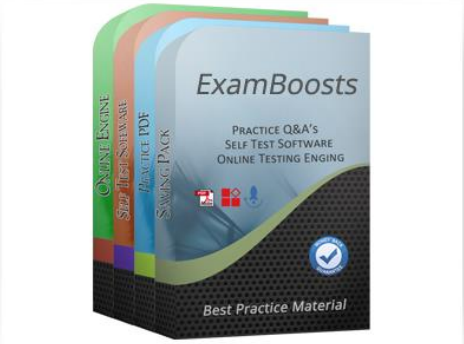
ExamBoosts

TRY BEFORE YOU BUY

Download a free sample of any of our exam questions and answers

- 24/7 customer support, Secure shopping site
- Free One year updates to match real exam scenarios
- If you failed your exam after buying our products we will refund the full amount back to you.



365 Days Free Updates

Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Security & Privacy

We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Instant Download

After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact us.

Money Back Guarantee

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

http://www.examboosts.com/

Reliable & Efficient Test Practice Questions to Satisfy All Candidates

Exam : **NSE5_FAZ-7.2-JPN**

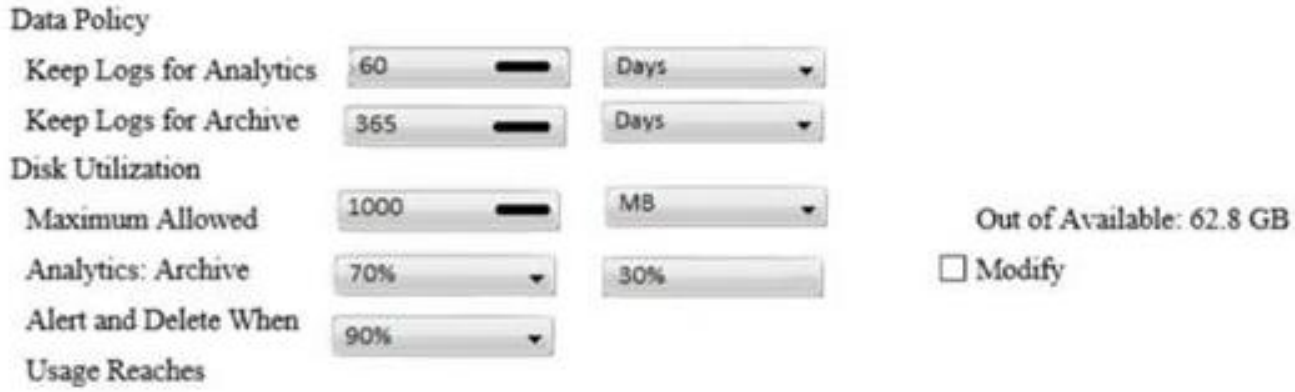
Title : Fortinet NSE 5 - FortiAnalyzer 7.2 Analyst (NSE5_FAZ-7.2日本語版)

Vendor : Fortinet

Version : DEMO

QUESTION NO: 1
FortiAnalyzer およびそのすべての登録デバイスで NTP
サーバーを使用する主な目的は何ですか?
A. ログ相関
B. ホスト名解決
C.ログ収集
D. リアルタイム転送
Answer: A

QUESTION NO: 2
展示品を見る:



ディスク使用量の最大 1000MB とは何を指しますか?
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
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/configuring-log-storage-poli

QUESTION NO: 3
RAID 管理において、ディスクのステータス「劣化」は何を意味しますか?
A. FortiAnalyzer ユニットに 1
つ以上のドライブがありません。ドライブはオペレーティング
システムで使用できなくなりました。
B. FortiAnalyzer デバイスは、アレイをフォールト
トレラントにするために、デバイス上のすべてのハード
ドライブに書き込みを行っています。
C. FortiAnalyzer デバイスは、ハード
ドライブを最適な状態に復元するために、新しく追加されたハード
ドライブにデータを書き込んでいます。
D. ハードドライブは RAID コントローラによって使用されなくなりました
Answer: D

