VMware.5V0-41.21.v2023-03-07.q24

試験コード:	5V0-41.21
試験名称:	VMware NSX-T Data Center 3.1 Security
認定資格:	VMware
無料問題数:	24
バージョン:	v2023-03-07
アクセス数:	390
ページビュー数:	240
https://www.jpnpdf.com/VMware.5V0-41.21.v2023-03-07.q24-mondaishu.html	

最新問題: **1**
NSX-T で URL 分析を使用する場合、TCP および UDP 経由でトラフィックをキャプチャするために URL ルールで設定する必要がある 2 つのサービスはどれですか? (2つ選んでください。)
A. DHCPv6
B. DNS
C. DHCP
D. DNS-TSIG
E. DNS-UDP
Answer: (解答を表示する)

最新問題: **2**
セキュリティ管理者は最近、NSX-T Data Center でゲスト イントロスペクションを有効にしました。
Microsoft Windows ベースの VM で情報が報告されない理由はどれですか?
A. VMware Tools を再構成する必要があります。
B. Windows VM は再起動が必要です。
C. NSX Manager を再構成する必要があります。
D. NSX Manager には再起動が必要です。
Answer: C (メーッセージを残す)

最新問題: **3**
NSX 管理者は、sa-web-01 仮想マシン トラフィックをキャプチャするために、sa-web-01 仮想マシンの dvfilter 名を見つけようとしています。コマンド出力に sa-web-01 VM dvfilter 名が表示されない理由は何ですか?
A. ESXi ホストで sa-web-01 の電源がオフになっています。
B. ESXi ホストで 5SH が無効になっています。
C. ESXi ホストのファイアウォールはオフになっています。
D. sa-web-01 VM にはファイアウォール ルールが構成されていません。

Answer: A (メーッセージを残す)

最新問題: **4**
CLI 出力を参照してください。

```
[root@sa-esxi-03:~] vsipioctl getfwconfig -f nic-266154-eth0-vmware-sfw.2
ruleset mainrs {
rule 3054 at 1 (s) inout protocol tcp strict from addrset 6a966fb0-6388-42d7-9585-03acee45028e to addrset 04ee3f8f-af45-45d3-a7d3-43843216c5cf port
8443 accept;
rule 3055 at 2 (s) inout protocol tcp strict from addrset 04ee3f8f-af45-45d3-a7d3-43843216c5cf to addrset c104b8af-4de9-4779-8d00-aa329991305a port
80 accept;
rule 3056 at 3 inout protocol any from addrset 084bb65c-a4b9-45c2-b743-1477fcfffe15 to addrset 084bb65c-a4b9-45c2-b743-1477fcfffe15 reject;
}

addrset 04ee3f8f-af45-45d3-a7d3-43843216c5cf {
ip 172.16.20.11,
}
addrset 084bb65c-a4b9-45c2-b743-1477fcfffe15 {
ip 172.16.10.11,
ip 172.16.20.11,
ip 172.16.30.11,
}
addrset 6a966fb0-6388-42d7-9585-03acee45028e {
ip 172.16.10.11,
ip 172.16.10.12,
}

addrset c104b8af-4de9-4779-8d00-aa329991305a {
ip 172.16.30.11,
}
```

HTTP トラフィックを受け入れるための分散ファイアウォール ルールの送信元 IP アドレスは?
A. 172.16.10.12
B. 172.16.20.11
C. 172.16.10.11
D. 172.16.30.11
Answer: C (メーッセージを残す)

最新問題: **5**
ネットワークに接続されたデバイスのゼロトラスト ネットワークの主な概念を説明しているのは、次のうちどれですか?
A. ネットワークに接続されたデバイスは、ユーザーが正常に認証された場合にのみ信頼されるべきです。
B. ネットワークに接続されたデバイスは、組織の境界内にある場合にのみ信頼する必要があります。
C. ネットワークに接続されたデバイスは、その身元と完全性が継続的に検証できる場合にのみ信頼されるべきです。
D. ネットワークに接続されたデバイスは、組織によって発行された場合にのみ信頼する必要があります。
Answer: A (メーッセージを残す)

最新問題: **6**
NSX 管理者は、リモート ログ サーバー (192.168.110.60) を構成して、FW 接続とパケット ログをリモート ログ サーバーに送信する任務を負っています。管理者は、NSX-T 3.1 ドキュメントにある次のコマンド構文を使用しています。

```
set logging-server <hostname-or-ip-address[:port]> proto <proto> level <level> [facility <facility>] [messageid <messageid>] [serverca <filename>]
[clientca <filename>] [certificate <filename>] [key <filename>] [structured-data <structured-data>]
```

管理者が構成タスクを完了するために使用するコマンドは次のうちどれですか?
A. logging-server 192.168.110.60 proto udp レベル情報機能 syslog メッセージ Id FIREWALL-CONNECTION を設定します。
B. logging-server 192.168.110.60 proto udp レベル情報機能 syslog メッセージ ID FIREWALL-PKTLOG を設定します。
C. ロギング サーバー 192.168.110.60 proto udp レベル情報機能 syslog メッセージを設定します!-モニター。ファイアウォール

