Fortinet.NSE5_FAZ-7.0.v2023-09-01.q54

試験コード:	NSE5_FAZ-7.0
試験名称:	Fortinet NSE 5 - FortiAnalyzer 7.0
認定資格:	Fortinet
無料問題数:	54
バージョン:	v2023-09-01
アクセス数:	727
ページビュー数:	540
https://www.jpnpdf.com/Fortinet.NSE5_FAZ-7.0.v2023-09-01.q54-mondaishu.html	

最新問題: **1**
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 (メーッセージを残す**)**
参照：
81a4-00505692583a/FortiAnalyzer-6.0.5-管理ガイド.pdf
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/355632/log-browse

最新問題: **2**
FortiAnalyzer で作成されたシステム バックアップに含まれる 2 つの要素はどれですか? (2つお選びください。)
A. レポート情報
B. システム情報
C. データベースのスナップショット
D. 登録されたデバイスからのログ
Answer: B,D (メーッセージを残す**)**

最新問題: **3**
構成されたイベント ハンドラーと一致するイベントが発生したときに、イベント通知を送信するために使用できる 2 つの方法はどれですか? (2つお選びください。)
A. SMS
B. メールアドレス
C. SNMP

D. IM
Answer: B,C (メーッセージを残す**)**
参照：
FortiAnalyzer_Admin_Guide/1800_Events/0200_Event_handlers/0600_Create_event_handlers.htm

最新問題**: 4**
FortiAnalyzer ファームウェアをアップグレードすると、どのレポート要素が影響を受ける可能性がありますか?
A. レポートのスケジュール設定
B. レポート設定
C. カスタム データセット
D. 出力プロファイル
Answer: (解答を表示する**)**

最新問題**: 5**
展示を参照してください。
Laptopt は、FortiAnalyzer を管理するために複数の管理者によって使用されます。「admin」以外のユーザーによって生成され、Laptop1 からの Web インターフェイスへのすべてのログイン試行と一致する汎用テキスト フィルターを構成したいとします。
どのフィルタが望ましい結果を達成しますか?
A. 操作ログイン & 実行済み_on=="GUI(10.1.1.100)" & ユーザー!=管理者
B. 操作ログイン & srcip==10.1.1.100 & dstip==10.1.1.210 & user==admin
C. 操作ログイン & dstip==10.1.1.210 & ユーザー管理者
D. 操作ログイン & 実行済み_on=="GUI(10.1.1.210)' & ユーザー!=管理者
Answer: A (メーッセージを残す**)**
そこでのタスクは、ローカル コンピュータ以外の他の場所からのログイン失敗に対するフィルタを作成することでした。 テキスト Performed_on!~10.0.1.10 を追加します。これには、設定されている IP アドレスではないデバイスからの試行が含まれます」ローカルクライアントコンピュータ。」

最新問題**: 6**
ハードウェア RAID をサポートする FortiAnalyzer でハードディスク障害を処理する最善のアプローチは何ですか?
A. ディスクをホットスワップします。
B. ディスクは自己修復するため、何もする必要はありません。
C. フォーマット ディスクの実行を実行して、FortiAnalyzer デバイスをフォーマットし、再起動します。
D. FortiAnalyzer をシャットダウンし、ディスクを交換します。
Answer: A (メーッセージを残す**)**
https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/0700_RAID/0800_Swapping%20Disks.htm#:~:text=If%20a%20hard%20disk%20on,to %20交換%20、%20ハード%20ディスク。

最新問題: **7**
FortiAnalyzer のマクロに関して正しいのはどれですか?
A. マクロは ADOM 固有であり、各 ADOM にはその ADOM に関連する固有のマクロがあります。
B. マクロは FortiGate ADOM でのみサポートされます。
C. マクロは、レポート設定に基づいて Excel ログ ファイルを自動的に生成する場合に便利です。
D. マクロはレポート用に事前定義されたテンプレートであり、カスタマイズできません。
Answer: A (メーッセージを残す**)**
FortiAnalyzer_7.0_Study_Guide-Online.pdf ページ 283: マクロは ADOM 固有であり、FortiGate および FortiCarrier ADOM でのみサポートされていることに注意してください。

