# Cisco.300-445.v2026-07-08.q119

| | |
|---|---|
| 試験コード： | 300-445 |
| 試験名称： | Designing and Implementing Enterprise Network Assurance |
| 認証ベンダー： | Cisco |
| 無料問題の数： | 119 |
| バージョン： | v2026-07-08 |
| ページの閲覧量： | 107 |
| 問題集の閲覧量： | 1224 |

https://www.jpnshiken.com/shiken/Cisco.300-445.v2026-07-08.q119.html

**質問: 1**

Ciscoのネットワーク保証プラットフォームを選択する際、効率的なネットワークトラブルシューティングのために優先すべき要素は何ですか？

**A.** ネットワーク美学

**B.** お客様の声

**C.** アラートメカニズム

**D.** 履歴データの保存

正解: **C** (コメントを発表する)

効率的なネットワークのトラブルシューティングと問題解決のためにCiscoのネットワーク保証プラットフォームを選択する際には、アラートメカニズムの優先順位付けが非常に重要です。

**質問: 2**

エンドポイントを別のネットワークに移動した後、エンドポイントがオンライン表示されなくなりました。顧客はエンドポイントのログを確認しましたが、不審な点は見つかりませんでした。また、エンドポイントは以前のネットワークではオンラインであり、新しいネットワークも完全に動作していることを確認しました。新しいネットワークに移動した他のエンドポイントもオンラインです。新しいネットワークは小規模であるため、管理者は静的IPアドレス割り当てを使用しています。エンドポイントをオンラインにする最善の方法は何でしょうか？

```
2024-05-07 13:20:12.452 DEBUG [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:206 - RECONNECT is currently scheduled or running, ignoring schedule attempt for CONNECT
2024-05-07 13:20:14.468 DEBUG [3068.8116] agent.services.AgentSettingsService@DefaultAgentSettingsService.cpp:496 - Checkin failed with error code: 1
2024-05-07 13:20:14.468 DEBUG [3068.8116] agent.services.AgentSettingsService@DefaultAgentSettingsService.cpp:558 - Calling connect on persistent connection
2024-05-07 13:20:14.468 DEBUG [3068.8116] agent.services.AgentSettingsService@DefaultAgentSettingsService.cpp:576 - Will consider polling for scheduled tests in 30s
2024-05-07 13:20:14.468 DEBUG [3068.8116] agent.services.AgentSettingsService@DefaultAgentSettingsService.cpp:432 - Scheduling checkin in 10m
2024-05-07 13:20:14.468 DEBUG [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:198 - Running pre-schedule checks for CONNECT, isRetry=false, prev=CONNECT, current=RECONNECT, next=NONE
2024-05-07 13:20:14.468 DEBUG [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:206 - RECONNECT is currently scheduled or running, ignoring schedule attempt for CONNECT
2024-05-07 13:20:24.753 DEBUG [3068.8240] system.etwTraceConsumer@DefaultEtwTraceConsumer.cpp:108 - Flushed ETW trace buffers to file. path="C:\ProgramData\ThousandEyes\Endpoint Agent\etwTraces\ThousandEyes Endpoint Agent.etl", size=320kB
2024-05-07 13:20:24.765 DEBUG [3068.8240] net.SocketMonitoring@WinSocketMonitoringService.cpp:335 - Processed ETW event batch: published=2, stale=213, deduped=0, duplicatesDueToCoalesceInterval=0, skipped=41
2024-05-07 13:20:24.812 DEBUG [3068.7712] scheduler.task.statscommitter@UsageStatsCommitter.cpp:43 - Starting UsageStatsCommitter task
2024-05-07 13:20:24.813 DEBUG [3068.7712] tests.scheduledtestsmetric@DefaultScheduledTestsMetricsService.cpp:54 - End metric tracking period at: 2024-May-07 13:20:24.812000
2024-05-07 13:20:24.813 DEBUG [3068.7712] scheduler.task.statscommitter@UsageStatsCommitter.cpp:95 - Updated usage stats object with 69 entries.
2024-05-07 13:20:25.109 DEBUG [3068.2148] scheduler.simple@DefaultTaskScheduler.cpp:173 - Scheduled task: te::agent::UsageStatsCommitter/0x1, delay=60000 ms
2024-05-07 13:20:28.498 DEBUG [3068.2148] net.WinHttpClient@WinHttpClient.cpp:2115 - Request to: wss://c1.eb.thousandeyes.com/relay/connect timed out: 12002: The operation timed out
2024-05-07 13:20:28.499 DEBUG [3068.8240] net.WinHttpClient@WinHttpClient.cpp:2115 - Request to: https://c1.eb.thousandeyes.com/status.json timed out: 12002: The operation timed out
2024-05-07 13:20:28.499 DEBUG [3068.4352] net.DefaultWebSocketStompConnection@DefaultWebSocketStompConnection.cpp:135 - Websocket connection wait: 42108ms
2024-05-07 13:20:28.499 ERROR [3068.4352] net.DefaultWebSocketStompConnection@DefaultWebSocketStompConnection.cpp:148 - asyncOpen (Websocket): Input/output error [generic:5]
2024-05-07 13:20:28.499 ERROR [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:317 - asyncOpen: Input/output error [generic:5]
2024-05-07 13:20:28.499 DEBUG [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:485 - Running post-run checks for RECONNECT, next=NONE, retry=true
2024-05-07 13:20:28.499 DEBUG [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:198 - Running pre-schedule checks for RECONNECT, isRetry=true, prev=RECONNECT, current=NONE, next=NONE
2024-05-07 13:20:28.499 DEBUG [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:300 - Set schedule delay=1500ms, jitter=323ms, nextDelay=2250ms
2024-05-07 13:20:28.499 INFO  [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:226 - Scheduling RECONNECT after 1823ms
2024-05-07 13:20:28.771 INFO  [3068.8072] agent.services.CheckinService@CheckinService.cpp:422 - Checking in with ThousandEyes backend. Last successful check-in: 2024-May-07 13:16:04.698000. Last attempt: 2024-May-07 13:18:24.548000
2024-05-07 13:20:28.771 DEBUG [3068.8072] api.usp@UserSpaceProxyClient.cpp:50 - Relaying HTTP request https://c1.eb.thousandeyes.com/eyebrow/enterprise/agent/checkin to user space proxy
2024-05-07 13:20:30.327 DEBUG [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:244 - Running RECONNECT now
2024-05-07 13:20:30.327 DEBUG [3068.4352] net.DefaultWebSocketStompConnection@DefaultWebSocketStompConnection.cpp:308 - STOMP connection closed successfully
2024-05-07 13:20:30.327 DEBUG [3068.4352] net.DefaultWebSocketStompConnection@DefaultWebSocketStompConnection.cpp:327 - Websocket connection closed successfully
```