D. ログ サーバー 192.168.110.60 proto udp levelinfo ファシリティ syslog メッセージ ID システム、ファブリックを設定します。
Answer: B (メーッセージを残す**)**

最新問題**: 7**
NSX Distributed Firewall の使用例を 2 つ選んでください (2 つ選択してください)。
A. セグメンテーションによるゼロトラスト
B. ネットワークの可視化
C. ソフトウェア定義ネットワーキング
D. セキュリティ分析
E. 攻撃防止の横移動
Answer: (解答を表示する**)**

最新問題**: 8**
管理者は、NSX-T のログを構成して、ファイアウォール セキュリティ ポリシーの変更を監査する必要があります。管理者は、NSX-T3.1 ドキュメントの次のコマンドを使用しています。

```
set logging-server <hostname-or-ip-address[:port]> proto <proto> level <level> [facility <facility>] [messageid <messageid>] [serverca <filename>] [clientca
<filename>] [certificate <filename>] [key <filename>] [structured-data <structured-data>]
```

次のリストから、管理者がファイアウォール セキュリティ ルールの変更を追跡できるようにするメッセージ ID はどれですか?
A. システム
B. モニター
C. ファイアウォール
D. 生地
Answer: B (メーッセージを残す**)**

最新問題**: 9**
ESXi ホストのファイアウォール構成を一覧表示する esxcli コマンドはどれですか?
A. vsipioct1 getrules -f <フィルター名>
B. esxcli ネットワーク ファイアウォール ルール
C. vsipioct1getrules -filter <フィルター名>
D. esxcli ネットワーク ファイアウォール ルールセット リスト
Answer: D (メーッセージを残す**)**

最新問題**: 10**
中央制御プレーンからファイアウォール構成を受け取るトランスポート ノードのコンポーネントはどれですか?
A. nsx-appl-proxy
B. nsx-ccp
C. nsx-mpa
D. nsx プロキシ
Answer: (解答を表示する**)**

最新問題**: 11**

企業の CTO は、すべての NSX-T Data Center Distributed Firewall ルールに対してすべてのログを有効にするよう要求しました。このリクエストを実行する前に考慮すべきことは何ですか?
A. ロギングはセクションに対してのみ有効にでき、単一のルールに対しては有効にできません。
B. 大量のログ情報がパフォーマンスに影響を与える可能性があります。
C. 大量のログ情報により、vSphere Server データベースがいっぱいになる可能性があります。
D. すべてのルールでログを有効にすると、後で無効にすることはできません。
Answer: D (メーッセージを残す)

最新問題**: 12**
East-West サービス挿入の挿入ポイントはどれですか?
A. トランスポート ノード
B. パートナー SVM
C. Tier-1 ゲートウェイ
D. ゲスト VM vNIC
Answer: (解答を表示する)

最新問題**: 13**
NSX Intelligence の推奨セッションで出力として提供される 3 つのセキュリティ オブジェクトはどれですか?
（3つ選んでください。）
A. セキュリティ グループ
B. 分散ファイアウォール ルール
C. コンテキスト プロファイル
D. セキュリティ サービス
E. ゲートウェイ ファイアウォール ルール
Answer: (解答を表示する)

最新問題**: 14**
N5X 管理者が分散ファイアウォール ルールのロギングをオンにしました。ESXi ホストでは、ログはどこに保存されますか?
A. /var/log/hostd.log
B. /var/log/esxupdate.log
C. /var/log/dfwpktlogs.log
D. /var/log/vmkerntl.log
Answer: C (メーッセージを残す)

最新問題**: 15**
セキュリティ管理者は、NSX 分散ファイアウォールを使用して East-West 仮想マシン トラフィックを保護する必要があります。ルールを適用する前に、仮想マシンの vNIC で完了する必要があること
A. トランスポート ゾーンに接続されています。
B. NSX 管理セグメントに接続されています。
C. vSphere 標準スイッチに接続する必要があります。

D. 下敷きとつながっています。
Answer: B (メーッセージを残す**)**

最新問題**: 16**
セキュリティ管理者が NSX Intelligence を検出用に構成しました。彼らは、1 時間ごとに入力エンティティの範囲の変更に基づいて推奨事項を取得したいと考えています。
要件を達成するために何を構成する必要がありますか?
A. 推奨事項を公開します。
B. 時間範囲を 1 時間に調整します。
C. 監視オプションをオンに切り替えます。
D. 新しいレコメンデーションを開始します。
Answer: C (メーッセージを残す**)**