最新問題: **8**
FortiAnalyzer レポートをサポートされている外部サーバーにアップロードするには、FortiAnalyzer で何を設定する必要がありますか?
(2つお選びください。)
A. SFTP、FTP、または SCP サーバー
B. メールサーバー
C. 出力プロファイル
D. レポートのスケジュール設定
Answer: (解答を表示する**)**
https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration-guide/598322/creating-output-profiles

最新問題: **9**
CLI コマンド # detect test application oftpd 3 は何を判断するのに役立ちますか?
A. FortiAnalyzer に接続しているデバイスと IP アドレス
B. FortiAnalyzer に到達しているログ (存在する場合)
C. どの ADOM が有効化および構成されているか
D. 登録されているデバイスと登録されていないデバイス
Answer: A (メーッセージを残す**)**
https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/395556/test#test_application

最新問題: **10**
展示品をご参照ください。
このプレイブックを実行した後に作成されたインシデントには、いくつのイベントが追加されますか?
A. イベントが10件追加されます。
B. 5つのイベントが追加されます。
C. イベントは追加されません。
D. イベントが13個追加されます。
Answer: B (メーッセージを残す**)**

最新問題: **11**

次の CLI コマンドを考えてみましょう。
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場合
C. ログファイルのチェックサムを追加する場合
D. ログ通信を暗号化する場合
Answer: C (メーッセージを残す**)**
https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/849211/global

最新問題**: 12**
FortiAnalyzer の高可用性 (HA) 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. FortiAnalyzer HA は VRRP なしでも機能します。VRRP は、クラスター内に 3 つ以上の FortiAnalyzer デバイスがある場合にのみ必要です。
B. FortiAnalyzer HA クラスター内のすべてのデバイスは、同じ動作モード (アナライザーまたはコレクター) で実行する必要があります。
C. FortiAnalyzer HA の実装は、AWS、Microsoft Azure、Google Cloud などの多くのパブリック クラウド インフラストラクチャによってサポートされています。
D. FortiAnalyzer HA は、ログの同期と一部のシステム設定および構成設定をサポートします。
Answer: B,D (メーッセージを残す**)**

最新問題**: 13**
レポートの自動キャッシュ設定の目的は次の 2 つのうちどれですか? (2つお選びください。)
A. 新しいログが到着すると、hcache が自動的に更新されます。
B. レポート生成時の診断を提供します。
C. ログ挿入遅延率を軽減します。
D. レポートの作成時間を短縮します。
Answer: (解答を表示する**)**
参照：
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/384416/how-auto-cache-works
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/86926/enabling-auto-cache

最新問題**: 14**
インシデントの更新に関する通知の送信について正しいのはどれですか?
A. インシデントが更新または削除された場合にのみ通知を送信できます。
B. 複数の外部プラットフォームに通知を送信できます
C. 通知はメールでのみ送信できます。
D. 複数のファブリック コネクタを使用する場合、すべてのコネクタが同じ通知設定を持つ必要があります。
Answer: (解答を表示する**)**

最新問題: **15**
FortiAnalyzer レポートに関して正しい記述はどれですか? (2つお選びください)
A. FortiAnalyzer では、FortiGate デバイスのレポートのみが許可されます。
B. FortiAnalyzer はカスタム レポートを作成する機能を提供します。
C. FortiAnalyzer を使用すると、レポートの実行をスケジュールできます。
D. FortiAnalyzer には事前定義されたレポートのみが含まれています。
Answer: B,C (メーッセージを残す**)**

最新問題: **16**
不正な管理者が許可なく FortiAnalyzer にアクセスしていました。あなたは、その不正な管理者が FortiAnalyzer 上でどのようなアクティビティを実行したかを確認する必要があります。
これを達成するには、FortiAnalyzer で何ができるでしょうか?
A. [ログ ビュー] をクリックして、その管理者用のレポートを生成します。
B. FortiView をクリックして、その管理者向けのレポートを生成します。
C. [タスク モニター] をクリックして、その管理者が実行したタスクを表示します。
D. 不正な管理者によって実行されたタスクをファブリック ビューで表示します。
Answer: C (メーッセージを残す**)**