**A.** 新しいネットワークの容量不足が原因かもしれません。エンドポイントを古いネットワークに戻してください。

**B.** エンドポイントエージェントを再インストールしてオンラインにする必要があります。これは常に効果があります。

**C.** エンドポイントは10〜15分後に自動的にオンラインになります。操作は不要です。

**D.** エンドポイントのIP設定とc1.eb.thousandeyes.comへの接続を確認する必要があります。

正解: **D** (コメントを発表する)

エンタープライズ ネットワーク保証の設計と実装 (300-445 ENNA) カリキュラムでは、エンドポイント接続のトラブルシューティングには、ローカル デバイス ログとネットワーク環境の変更の体系的な分析が必要です。図に示されているログ メッセージによると、エージェントが ThousandEyes バックエンドにアクセスしようとしたときに、特定のタイムアウト エラーが発生していました。ログには、次のように明示的に記載されています。リクエスト先: wss://c1。
eb.thousandeyes.com/relay/connect がタイムアウトしました: 12002: 操作がタイムアウトしました。
エンドポイントが静的IPアドレス割り当てを使用する新しいネットワークに移動され、同じネットワーク上の他のエンドポイントは正常に機能していることから、問題はこの特定のデバイスの設定に限ったものであると考えられます。静的IP環境では、IPアドレス、サブネットマスク、デフォルトゲートウェイ、またはDNSサーバーの手動入力時の人為的ミスが、接続障害の一般的な根本原因となります。ゲートウェイが間違っている場合、エージェントはインターネットにアクセスできません。DNSが間違っている場合、c1.eb.thousandeyes.comを解決できません。したがって、エンドポイントをオンラインにする最善の方法は、IP設定の正確性を確認し、ThousandEyesリレーURLへの直接接続をテストすることです。
代替案では、ログに記録されている技術的な証拠に対処できていない。
* オプションA :デバイスを元の場所に戻すことは、デバイスが新しい場所で機能する必要性を解決するものではない後退的な措置です。
* オプション B: ソフトウェアの再インストールは 「力任せ」の方法であり、誤った静的 IP アドレスなどの根本的なネットワーク層の設定ミスを修正することはめったにありません。
* オプション C:タイムアウトエラー (12002) は、管理者の介入なしには解決しない、持続的な接続ブロックを示しています。
静的IPアドレスの認証情報を確認することで、デバイスがインターネットへの有効な経路を確保し、ThousandEyesプラットフォームへのセキュアなWebSocket（WSS）接続を確立できることが保証されます。

