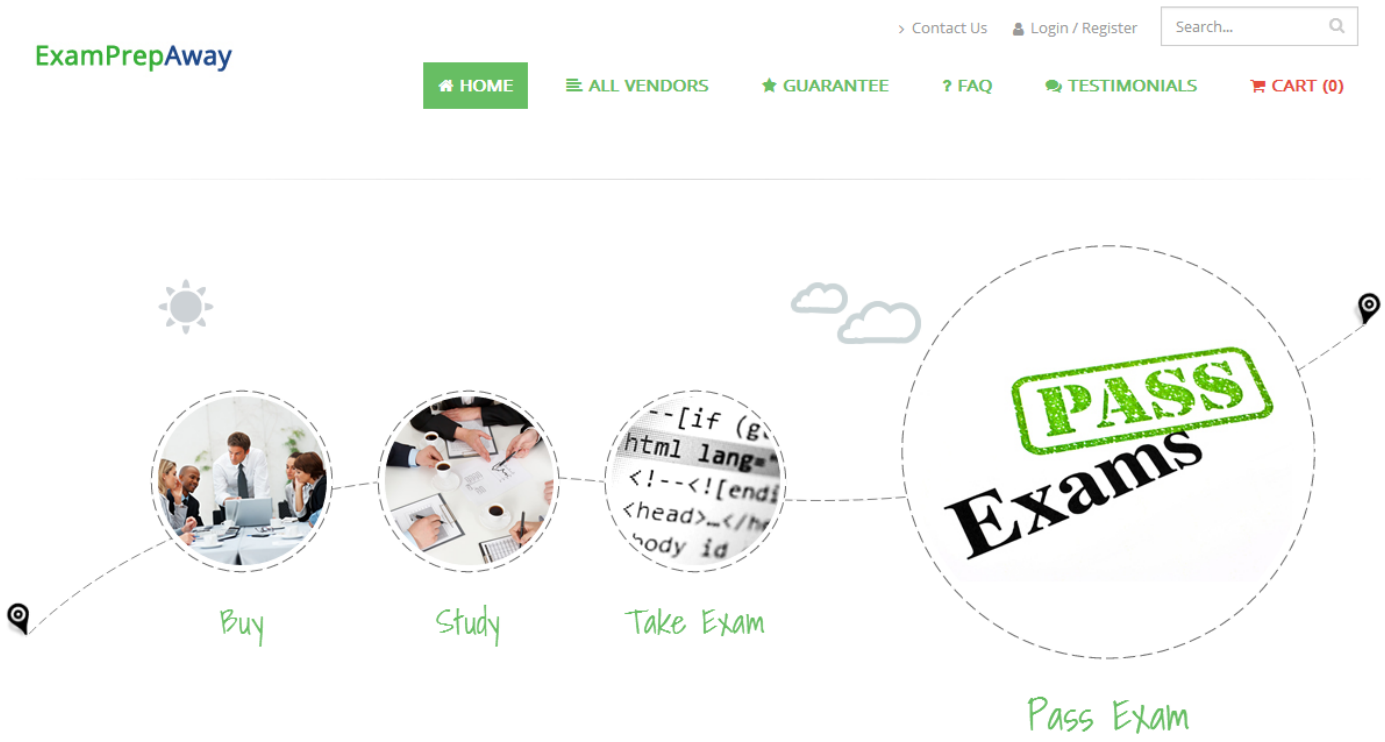
ExamPrepAway



Try **Online Engine** before you buy

We're not the only ones **happy** about ExamPrepAway Practice Material ...

56295+ customers in 100+ countries use ExamPrepAway Test Engine. Meet our customers.