有効な **NSE5_FAZ-7.0** 問題集は GoShiken.com が提供された合格しやすい NSE5_FAZ-7.0 試験問題集！ GoShiken.com が最新の **NSE5_FAZ-7.0** 試験問題集を提供しています。GoShiken.com NSE5_FAZ-7.0 試験問題は最新で、解答が正確でございます。最新の GoShiken.com NSE5_FAZ-7.0 問題集をゲットする人はこちら: https://www.goshiken.com/Fortinet/NSE5_FAZ-7.0-mondaishu.html
(**11630%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **17**
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: (解答を表示する**)**
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

最新問題: **18**
管理者は次の設定を構成しました。

システム fortiview 設定を構成する
解決IPを有効に設定する
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、送信元 IP アドレスが FortiGate で解決されない場合にのみ使用します。
B. FortiAnalyzer 上の FortiView で宛先 IP アドレスをホスト名に解決します。
C. このコマンドが Forti Analyzer で IP アドレスを解決できるように、FortiGate でローカル DNS サーバーを構成する必要があります。
D. FortiAnalyzer 上の FortiView で、送信元および宛先 IP アドレスをホスト名に解決します。
Answer: (解答を表示する**)**

最新問題**: 19**
次の CLI コマンドの目的は何ですか?
A. ログファイルのチェックサムを追加する場合
B. MDのハッシュ値と認証コードを追加する場合
C. 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。
D. ログ通信を暗号化する場合
Answer: (解答を表示する**)**
https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global

最新問題**: 20**
FortiAnalyzer はどの 2 つの SAML ロールに対して構成できますか? (2つお選びください。)
A. 校長
B. サービスプロバイダー
C. ID コレクター
D. アイデンティティプロバイダー
Answer: (解答を表示する**)**
参照：
20the%20identity%20provider%20(IdP、external%20identity%20provider%20is%20available.
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/981386/saml-admin-authentication

最新問題**: 21**
次の CLI コマンドの目的は何ですか?
A. ログファイルのチェックサムを追加する場合
B. MDのハッシュ値と認証コードを追加する場合
C. 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。
D. ログ通信を暗号化する場合
Answer: (解答を表示する**)**
https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global

最新問題: **22**
展示品をご覧ください。
クォータの合計がシステム ストレージの合計よりも少ないのはなぜですか?
A. システム ストレージの 3.6% がすでに使用されています。
B. 一部のスペースは、圧縮ファイル、アップロード ファイル、一時レポート ファイルの保存など、システム使用のために予約されています。
C. oftpd プロセスはまだログをアーカイブしていません
D. ログファイルされたプロセスは合計クォータを見積もっているだけです
Answer: B (メーッセージを残す**)**
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation

最新問題: **23**
プレイブックには合計 5 つのタスクが含まれています。管理者がプレイブックを実行すると、5 つのタスクのうち 4 つが正常に終了しましたが、1 つのタスクは失敗しました。プレイブックの実行後のステータスはどうなりますか?
A. 成功
B. 失敗しました
C. 実行中
D. アップストリーム_失敗
Answer: B (メーッセージを残す**)**
1 つ以上の失敗したタスクを含む Playbook ジョブには、Playbook Monitor で 「失敗」というラベルが付けられます。FortiAnalyzer_7.0_スタディ ガイド ページ番号: 247 1 つ以上の失敗したタスクを含む Playbook ジョブには、Playbook Monitor で 「失敗」というラベルが付けられます。ただし、失敗ステータスは、すべてのタスクが失敗したことを意味するわけではありません。一部の個別のアクションは正常に完了した可能性があります。

最新問題: **24**
出力変数の目的は何ですか?
A. プレイブックの実行統計を保存するため
B. 前のタスクの出力を現在のタスクの入力として使用する場合
C. プレイブックで使用されるコネクタの詳細を表示するには
D. プレイブックのエクスポート時にすべてのタスク設定を保存するには
Answer: B (メーッセージを残す**)**
FortiAnalyzer_7.0_Study_Guide-Online.pdf ページ 242: 出力変数を使用すると、前のタスクからの出力を現在のタスクへの入力として使用できます。
出力変数を使用すると、前のタスクからの出力を現在のタスクへの入力として使用できます。FortiAnalyzer_7.0_Study_Guide-オンライン 242 ページ