質問: **3**
ネットワーク保証のためのエージェント配置場所を決定する際、遅延を最小限に抑えるために不可欠な考慮事項は何ですか？
**A.** ネットワークトポロジー
**B.** 規制遵守
**C.** セキュリティ要件
**D.** 地理的分布
正解: **(**正解を表示します**)**
ネットワークの安全性を確保するためにエージェントの位置を決定する際、地理的な分散は遅延を最小限に抑え、効率的なデータ収集と監視のためにネットワークエンドポイントへの近接性を確保するために不可欠です。

質問: **4**
ネットワークエンジニアが、アプリホスティングを使用してスイッチ上にThousandEyes Dockerエージェントをデプロイします。エージェントはプロキシサーバー経由で通信する必要がありますが、初期デプロイ時にこの設定が漏れていました。エンジニアは、アプリホスティングの設定にプロキシ設定を追加します。エージェントがプロキシを使用し、ThousandEyesポータルでオンラインとして表示されるようにするには、次にどのような手順を踏めばよいでしょうか？
**A.** app-hosting stop appid agentname を実行してから app-hosting start appid agentname を実行してコンテナを再起動します。
**B.** 正しいプロキシ設定を使用して、app-hosting install コマンドでエージェントを再インストールします。
**C.** エージェントのライフサイクル全体を実行します: app-hosting stop appid agentname、app-hosting deactivate appid agentname、app-hosting activate appid agentname、app-hosting start appid agentname
**D.** 操作は不要です。エージェントが自動的に設定を取得します。
正解: **C (**コメントを発表する**)**
『Designing and Implementing Enterprise Network Assurance (300-445 ENNA)』実装ガイドでは、Cisco IOS XEアプリケーションホスティングのライフサイクルは、トラブルシューティングと構成管理において重要な概念です。アプリケーションホスティング構成でプロキシ設定などのアプリケーション環境変数が変更された場合、コンテナを単に再起動するだけでは不十分です。
正しい手順は、アプリケーションを 「構成済み」状態に戻してから 「実行中」状態に戻すことです。これには、4段階のライフサイクル実行が必要です （オプションC）。
* Stop: 現在実行中のコンテナのインスタンスを終了します。
* 非アクティブ化: ハードウェア リソース (CPU、メモリ、仮想インターフェイス) を解放し、重要なことに、以前のランタイム構成を切り離します。
* Activate: リソースを再割り当てし、新しい構成パラメータ (更新されたプロキシ設定を含む) をコンテナの環境に注入します。

* 開始: 新しく適用された構成でコンテナを初期化します。
非アクティブ化/アクティブ化シーケンスがない場合、コンテナは最初のアクティブ化時に存在していた環境変数を引き続き使用するため、プロキシなしでは ThousandEyes ポータルにアクセスできず、エージェントはオフラインのままになります。再インストール (オプション B) は不要で時間のかかる手順であり、イメージの再ダウンロードまたは再コピーが必要となります。一方、何もしない (オプション D) では、エージェントの接続ステータスに変更はありません。

質問: **5**
Thousand Eyesを使用してテストを設定する際、「Web」という用語は通常何を指しますか？
**A.** インターネット閲覧パフォーマンス
**B.** Webサーバーのセキュリティ
**C.** ウェブトラフィックの暗号化
**D.** Webアプリケーションの動作
正解: **D** (コメントを発表する)
Thousand Eyesの文脈において、「Web」という用語は通常、最適なパフォーマンスとユーザーエクスペリエンスを確保するために、ページ読み込み時間、HTTPリクエスト、レスポンスコードなど、Webアプリケーションの動作を監視および分析することを指します。

質問: **6**
添付資料を参照してください。エンドポイントのIP認証情報は以下のとおりです。
192.168.100.9/24、DNS: 8.8.8.8、8.8.4.4、GW: 192.168.100.1
展示資料に示された見解に基づくと、5月5日（日）23:27（GMT+2）に発生したエラーの原因は何だったのでしょうか？

