 weeks ago
answer : a
upvoted 2 times

Question #74 *Topic 1*

Which configuration file would be used to forward the Splunk internal logs from a search head to the indexer?

A. props.conf

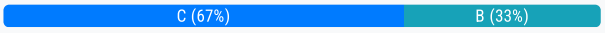
B. inputs.conf

C. outputs.conf

D. collections.conf

Suggested Answer: *C*
Reference:
https://community.splunk.com/t5/Getting-Data-In/How-to-configure-search-head-to-forward-internal-data-to-the/td-p/111658

Community vote distribution



hwangho Highly Voted 3 years, 8 months ago
C is correct.
https://docs.splunk.com/Documentation/Splunk/8.1.1/DistSearch/Forwardsearchheaddata
upvoted 9 times

ucsdmiami2020 2 years, 11 months ago
Per the provided Splunk reference URL by @hwangho, scroll to section Forward search head data, subsection titled, 2. Configure the search head as a forwarder.
"Create an outputs.conf file on the search head that configures the search head for load-balanced forwarding across the set of search peers (indexers)."
upvoted 1 times

FrozenYeti Most Recent 1 month, 2 weeks ago
Selected Answer: C
The correct answer is C. This question is assuming that the indexer is already configured for listening, you are only configuring the search head to forward data to the indexer, in which case you only need to modify the outputs.conf on the search head.
upvoted 1 times

PrincePazol 7 months, 1 week ago
Selected Answer: C
In outputs.conf:
[tcpout]
defaultGroup = indexers1

[indexAndForward]
index=false

[tcpout:indexers1]
server = 10.1.1.197:9997, 10.1.1.200:9997
upvoted 1 times

CactiAZ 9 months, 3 weeks ago
Selected Answer: C
This community usually gets these questions right, but I'm surprised by how many are putting the wrong answer. The correct answer is C. See the link in hwangho's post. Search heads, and all Splunk instances, already have inputs built to read internal logs by default. They just need an outputs.conf to create a tcpout stanza to your indexers to get them to send their internal logs, which is what this question is asking about. In our Splunk environment we have NEVER set up an inputs for internal logs, we only deploy an outputs.conf with our indexers listed in a tcpout stanza, and we get all of our internal logs just fine.

If you had other logs on a search head (like from a script or something), then yes, you would need an inputs.conf to get those to be read. But that is definitely not what this question is asking about.
upvoted 2 times

yaman778 1 year ago

Selected Answer: B

B for sure. inputs.conf allows you to define data inputs that the Splunk instance should monitor and forward to indexers.
Use monitor stanza specifying the path to log files and destination indexer's host name, port.
Stanza Sample
[monitor:///opt/splunk/var/log/splunk]
Index = _internal
Soucetype = Splunkd
Disabled = false
_TCP_ROUTING = indexer_group

upvoted 1 times

kolaturka 1 year, 5 months ago

he correct answer is B. inputs.conf is used to configure the inputs on a Splunk instance, including forwarding data from one instance to another. In this case, to forward the Splunk internal logs from a search head to the indexer, you would need to add a stanza to inputs.conf on the search head that specifies the indexer as the destination for the logs. The props.conf file is used to configure how data is processed after it has been indexed, outputs.conf is used to configure the destination of data for specific stanzas, and collections.conf is used for managing data in collections.

upvoted 1 times

anonyuser 1 year, 9 months ago

Just for a little clarification, configuring the sh as a forwarder using outputs.conf does not necessarily tell the sh to send a certain type of data that you would use inputs.conf for. However, this is talking about _internal, which I believe is data that is sent by default, without the need for inputs.conf. Please correct me if I am wrong here

upvoted 1 times

Hudda 3 years, 2 months ago

Friends, could you please confirm this answer?

upvoted 2 times

Question #75 *Topic 1*

When configuring HTTP Event Collector (HEC) input, how would one ensure the events have been indexed?

A. Enable indexer acknowledgment.

B. Enable forwarder acknowledgment.

C. splunk check-integrity -index <index name>

D. index=_internal component=ACK | stats count by host

Suggested Answer: *A*
Reference -
https://docs.splunk.com/Documentation/Splunk/8.0.5/Data/AboutHECIDXAck

Community vote distribution
A (100%)

shivi Highly Voted 3 years ago
A. Enable indexer acknowledgment.
upvoted 12 times

ucsdmiami2020 2 years, 5 months ago
Per the provided Splunk reference URLhttps://docs.splunk.com/Documentation/Splunk/8.0.5/Data/AboutHECIDXAck
"While HEC has precautions in place to prevent data loss, it's impossible to completely prevent such an occurrence, especially in the event of a network failure or hardware crash. This is where indexer acknolwedgment comes in."
upvoted 2 times

FrozenYeti Most Recent 1 month, 2 weeks ago
Selected Answer: A
The correct answer is A. This has to be enabled at the token level in Splunk Web. If you want to enable it via the configuration files, you would add a stanza with the corresponding token and add the line useACK=true.
upvoted 1 times

adamsca 7 months, 3 weeks ago
Selected Answer: A
A is correct
upvoted 1 times

mngesha 1 year, 1 month ago
A would be the most appropriate answer in this case. C looks like just a query. The document in the link should clarify.
upvoted 2 times

rockhorse 1 year, 9 months ago
D for sure
upvoted 1 times