最新問題: **25**

FortiAnalyzer による高可用性 (HA) ダスターの処理に関して正しい記述はどれですか? (2つお選びください)
A. FortiAnalyzer はクラスター内のプライマリ デバイスからのみ BGS を受信します。
B. FortiAnalyzer はシリアル番号によってさまざまなデバイスを区別します。
C. FortiAnalyzer はクラスター内のプライマリ デバイスのシリアル番号のみを知る必要があり、他のデバイスは自動的に検出されます。
D. FortiAnalyzer はダスター内の d デバイスからログを受信します。
Answer: (解答を表示する**)**

最新問題**: 26**
ローカル以外の管理者が単一の LDAP グループ内の任意のユーザー アカウントで FortiAnalyzer に認証できるようにするには、FortiAnalyzer でどの 2 つの設定を構成する必要がありますか? (2つお選びください。)
A. LDAP グループへのアクセスを制限する信頼できるホスト プロファイル
B. ローカルのワイルドカード管理者アカウント
C. リモート LDAP サーバー
D. 管理者グループ
Answer: B,C (メーッセージを残す**)**

最新問題**: 27**
ログ ビューでは、チャート ビルダー機能を使用して、フィルターされた検索結果に基づいてデータセットとチャートを構築できます。
同様に、FortiView ではどの機能を使用できますか?
A. チャートビルダーにエクスポート
B. カスタムチャートにエクスポート
C. レポートチャートにエクスポート
D. PDF にエクスポート
Answer: (解答を表示する**)**

最新問題**: 28**
FortiAnalyzer で管理アクセスを制御および制限する最も一般的な 2 つの方法はどれですか? (2つお選びください。)
A. 仮想ドメイン
B. 管理アクセスプロファイル
C. 信頼できるホスト
D. セキュリティ ファブリック
Answer: B,C (メーッセージを残す**)**
参照：
https://docs2.fortinet.com/document/fortianalyzer/6.0.0/administration-guide/581222/trusted-hosts

最新問題: **29**
出力変数の目的は何ですか?
A. 前のタスクの出力を現在のタスクの入力として使用する場合
B. プレイブックで使用されるコネクタの詳細を表示するには
C. プレイブックのエクスポート時にすべてのタスク設定を保存するには
D. プレイブックの実行統計を保存するため
Answer: (解答を表示する**)**

最新問題: **30**
fortinet 管理者は、ログを表示し、登録済みデバイスの追加や削除などのデバイス管理タスクを実行できます。ただし、管理者 fortinet は、電子メールの送信に使用できるモール サーバーを作成できません。
何が問題なのでしょうか?
A. フォーティネットには、Restricted_ User 管理者プロファイルが割り当てられます。
B. フォーティネットには Standard_User 管理者プロファイルが割り当てられます。
C. ADOM モードはアドバンスト モードで構成されています。
D. 信頼できるホストが構成されています。
Answer: B (メーッセージを残す**)**

最新問題: **31**
FortiAnalyzer レポートをサポートされている外部サーバーにアップロードするには、FortiAnalyzer で何を設定する必要がありますか?
(2つお選びください。)
A. SFTP、FTP、または SCP サーバー
B. メールサーバー
C. 出力プロファイル
D. レポートのスケジュール設定
Answer: (解答を表示する**)**
https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration-guide/598322/creating-output-profiles

有効な **NSE5_FAZ-7.0** 問題集は GoShiken.com が提供された合格しやすい NSE5_FAZ-7.0 試験問題集！ GoShiken.com が最新の **NSE5_FAZ-7.0** 試験問題集を提供しています。GoShiken.com NSE5_FAZ-7.0 試験問題は最新で、解答が正確でございます。最新の GoShiken.com NSE5_FAZ-7.0 問題集をゲットする人はこちら: https://www.goshiken.com/Fortinet/NSE5_FAZ-7.0-mondaishu.html
(**11630%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **32**
FortiAnalyzer の動作モードに関して正しい 2 つの記述はどれですか? (2つお選びください。)