VIEWS

CTF ▾ Run Now ▾ Add a filter ▾ Save and Share

Dynamic Tests >

Scheduled Tests

**HTTP Server**

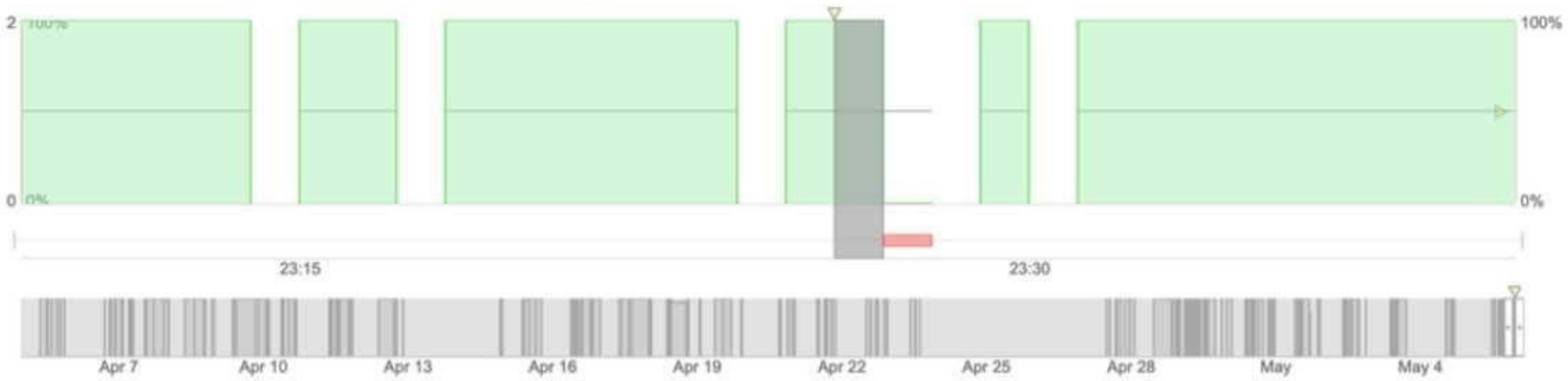
Network

Real User Tests >

Local Networks >

24h 7d 14d Metric **Availability**

Average Availability Number of Agents




Map **Table**

Showing data from **Sun, May 5 23:26 - 23:27 GMT+2** (15 minutes ago) Latest

Search... 0 selected Apply To Filter View Path

| Agent | Date (GMT+2) | Target IP | Response | No. of Redirects | Error Type ↓ | Error Details |
|---|---|---|---|---|---|---|
| OATROSHC-M-J015 | 2024-05-05 23:26:17 | 172.67.68.44 | 200 [Headers] | – | – | – |

VIEWS

CTF ▾ Run Now ▾ Add a filter ▾

Save and Share

Dynamic Tests >

Scheduled Tests

**HTTP Server**

Network

Real User Tests >

Local Networks >

24h 7d 14d Metric **Availability**

Average Availability  Number of Agents


Map **Table**

Showing data from **Sun, May 5 23:27 - 23:28 GMT+2** (15 minutes ago)

Latest

Search...  0 selected  Apply To Filter  View Path

| Agent | Date (GMT+2) | Target IP | Response | No. of Redirects | Error Type ↓ | Error Details |
|---|---|---|---|---|---|---|
| OATROSHC-M-J015 | 2024-05-05 23:27:07 | – | | – | DNS | The host name could not be resolved. |

VIEWS

CTF ▾ Run Now ▾ Add a filter ▾ Save and Share

Dynamic Tests >

Scheduled Tests

HTTP Server

**Network**

Real User Tests >

Local Networks >

24h 7d 14d Metric **Loss** ▾

Average Loss Number of Agents


**Path Visualization** Map Table

Showing data from **Sun, May 5 23:26 - 23:27 GMT+2** (17 minutes ago) ◂ ▸ Latest→|

Showing: VPN **Overlay** ▾ Add a filter ▾

Grouping: Agents by **Network** ▾ Interfaces by **Network** ▾

Highlighting: **Forwarding Loss > 10 %** ( 0 nodes ) ▾ **Link Delay > 100 ms** ( 0 links ) ▾