GetCustom JET ORANGE iCompany Paradoxx iMessenger VOREED

http://www.examprepaway.com/

Latest Exam Guide & Learning Materials

Exam : **NSE5_FAZ-7.0-JPN**

Title : Fortinet NSE 5 - FortiAnalyzer 7.0 (NSE5_FAZ-7.0日本語版)

Vendor : Fortinet

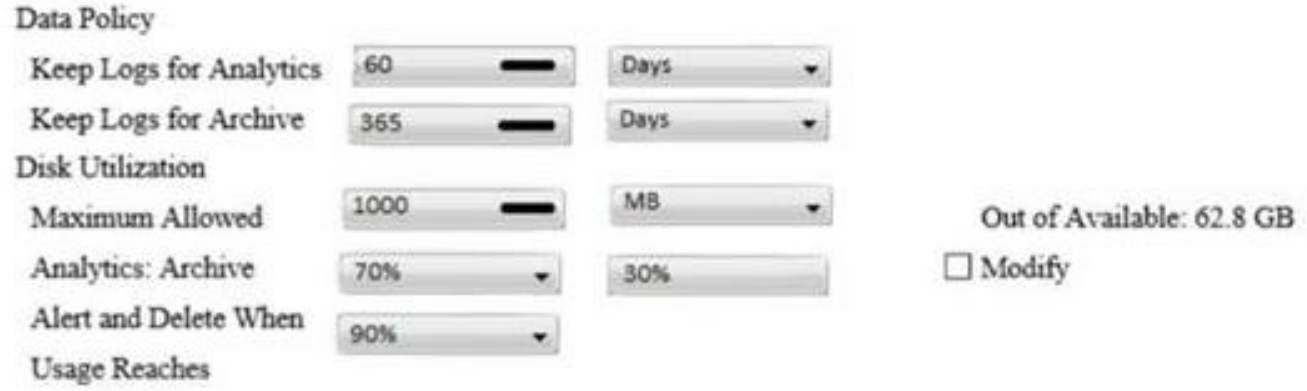
Version : DEMO

QUESTION NO: 1
FortiAnslyzer でデータベースをクエリする正しい順序の SQL クエリはどれですか?
A. SELECT devid FROM Slog GROOP BY devid WHERE * user' =* USERl'
B. SELECT devid WHERE 'u3er'='USERl' FROM $ log GROUP BY devid
C. SELECT devid FROM Slog- WHERE *user' =' USERl' GROUP BY devid
D. FROM Slog WHERE 'user* =' USERl' SELECT devid GROUP BY devid
Answer: C
FortiAnalyzer_7.0_Study_Guide-Online.pdf page 259: The main clauses FortiAnalyzer reports use are as follows:
* FROM
* WHERE
* GROUP BY
* ORDER BY
* LIMIT
* OFFSET
Accordingly, following the SELECT keyword, the statement must be followed by one or more clauses in the order in which they appear in the table shown on this slide.

QUESTION NO: 2
FortiAnalyzer でのログ取得に関して正しい説明はどれですか?(2つ選んでください。)
A. FortiAnalyzer デバイスは、フェッチ
サーバーまたはクライアントの役割のいずれかを実行でき、反対側の同じ FortiAnalyzer デバイスで同時に 2 つの役割を実行できます。
B. ログのフェッチは、同じファームウェア バージョンを実行している 2 つの FortiAnalyzer デバイスでのみ実行できます。
C. ログの取得により、管理者は冗長性のために別の FortiAnalyzer
から分析ログを取得できます。
D. ログ フェッチにより、管理者は、1 つの FortiAnalyzer デバイスからアーカイブ
ログを取得して別の FortiAnalyzer
デバイスに送信することにより、履歴データに対してクエリとレポートを実行できます。
Answer: B,D
Reference:
Using FortiAnalyzer, you can enable log fetching. This allows FortiAnalyzer to fetch the archived logs of specified devices from another FortiAnalyzer, which you can then run queries or reports on for forensic analysis.
The FortiAnalyzer device that fetches logs operates as the fetch client, and the other FortiAnalyzer device that sends logs operates as the fetch server. Log fetching can happen only between two FortiAnalyzer devices, and both of them must be running the same firmware version. A FortiAnalyzer device can perform either the fetch server or client role, and it can perform two roles at the same time with different FortiAnalyzer devices at the other end.
FortiAnalyzer_7.0_Study_Guide-Online pag. 168

QUESTION NO: 3

展示を見る:



ディスク使用率の最大 1000MB は何を指していますか?