最新問題**: 17**
NSX ゲートウェイ ファイアウォールについて正しいものはどれですか? 2つ選んでください。)
A. システム カテゴリのファイアウォール ルールは編集できません。
B. 適用先は、ファイアウォール ポリシー レベルで構成できます。
C. セキュリティ グループは適用先列で使用できます。
D. Pre Rule カテゴリのファイアウォール ルールがすべてのゲートウェイに適用されます。
E. NSX ゲートウェイ ファイアウォール ポリシーで NAT サービスを構成できます。
Answer: (解答を表示する**)**

最新問題**: 18**
ある組織が、請負業者の仮想デスクトップにセキュリティ制御を追加したいと考えています。NSX Identity ファイアウォール ルールを構成する場合、正しいものはどれですか?
A. ユーザー ID は、ファイアウォール ルールの宛先セクションでのみ使用できます。
B. ユーザー ID は、ファイアウォール ルールのソースまたは宛先セクションでは使用できません。
C. ユーザー ID は、ファイアウォール ルールのソース セクションと宛先セクションの両方で使用できます。
D. ユーザー ID は、ファイアウォール ルールのソース セクションでのみ使用できます。
Answer: (解答を表示する**)**

最新問題**: 19**
ユーザーが 192.168.1.100 と 192.168.1.101 の間で ICMP をブロックできるようにする NSX の機能は何ですか?

A. NSX Distributed Switch エージェント
B. NSX 分散 IDS/IPS
C. NSX 分散ファイアウォール
D. NSX 分散ルーティング
Answer: D (メーッセージを残す)

最新問題**: 20**
セキュリティ管理者は、NSX 分散 IDS/IPS ポリシーを更新して、標的のシステムからの認証情報の盗難につながる重要な CVSS スコアを伴う新しい攻撃を検出する必要があります。
どのアクションを実行する必要がありますか?
A. * [セキュリティ] > [分散 IDS/IPS] > [ルール] から分散 IDS ルールを編集します。
* 攻撃の種類でフィルター処理し、[資格情報の盗難が検出されました] を選択します。
*検出および防止する更新モード
* 歯車のアイコンをクリックし、方向を OUT に変更します
B. * [セキュリティ] > [分散 IDS/IPS] > [ルール] から分散 IDS ルールを編集します。
* 攻撃の種類でフィルター処理し、[資格情報の盗難が検出されました] を選択します。
*検出および防止する更新モード
* 歯車のアイコンをクリックし、方向を IN-OUT に変更します
C. * [セキュリティ] > [分散 IDS] > [プロファイル] から新しいプロファイルを作成します
* Critical 重大度を選択し、攻撃タイプでフィルタリングして、Success Credential Theft Detected を選択します
* Distributed IDS ルールでプロファイルが適用されていることを確認します
* Distributed IDS アラートを監視して、変更が適用されていることを確認する
D. * 分散型 IDS/IPS シグネチャ データベースを更新する
* Security > Distributed IDS > Profiles からプロファイルを編集します
* Critical 重大度を選択し、攻撃タイプでフィルタリングして、Success Credential Theft Detected を選択します
* Distributed IDS ルールでプロファイルが適用されていることを確認します
Answer: (解答を表示する)

最新問題**: 21**
セキュリティ管理者は、NSX サービス インスタンスの健全性ステータスを確認しています。
ヘルス ステータスが Up と表示されるには、どの 2 つのパラメータが機能している必要がありますか? 2つ選んでください。)
A. VM には、既存のエンドポイント保護ルールがあってはなりません。
B. VM には少なくとも 1 つの vNIC が必要です。
C. VM の電源が入っている必要があります。
D. ホストで VM が使用可能である必要があります。
E. VM には、仮想ハードウェア バージョン 9 以降が必要です。
Answer: D,E (メーッセージを残す)

最新問題**: 22**

NSX-T Data Center Distributed Firewall の時間ベースのルール発行を使用する前に、各トランスポート ノードで何を構成する必要がありますか?
A. NAT
B. DNS
C. パット
D. NTP
Answer: D (メーッセージを残す**)**

最新問題**: 23**
NSX Intelligence について正しい記述はどれですか? 2つ選んでください。)
A. NSX Intelligence は、分散ファイアウォール ルールとポリシーの計画をサポートします。
B. NSX Intelligence は、パートナー SVM を使用したサービス挿入の構築を支援します。
C. NSX Intelligence は、NSX-T Edge ファイアウォールのルールとポリシーの計画をサポートします。
D. NSX Intelligence は、vRealize Network Insight と組み合わせて使用できます。
E. NSX Intelligence は、ネットワークの物理インフラストラクチャを視覚化するのに役立ちます。
Answer: A,D (メーッセージを残す**)**

最新問題**: 24**
リダイレクトされた North-South トラフィックを効率的に処理するために、パートナー セキュリティ仮想マシン (パートナー SVM) はどこにデプロイされていますか?
A. NSX Edge ノードの近くにデプロイされます。
B. コンピューティング ノードの近くにデプロイされます。
C. パートナー マネージャーの近くに配置されます。
D. VMware vCenter Server の近くにデプロイされます。
Answer: D (メーッセージを残す**)**