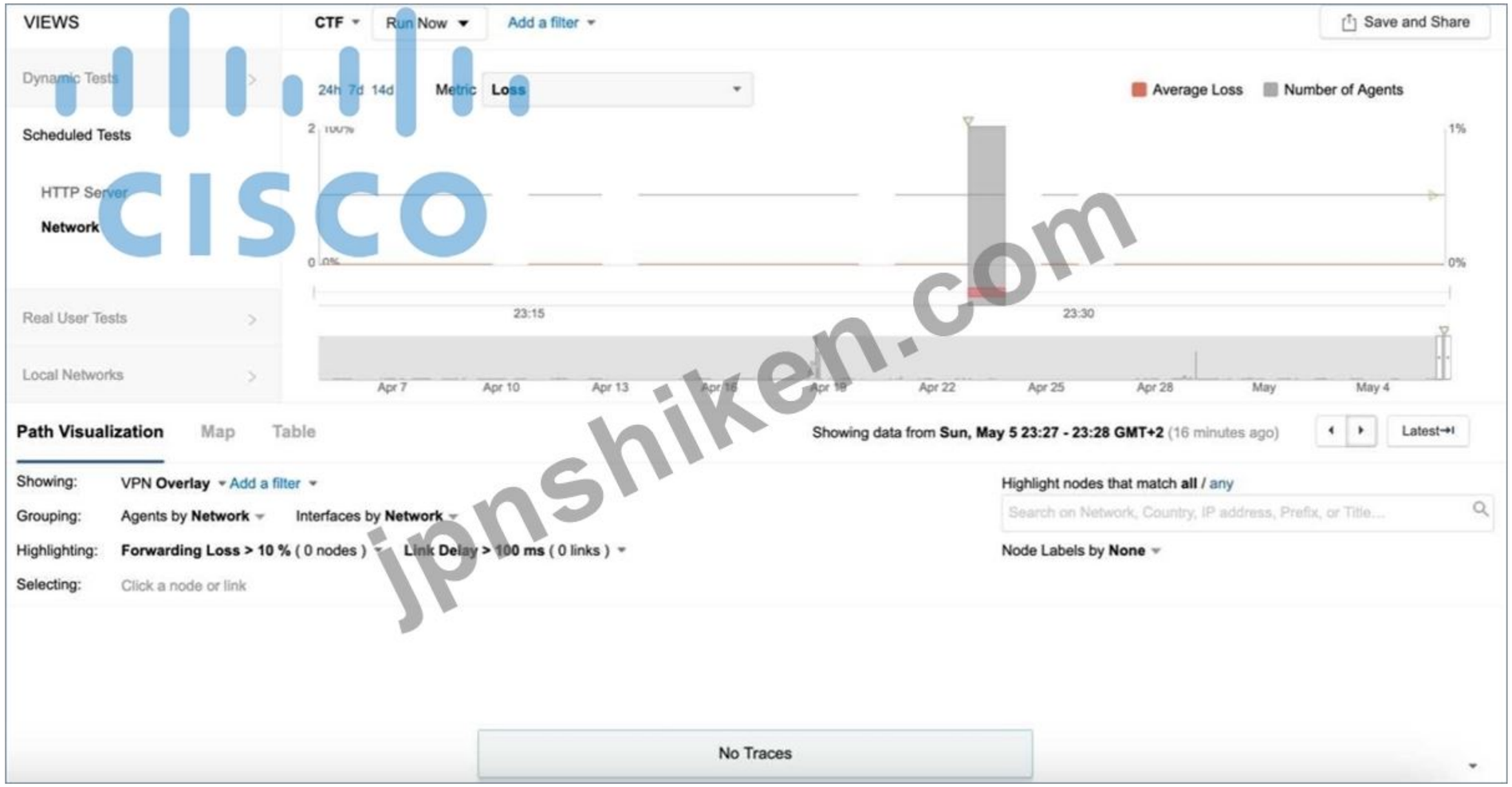
Selecting: Click a node or link

**3 hops** **0 hops**

Highlight nodes that match **all** / any

Search on Network, Country, IP address, Prefix, or Title...