A. コレクター モードの場合、FortiAnalyzer は複数のデバイスからログを収集し、これらのログを元のバイナリ形式で転送します。
B. コレクタ モードがデフォルトの動作モードです。
C. コレクタモード時。FortiAnalyzer は、イベント管理およびレポート機能をサポートしています。
D. コレクター モードとアナライザー モードを備えたさまざまな FortiAnalyzer デバイスをネットワークに展開することで、ログの受信、分析、レポートの全体的なパフォーマンスを向上させることができます。
Answer: A,D (メーッセージを残す**)**
参照：
https://docs.fortinet.com/document/fortianalyzer/7.0.0/administration-guide/312644/analyzer-collector-collaboration

最新問題**: 33**
FortiAnalyzer の高可用性 (HA) 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. FortiAnalyzer HA は VRRP がなくても機能します。VRRP は、クラスター内に 3 つ以上の FortiAnalyzer デバイスがある場合にのみ必要です。
B. FortiAnalyzer HA は、ログの同期と一部のシステム設定および構成設定をサポートします。
C. FortiAnalyzer HA クラスター内のすべてのデバイスは、同じ動作モード (アナライザーまたはコレクター) で実行する必要があります。
D. FortiAnalyzer HA の実装は、AWS、Microsoft Azure、Google Cloud などの多くのパブリック クラウド インフラストラクチャによってサポートされています。
Answer: B,C (メーッセージを残す**)**
参照：
FortiAnalyzer HA 実装は、仮想ルーター冗長プロトコル (VRRP) が許可されているネットワークでのみ機能します。したがって、一部のパブリック クラウド インフラストラクチャではサポートされていない可能性があります。

最新問題**: 34**
2 つの FortiAnalyzer デバイスで構成される HA クラスター上のファームウェアをアップグレードする場合、正しいのはどれですか?
A. まず、セカンダリ デバイスをアップグレードし、次にプライマリ デバイスをアップグレードします。
B. 両方の FortiAnalyzer デバイスが同時にアップグレードされます。
C. 無中断アップグレードを有効にすると、クラスター ファームウェアのアップグレード中に通常の FortiAnalyzer 操作が中断されなくなります。
D. コンソール接続のみを使用してファームウェアのアップグレードを実行できます。
Answer: A (メーッセージを残す**)**
FortiAnalyzer_7.0_Study_Guide-Online.pdf ページ 64: FortiAnalyzer HA クラスター ファームウェアをアップグレードするには:
1. 各セカンダリ デバイスにログインします。
2. すべてのセカンダリ デバイスのファームウェアをアップグレードします。

3. アップグレードが完了するまで待ち、すべてのセカンダリ デバイスがクラスタに参加していることを確認します。
4. すべてのセカンダリ デバイスのログがプライマリ デバイスと同期されていることを確認します。
5. プライマリ デバイスをアップグレードします。
https://docs.fortinet.com/document/fortianalyzer/7.2.0/upgrade-guide/262607/upgrading-fortianalyzer-firmware

最新問題: **35**
ログ転送に関する 2 つの記述のうち、正しいものはどれですか? (2つお選びください。)
A. 転送されたログは、特定の条件に一致するようにフィルタリングできません。
B. ログはリアルタイムのみで転送されます。
C. クライアントは、転送後にログのローカル コピーを保持します。
D. 集計モードは別の FortiAnalyzer でのみ使用できます。
Answer: C,D (メーッセージを残す**)**
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/420493/modes
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/621804/log-forwarding

最新問題: **36**
FortiAnalyzer の動作モードは何ですか? (2つお選びください)
A. アナライザー
B. マネージャー
C. スタンドアロン
D. コレクター
Answer: A,D (メーッセージを残す**)**

最新問題: **37**
ログ ビューでは、チャート ビルダー機能を使用して、フィルターされた検索結果に基づいてデータセットとチャートを構築できます。
同様に、FortiView ではどの機能を使用できますか?
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: (解答を表示する**)**
参照：
ログ ビューのチャート ビルダー機能と同様に、FortiView からチャートをエクスポートできます。チャートのエクスポートには、FortiView で設定したフィルターがすべて含まれます。FortiAnalyzer_7.0_Study_Guide-オンライン ページ。292.