QUESTION NO: 4
FortiAnalyzer 上の Ha の初期ログ同期とログ データ同期に関係なく、正しい 2 つのステートメントはどれですか?
A. デフォルトでは、ログ データ同期はすべてのバックアップ デバイスで無効になっています。
B. ログ データ同期は、すべてのバックアップ デバイスにリアルタイムのログ同期を提供します。
C. 初期ログ同期では、HA クラスターにユニットを追加すると、プライマリ デバイスがそのログをバックアップ デバイスと同期します。
D. ログ データ同期がオンになると、バックアップ デバイスが再起動され、同期されたログを使用してログ データベースが再構築されます。
Answer: C D

QUESTION NO: 5
FortiOS コネクタを使用する FortiAnalyzer のプレイブックをクレストしました FortiGate 側を設定するとき、オートメーション ステッチのアクションを FortiOS コネクタで利用できるようにするには、どのタイプのトリガーを使用する必要がありますか ?
A. FortiAnalyzer イベント ハンドラー
B. 受信 Webhook
C. FortiOS イベントログ
D. ファブリックコネクタイベント
Answer: C
Explanation:
"One possible scenario is shown on the slide:
1. Traffic flows through the FortiGate
2. FortiGate sends logs to FortiAnalyzer
3. FortiAnalyzer detects some suspicious traffic and generates an event
4. The event triggers the execution of a playbook in FortiAnalyzer, which sends a webhook call to FortiGate so that it runs an automation stitch
5. FortiGate runs the automation stitch with the corrective or preventive actions"
FortiAnalyzer_7.0_Study_Guide-Online page 228 In order to see the actions related to the FOS connector, you must enable an automation rule using the Incoming Webhook Call trigger on the FortiGate side. FortiAnalyzer_7.0_Study Guide page no 233

QUESTION NO: 6
FortiAnalyzer のオンライン ログを説明するステートメントはどれですか?
A. 特定のサイズに達してロールオーバーされたログ
B.レポート作成に使用できるログ
C. ログブラウズで閲覧できるログ
D. ディスクに保存され、圧縮され、FortiView で使用できるログ
Answer: B

QUESTION NO: 7
管理者は次の設定を構成しました。
システムグローバルの設定
ログチェックサム md5-auth を設定します
終わり
このコマンドを実行する意味は何ですか?
A. このコマンドはログ ファイルの MD5 ハッシュ値を記録します。
B. このコマンドは、パスワードをログ ファイルに記録し、暗号化します。
C. このコマンドは、FortiAnalyzer と他のデバイス間のログ転送を暗号化します。
D. このコマンドは、ログ ファイルの MD5 ハッシュ値と認証コードを記録します。
Answer: D

QUESTION NO: 8
FortiAnalyzer FortiView では、FortiGate デバイスの送信元および宛先 IP
アドレスがホスト名に解決されません。
FortiAnalyzer に追加のパフォーマンスへの影響を与えずに、送信元 IP アドレスと宛先 IP
アドレスを解決するにはどうすればよいでしょうか?
A. ADOM ごとに IP アドレスを解決し、IP 解決中の FortiView での遅延を軽減します。
B. システムの FortiView 設定で # setsolve-ipenable を構成します
C. FortiAnalyzer でローカル DNS サーバーを構成する
D. FortiGate で IP アドレスを解決します。
Answer: D
Explanation:
https://packetplant.com/fortigate-and-fortianalyzer-resolve-source-and-destination-ip/
"As a best practice, it is recommended to resolve IPs on the FortiGate end. This is because you get both source and destination, and it offloads the work from FortiAnalyzer. On FortiAnalyzer, this IP resolution does destination IPs only"