Node Labels by **None** ▾






**A.** エンドポイントに割り当てられているDNSサーバーに到達できません。
**B.** テスト対象のFQDNが存在しません。
**C.** エンドポイントのDNS設定が間違っています。
**D.** テスト対象が応答しなくなりました。
正解: **A** (コメントを発表する)

質問: **7**
展示されているアラートは、次のうちどのネットワークセキュリティ上の問題を検出するように設計されていますか？
**A.** ルート中毒
**B.** DNSポイズニング
**C.** BGPハイジャック
**D.** DNSハイジャック
正解: **C** (コメントを発表する)

図4.1-1（image_6e19fb.png）に示すように、アラートルールは「AS origin AS 1234」という名前のBGPレイヤに対して設定されています。クリティカルロジックはアラート条件セクションで定義されており、BGP Originが「ASNが1234に含まれない」というすべての条件を満たしていることを示しています。
この特定の設定は、ThousandEyesでBGPハイジャックを検出するために用いられる標準的な方法です（オプションC）。BGPハイジャックとは、権限のない自律システム（AS）が、自身が所有していないネットワークプレフィックスをアナウンスし、正当な所有者宛てのトラフィックを盗み出す行為です。
ThousandEyesは、監視対象のプレフィックスが、想定される正規の自律システム番号（ASN）（この場合はAS 1234）とは異なるASNから発信されていることが確認された場合にアラートを発するように設定することで、ルーティングの乗っ取りを即座に通知します。
BGPオリジンアラートを介してこの問題を特定する方法は、ルーティング制御プレーンで問題を検出できるため、単純な接続チェックよりも優れています。

質問: **8**
リアルタイムストリーミングに関連して収集されたデータを使用して診断される一般的な問題は何ですか？
**A.** ネットワークの混雑
**B.** DNSサーバーの障害
**C.** パケット損失
**D.** CPU使用率の急上昇
正解: **(正解を表示します)**
パケット損失は、リアルタイムストリーミングに関連して収集されたデータを使用して診断される一般的な問題であり、ネットワーク保証における潜在的なネットワークパフォーマンスの低下を示すものです。