最新問題: **38**

次の CLI コマンドを考えてみましょう。
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場合
C. ログファイルのチェックサムを追加する場合
D. ログ通信を暗号化する場合
Answer: (解答を表示する**)**
https://docs.fortinet.com/document/fortianalyzer/6.2.5/cli-reference/849211/global

最新問題**: 39**
FortiAnalyzer が FortiGate デバイスからログを収集するには、どのような構成が必要ですか? (2つお選びください。)
A. FortiGate でリモート ログを有効にする必要があります
B. ログ暗号化を有効にする必要があります
C. ADOM を有効にする必要があります
D. FortiGate を FortiAnalyzer に登録する必要があります
Answer: A,D (メッセージを残す**)**
ページ 70: FortiGate デバイスを FortiAnalyzer ユニットに追加して登録した後、FortiGate デバイスが FortiAnalyzer ユニットにログを送信するように設定されていることも確認する必要があります。」
https://docs.fortinet.com/uploaded/files/4614/FortiAnalyzer-5.4.6-Administration%20Guide.pdf ページ 45: FortiCarrier などの非 FORTIGATE デバイスのログとレポートをサポートするには、ADOM を有効にする必要があります」、FortiClientEMS、FortiMail、FortiWeb、FortiCache、および FortiSandbox。

最新問題**: 40**
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: B (メッセージを残す**)**
考えられるシナリオの 1 つをスライドに示します。
1. トラフィックは FortiGate を通過します
2.FortiGate が FortiAnalyzer にログを送信します
3. FortiAnalyzer が不審なトラフィックを検出し、イベントを生成します
4. イベントは、FortiAnalyzer でのプレイブックの実行をトリガーします。これにより、Webhook 呼び出しが FortiGate に送信され、自動化ステッチが実行されます。

5. FortiGate は、修正または予防アクションを使用して自動化ステッチを実行します」
FortiAnalyzer_7.0_Study_Guide-Online ページ 228 FOS コネクタに関連するアクションを確認するには、FortiGate 側で Incoming Webhook Call トリガーを使用して自動化ルールを有効にする必要があります。FortiAnalyzer_7.0_スタディ ガイド ページ番号 233

最新問題**: 41**
展示を参照してください。
FortiAnalyzer での自動キャッシュの有効化に関して正しい 2 つの記述はどれですか? (2つお選びください。)
A. FortiAnalyzer のディスク容量を節約するために、レポートのサイズが最適化されます。
B. レポートはメモリにキャッシュされます。
C. この機能は、スケジュールされたレポートに対して自動的に有効になります。
D. 自動キャッシュを有効にすると、データセットの組み立てに長時間を必要とするレポートの生成時間が短縮されます。
Answer: C,D (メーッセージを残す**)**
『レポート設定で自動キャッシュを有効にすると、レポートのパフォーマンスが向上し、レポートの生成時間が短縮されます。スケジュールされたレポートでは、自動キャッシュがすでに有効になっています。』FortiAnalyzer_7.0_Study_Guide-オンライン 306 ページ

最新問題**: 42**
FortiAnalyzer の侵害インジケーター機能は、感染したホストを特定するためにどのログ タイプを使用しますか?
A. ウイルス対策ログ
B. Webフィルタログ
C. IPS ログ
D. アプリケーション制御ログ
Answer: B (メーッセージを残す**)**
参照：
FortiAnalyzer_Admin_Guide/3600_FortiView/0200_Using_FortiView/1200_Compromized_hosts_page.htm?TocPath=FortiView%7CUsing%20FortiView%7C_____6

最新問題**: 43**
FortiAnalyzer のオフライン ログとは何ですか?
A. 圧縮ログはアーカイブ ログとも呼ばれ、オフライン ログとみなされます。
B. FortiAnalyzer を再起動したとき。保存されたすべてのログはオフライン ログとみなされます。
C. インデックスが付けられ、SQL データベースに保存されるログ。
D. オフラインデバイスの起動後に収集されるログ。
Answer: A (メーッセージを残す**)**
参照：