A. FortiAnalyzer モデルのディスク クォータ

B. ADOM 内のすべてのデバイスのディスク クォータ

C. ADOM 内の各デバイスのディスク クォータ

D. ADOM タイプのディスク クォータ

Answer: B

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuring-log-storage-policy

QUESTION NO: 4

FortiAnalyzer レポートを外部に電子メールで送信するには、FortiAnalyzer で構成する必要があるのは次のうちどれですか?

（2つ選んでください。）

A. メールサーバー

B. 出力プロファイル

C. SFTP サーバー

D. レポートのスケジュール

Answer: A,B

QUESTION NO: 5

ファブリック コネクタに関して正しい記述はどれですか?（2つ選んでください。）

A. インシデントの作成時に ITSM プラットフォームに通知を送信するようにファブリック コネクタを構成することは、FortiAnalyzer API からのサードパーティの情報よりも効率的です。

B. ファブリック コネクタにより、ストレージ コストを節約し、冗長性を向上させることができます。

C. ストレージ コネクタ サービスでは、ログをクラウド プラットフォームに送信するための個別のライセンスは必要ありません。

D. Cloud-Out 接続を使用すると、Amazon S3、Azure Blob、Google Cloud などのパブリック クラウド アカウントにリアルタイム ログを送信できます。

Answer: A,D

QUESTION NO: 6

次の CLI コマンドを検討してください。

```
# configure system global
    set log-checksum md5
  end
```

コマンドの目的は何ですか?
A. 各ログに一意のタグを追加して、この FortiAnalyzer からのものであることを証明します。
B. MD5 ハッシュ値と認証コードを追加するには
C. ログ ファイルのチェックサムを追加するには
D. ログ通信を暗号化する
Answer: C
https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/849211/global

QUESTION NO: 7
FortiAnalyzer の高可用性 (HA) ダスターの扱いに関して正しい記述はどれですか?
(2つ選んでください)
A. FortiAnalyzer は、シリアル番号によってさまざまなデバイスを識別します。
B. FortiAnalyzer は、ダスター内の d デバイスからログを受信します。
C. FortiAnalyzer はクラスタ内のプライマリ デバイスからのみ bgs を受信します。
D. FortiAnalyzer が知る必要があるのは、クラスタ内のプライマリ デバイスのシリアル番号だけです。他のデバイスは自動的に検出されます。
Answer: A,B

QUESTION NO: 8
ログ ビューでは、チャート ビルダー機能を使用して、フィルター処理された検索結果に基づいてデータセットとチャートを作成できます。
同様に、FortiView で使用できる機能はどれですか?
A. レポート チャートにエクスポート
B. PDF にエクスポート
C. チャートビルダーにエクスポート
D. カスタムチャートにエクスポート
Answer: A
Reference:
Similar to the Chart Builder feature in Log View, you can export a chart from a FortiView. The chart export includes any filters you set on the FortiView. FortiAnalyzer_7.0_Study_Guide-Online pag. 292.

QUESTION NO: 9
FortiAnalyzer は SSL を介した Optimized Fabric Transfer Protocok (OFTP) をどのような目的で使用しますか?
A. ログを SFTP サーバーにアップロードするには

B. バックアップ中のログの変更を防ぐため
C. 同一のログ セットを 2 番目のログ サーバーに送信するには
D. デバイス間のログ通信を暗号化する
Answer: D

QUESTION NO: 10
FortiAnalyzer でのデータセット クエリの目的は何ですか?
A. ログデータをテーブルにソートします
B. データベース スキーマを抽出します。
C. データベースからログデータを取得します
D. ログデータをデータベースに注入します
Answer: C