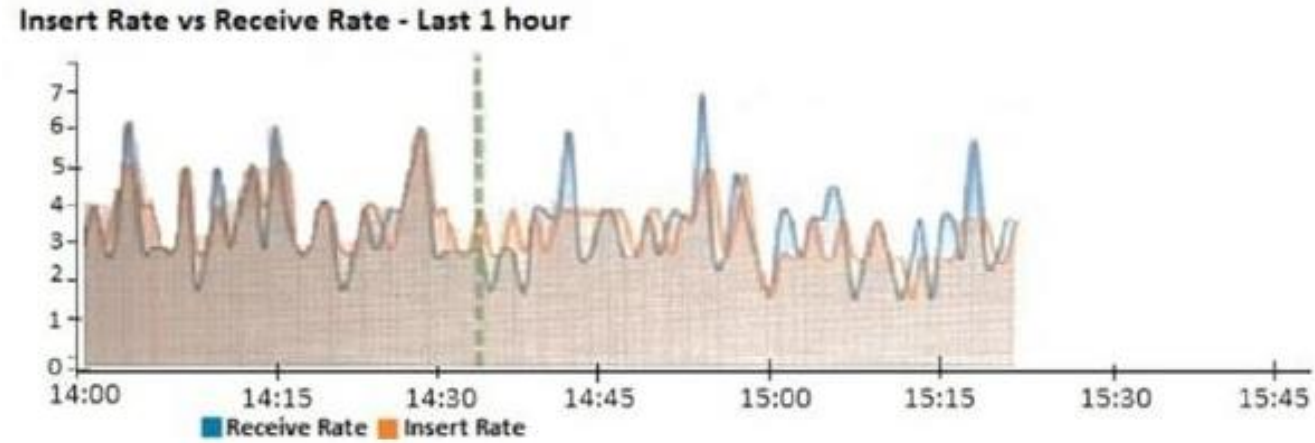
QUESTION NO: 9
コマンド detect sql status sqlplugind を実行するのはなぜですか?
A. 現在実行中の SQL プロセスを一覧表示します。
B. データベースログの挿入状況を確認する場合
C. SOL クエリ接続と hcache ステータスを表示する
D. 現在の hcache サイズを表示するには
Answer: D

QUESTION NO: 10
FortiAnalyzer ディスクに保存されたログ
ファイルがデバイスのログ設定で指定されたサイズに達するとどうなりますか?
A. ログ ファイルは生のログとして保存され、分析サポートに使用できます。
B. ログ ファイルはロールオーバーされ、アーカイブされます。
C. ログ ファイルがデータベースから削除されます。
D. ログファイルを上書きします。
Answer: B

QUESTION NO: 11
データ ポリシーで構成されたアーカイブ設定より前に、ADOM の 1 つからログが削除されています。最も可能性の高い問題は何ですか?
A. 合計ディスク容量が不足しているため、別のディスクを追加する必要があります。
B. CPU リソースが多すぎます。
C. ADOM ディスク クォータの設定が、ログ レートに基づいて低すぎます。
D. ADOM のログは別の FortiAnalyzer デバイスにリアルタイムで転送されます。
Answer: C
Explanation:
https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG FAZ/1100_Storage/0017_Deleted%20device%20logs.htm
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/87802/automatic-deletion

QUESTION NO: 12
管理者が FortiGate A をルート ADOM から ADOM1 に移動しました。
ログに関して正しい 2 つの記述はどれですか? (2つお選びください。)
A. 分析ログはルート ADOM から ADOM1 に自動的に移動されます。
B. アーカイブ ログはルート ADOM から ADOM1 に自動的に移動されます。
C. ログは移動直後に両方の ADOM に表示されます。
D. ADOM1 SQL データベースを再構築した後、分析ログはルート ADOM から ADOM1 に移動されます。
Answer: B D

QUESTION NO: 13
展示品をご覧ください。



14:35 のデータ ポイントは何を示していますか?
A. FortiAnalyzer はログを削除しています。
B. FortiAnalyzer は、ログの受信よりも速くログのインデックスを作成しています。
C. 古いログのインデックスを作成できるように、FortiAnalyzer はログの受信を一時的に停止しました。
D. sqlplugind デーモンは、インデックス作成において 1 つのログだけ進んでいます。

Answer: B
Explanation:
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/47690/insert-rate-vs-receive-rate-wid

QUESTION NO: 14
管理者は、FortiAnalyzer デバイスに FortiClient EMS を登録できません。
この失敗の原因は何でしょうか?
A. FortiAnalyzer は HA クラスター内にあります。
B. FortiClient EMS デバイスを登録するには、ADOM
モードをアドバンストに設定する必要があります。
C. ADOM は FortiAnalyzer で有効になっていません。
D. FortiClient EMS デバイスを登録するには、FortiAnalyzer に別のライセンスが必要です。
Answer: C