ログは受信され、FortiAnalyzer ディスク上のログ ファイルに保存されます。最終的に、ログ ファイルが設定されたサイズに達するか、設定されたスケジュールに従って、名前が変更されてロールオーバーされます。これらのファイル (ロールされたかどうかにかかわらず) はアーカイブ ログとして知られており、オフラインとみなされているため、即時の分析サポートは提供されません。これらを組み合わせると、アーカイブ クォータと保持制限の対象となり、ADOM データ ポリシーに基づいて削除されます。FortiAnalyzer_7.0_Study_Guide-オンライン 140 ページ

最新問題: **44**
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、パスワードをログ ファイルに記録し、暗号化します。
B. 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。
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: (解答を表示する**)**

最新問題: **45**
FortiAnalyzer のデータセット クエリの目的は何ですか?
A. データベースのスキーマを抽出します。
B. ログデータをデータベースに挿入します。
C. ログデータをテーブルにソートします。
D. データベースからログデータを取得します。
Answer: D (メーッセージを残す**)**

最新問題: **46**
展示を参照してください。
この展示では、「remoteservergroup」が LDAP サーバーと RADIUS サーバーを含む認証サーバー グループであることを示しています。
新しい管理者を構成するときに「リモート サーバー上のすべてのユーザーを一致させる」を有効にする重要性を表す 2 つのステートメントはどれですか? (2つお選びください。)
A. LDAP サーバーと RADIUS サーバーを使用してワイルドカード管理者を作成します。
B. LDAP および RADIUS サーバーからリモート管理を使用すると、いつでも FortiAnalyzer にログインできるようになります。
C. 管理者が 2 要素認証を使用できるようにします。
D. 管理者は、リモート サーバー LDAP および RADIUS 上の資格情報を使用して FortiAnalyzer にログインできます。

Answer: (解答を表示する**)**

有効な **NSE5_FAZ-7.0** 問題集は GoShiken.com が提供された合格しやすい NSE5_FAZ-7.0 試験問題集！ GoShiken.com が最新の **NSE5_FAZ-7.0** 試験問題集を提供しています。GoShiken.com NSE5_FAZ-7.0 試験問題は最新で、解答が正確でございます。最新の GoShiken.com NSE5_FAZ-7.0 問題集をゲットする人はこちら: https://www.goshiken.com/Fortinet/NSE5_FAZ-7.0-mondaishu.html (**11630%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題**: 47**
ファブリック ADOM をセットアップする 2 つの利点は何ですか? (2つお選びください。)
A. 高速なデータ処理とログの関連付けに使用できます。
B. 同じセキュリティ ファブリック内のデバイス間の通信を容易にするために使用できます。
C. 同じセキュリティ ファブリックの一部であるすべてのフォーティネット デバイスを含めることができます
D. 同じセキュリティ ファブリックの一部である FortiGate デバイスのみを含めることができます。
Answer: A,C (メーッセージを残す**)**
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-security-fabric-adom

最新問題**: 48**
HA クラスター内のプライマリ FortiAnalyzer に障害が発生した場合、新しいプライマリはどのように選択されますか?
A. 設定されている IP アドレスが最初にチェックされます。
B. アクティブなポート番号が最初にチェックされます。
C. 最初にファームウェアのバージョンを確認します。
D. 設定された優先度が最初にチェックされます。
Answer: (解答を表示する**)**
プライマリ デバイスに障害が発生した場合、FortiAnalyzer HA は次のルールを使用して新しいプライマリを選択します。
* すべてのクラスタ デバイスには 80 ～ 120 の優先順位が割り当てられます。デフォルトの優先順位は 100 です。プライマリ デバイスが使用できなくなった場合、最も高い優先順位を持つデバイスが新しいプライマリ デバイスとして選択されます。たとえば、優先度 110 のデバイスは、優先度 100 のデバイスよりも選択されます。
※ 複数のデバイスの優先順位が同じ場合、プライマリ IP アドレスの値が最も大きいデバイスが新しいプライマリ デバイスとして選択されます。たとえば、123.45.67.123 ではなく 123.45.67.124 が選択されます。
* より高い優先順位またはより大きな値の IP アドレスを持つ新しいデバイスがクラスターに参加した場合、新しいデバイスは現在のプライマリ デバイスを自動的に置き換え (または横取り) しません。