質問: **9**
エンドポイントを別のネットワークに移動した後、エンドポイントがオンライン表示されなくなりました。顧客はエンドポイントのログを確認しましたが、不審な点は見つかりませんでした。また、エンドポイントは以前のネットワークではオンラインであり、新しいネットワークも完全に動作していることを確認しました。新しいネットワークに移動した他のエンドポイントもオンラインです。新しいネットワークは小規模であるため、管理者は静的IPアドレス割り当てを使用しています。エンドポイントをオンラインにする最善の方法は何でしょうか？

```
2024-05-07 13:20:12.452 DEBUG [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:206 - RECONNECT is currently scheduled or running, ignoring schedule attempt for CONNECT
2024-05-07 13:20:14.468 DEBUG [3068.8116] agent.services.AgentSettingsService@DefaultAgentSettingsService.cpp:496 - Checkin failed with error code: 1
2024-05-07 13:20:14.468 DEBUG [3068.8116] agent.services.AgentSettingsService@DefaultAgentSettingsService.cpp:558 - Calling connect on persistent connection
2024-05-07 13:20:14.468 DEBUG [3068.8116] agent.services.AgentSettingsService@DefaultAgentSettingsService.cpp:576 - Will consider polling for scheduled tests in 30s
2024-05-07 13:20:14.468 DEBUG [3068.8116] agent.services.AgentSettingsService@DefaultAgentSettingsService.cpp:432 - Scheduling checkin in 10m
2024-05-07 13:20:14.468 DEBUG [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:198 - Running pre-schedule checks for CONNECT, isRetry=false, prev=CONNECT, current=RECONNECT, next=NONE
2024-05-07 13:20:14.468 DEBUG [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:206 - RECONNECT is currently scheduled or running, ignoring schedule attempt for CONNECT
2024-05-07 13:20:24.753 DEBUG [3068.8240] system.EtwTraceConsumer@DefaultEtwTraceConsumer.cpp:108 - Flushed ETW trace buffers to file. path="C:\ProgramData\ThousandEyes\Endpoint Agent\etwTraces\ThousandEyes Endpoint Agent.etl", size=320kB
2024-05-07 13:20:24.765 DEBUG [3068.8240] net.SocketMonitoring@WinSocketMonitoringService.cpp:335 - Processed ETW event batch: published=2, stale=213, deduped=0, duplicatesDueToCoalesceInterval=0, skipped=41
2024-05-07 13:20:24.812 DEBUG [3068.7712] scheduler.task.statscommitter@UsageStatsCommitter.cpp:43 - Starting UsageStatsCommitter task
2024-05-07 13:20:24.813 DEBUG [3068.7712] tests.scheduledtestsmetric@DefaultScheduledTestsMetricsService.cpp:54 - End metric tracking period at: 2024-May-07 13:20:24.812000
2024-05-07 13:20:24.813 DEBUG [3068.7712] scheduler.task.statscommitter@UsageStatsCommitter.cpp:95 - Updated usage stats object with 69 entries.
2024-05-07 13:20:25.109 DEBUG [3068.2148] scheduler.simple@DefaultTaskScheduler.cpp:173 - Scheduled task: te::agent::UsageStatsCommitter/0x1, delay=60000 ms
2024-05-07 13:20:28.498 DEBUG [3068.2148] net.WinHttpClient@WinHttpClient.cpp:2115 - Request to: wss://c1.eb.thousandeyes.com/relay/connect timed out: 12002: The operation timed out
2024-05-07 13:20:28.499 DEBUG [3068.8240] net.WinHttpClient@WinHttpClient.cpp:2115 - Request to: https://c1.eb.thousandeyes.com/status.json timed out: 12002: The operation timed out
2024-05-07 13:20:28.499 DEBUG [3068.4352] net.DefaultWebSocketStompConnection@DefaultWebSocketStompConnection.cpp:135 - Websocket connection wait: 42108ms
2024-05-07 13:20:28.499 ERROR [3068.4352] net.DefaultWebSocketStompConnection@DefaultWebSocketStompConnection.cpp:148 - asyncOpen (Websocket): Input/output error [generic:5]
2024-05-07 13:20:28.499 ERROR [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:317 - asyncOpen: Input/output error [generic:5]
2024-05-07 13:20:28.499 DEBUG [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:485 - Running post-run checks for RECONNECT, next=NONE, retry=true
2024-05-07 13:20:28.499 DEBUG [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:198 - Running pre-schedule checks for RECONNECT, isRetry=true, prev=RECONNECT, current=NONE, next=NONE
2024-05-07 13:20:28.499 DEBUG [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:300 - Set schedule delay=1500ms, jitter=323ms, nextDelay=2250ms
2024-05-07 13:20:28.499 INFO  [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:226 - Scheduling RECONNECT after 1823ms
2024-05-07 13:20:28.771 INFO  [3068.8072] agent.services.CheckinService@CheckinService.cpp:422 - Checking in with ThousandEyes backend. Last successful check-in: 2024-May-07 13:16:04.698000. Last attempt: 2024-May-07 13:18:24.548000
2024-05-07 13:20:28.771 DEBUG [3068.8072] api.usp@UserSpaceProxyClient.cpp:50 - Relaying HTTP request https://c1.eb.thousandeyes.com/eyebrow/enterprise/agent/checkin to user space proxy
2024-05-07 13:20:30.327 DEBUG [3068.4352] agent.DefaultPersistentConnection@DefaultPersistentConnection.cpp:244 - Running RECONNECT now
2024-05-07 13:20:30.327 DEBUG [3068.4352] net.DefaultWebSocketStompConnection@DefaultWebSocketStompConnection.cpp:308 - STOMP connection closed successfully
2024-05-07 13:20:30.327 DEBUG [3068.4352] net.DefaultWebSocketStompConnection@DefaultWebSocketStompConnection.cpp:327 - Websocket connection closed successfully
```

**A.** 新しいネットワークの容量不足が原因かもしれません。エンドポイントを古いネットワークに戻してください。
**B.** エンドポイントエージェントを再インストールしてオンラインにする必要があります。これは常に効果があります。
**C.** エンドポイントは10〜15分後に自動的にオンラインになります。操作は不要です。
**D.** エンドポイントのIP設定とc1.eb.thousandeyes.comへの接続を確認する必要があります。