FortiAnalyzer_7.0_Study_Guide-オンライン 62 ページ

最新問題: **49**
ファブリック認証を使用して FortiAnalyzer で FortiGate を認証するには何が必要ですか?
A. 事前共有キー
B. 有効な FortiAnalyzer 認証情報
C. FortiGate のシリアル番号
D. FortiGate ADOM
Answer: A (メーッセージを残す**)**

最新問題: **50**
RAID 管理ページでは、ディスクのステータスが 「初期化中」と表示されます。
Initializing というステータスは、FortiAnalyzer が現在実行していることを示していますか?
A. FortiAnalyzer は冗長ドライブのパリティ データが有効であることを確認しています
B. FortiAnalyzer は、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。
C. FortiAnalyzer はアレイをフォールト トレラントにするためにすべてのハード ドライブに書き込み中です
D. FortiAnalyzer は正常に機能しています
Answer: (解答を表示する**)**
参照：
8977-00505692583a/FortiAnalyzer-5.6.10-管理ガイド.pdf (40)

最新問題: **51**
set log checksum コマンドを使用する目的は次のうちどれですか? (2つお選びください。)
A. FortiAnalyzer から SFTP サーバーへのログのアップロード中の中間者攻撃から保護するため
B. ログの改ざんや改ざんを防止するため
C. ログ通信を暗号化する場合
D. 同一のログのセットを 2 番目のログ サーバーに送信します。
Answer: A,B (メーッセージを残す**)**
ストレージ内でのログの改ざんを防ぐために、config system global コマンドを使用してログ チェックサムを追加できます。ログがローリングおよびアーカイブされるとき、およびログがアップロードされるとき (その機能が有効な場合)、ログ ファイルのハッシュ値、タイムスタンプ、および認証コードを記録するように FortiAnalyzer を構成できます。これは、ログのアップロード中に FortiAnalyzer から SSH ファイル転送プロトコル (SFTP) サーバーに送信する場合にのみ、中間者攻撃に対しても役立ちます。
FortiAnalyzer_7.0_Study_Guide-オンライン 149 ページ

最新問題: **52**
展示を参照してください。
この画像は、管理者が既存の HA クラスタに参加したい FortiAnalyzer の構成を示しています。

表示された構成から何を結論付けることができますか?
A. この FortiAnalyzer は既存の HA クラスターにプライマリとして参加します。
B. この FortiAnalyzer は、port1 でログを受信するように構成されています。
C. この FortiAnalyzer は、ピアとの通信が 10 秒間失われた後、フェイルオーバーをトリガーします。
D. クラスターに参加した後、この FortiAnalyzer は更新されたログ データベースを保持します。
Answer: B (メーッセージを残す**)**
優先ロールがプライマリの場合、新しい HA クラスタで最初に設定されていれば、このユニットがプライマリ ユニットになります。既存のプライマリ ユニットが存在する場合、このユニットはセカンダリ ユニットになります。」(https://docs.fortinet.com/document/fortianalyzer/7.0.5/administration-guide/275104)

最新問題**: 53**
FortiAnalyzer のログ転送に関して正しい 2 つの記述はどれですか? (2つお選びください。)
A. 転送モードは、他の FortiAnalyzer デバイスにのみリアルタイムでログを転送します。
B. アグリゲーション モードでは、ログとコンテンツ ファイルが保存され、スケジュールされた時間に別の FortiAnalyzer デバイスにアップロードされます。
C. アグリゲーション モードでは、syslog サーバーと CEF サーバーにもログを転送できます。
D. 転送と集約の両方のモードで、デバイス間のログの暗号化がサポートされています。
Answer: A,B (メーッセージを残す**)**

最新問題**: 54**
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: (解答を表示する**)**
https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/743670/cconfiguring-log-storage-policy

Valid NSE5_FAZ-7.0 Dumps shared by GoShiken.com for Helping Passing NSE5_FAZ-7.0 Exam! GoShiken.com now offer the **newest NSE5_FAZ-7.0 exam dumps**, the GoShiken.com NSE5_FAZ-7.0 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com NSE5_FAZ-7.0 dumps with Test Engine here: https://www.goshiken.com/Fortinet/NSE5_FAZ-7.0-mondaishu.html (**116** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)