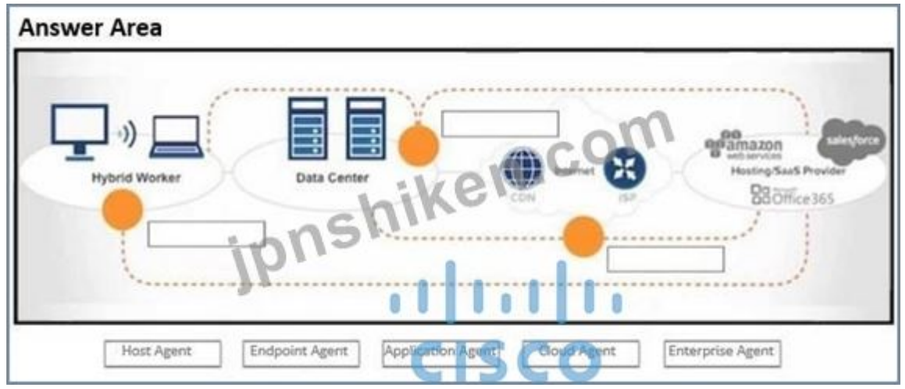
正解: (正解を表示します)
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）カリキュラムでは、エンドポイント接続のトラブルシューティングには、ローカルデバイスのログとネットワーク環境の変化を体系的に分析する必要があります。添付資料に示されているログメッセージによると、エージェントがThousandEyesバックエンドにアクセスしようとした際に、特定のタイムアウトエラーが発生しました。ログには、以下の内容が明記されています。
リクエスト先: wss://c1.eb.thousandeyes.com/relay/connect がタイムアウトしました: 12002: 操作がタイムアウトしました。
エンドポイントが静的IPアドレス割り当てを使用する新しいネットワークに移動され、同じネットワーク上の他のエンドポイントは正常に動作していることから、問題はこの特定のデバイスの設定に起因していると考えられます。静的IP環境では、IPアドレス、サブネットマスク、デフォルトゲートウェイ、またはDNSサーバーの手動入力時の人為的ミスが、接続障害の一般的な根本原因となります。ゲートウェイが間違っている場合、エージェントはインターネットにアクセスできません。DNSが間違っている場合、c1.eb.thousandeyes.comを解決できません。したがって、エンドポイントをオンラインにする最善の方法は、IP設定の正確性を確認し、ThousandEyesリレーURLへの直接接続をテストすることです。

質問: **10**
ウェブアプリケーションにおけるユーザー操作をシミュレートするのに最適なエージェントタイプはどれですか？
**A.** エンドポイントエージェント
**B.** 合成ユーザーエージェント
**C.** 現地集金代行業者
**D.** スクリプトエージェント
正解: (正解を表示します)
合成ユーザーエージェントは、Webアプリケーションとのユーザーインタラクションをシミュレートするように特別に設計されているため、このタスクに最も適した選択肢となります。

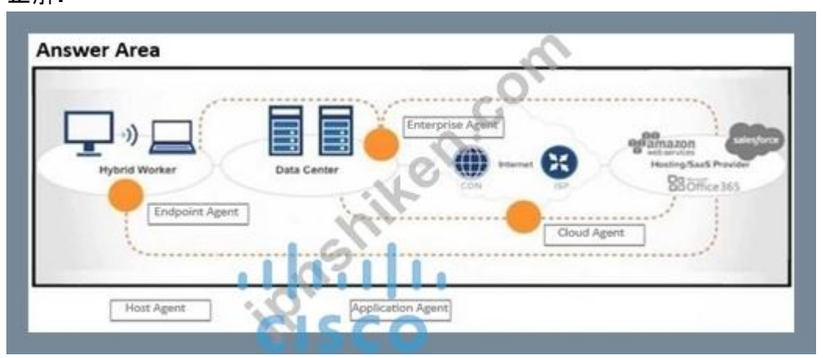
質問: **11**
ネットワークエンジニアが、アプリホスティングを使用してスイッチ上にThousandEyes Dockerエージェントをデプロイします。エージェントはプロキシサーバー経由で通信する必要がありますが、初期デプロイ時にこの設定が漏れていました。エンジニアは、アプリホスティングの設定にプロキシ設定を追加します。エージェントがプロキシを使用し、ThousandEyesポータルでオンラインとして表示されるようにするには、次にどのような手順を踏めばよいでしょうか？
**A.** app-hosting stop appid agentname を実行してから app-hosting start appid agentname を実行してコンテナを再起動します。
**B.** 正しいプロキシ設定を使用して、app-hosting install コマンドでエージェントを再インストールします。
**C.** エージェントのライフサイクル全体を実行します: app-hosting stop appid agentname、app-hosting deactivate appid agentname、app-hosting activate appid agentname、app-hosting start appid agentname
**D.** 操作は不要です。エージェントが自動的に設定を取得します。
正解: (正解を表示します)
『エンタープライズネットワーク保証の設計と実装（300-445 ENNA）』実装ガイドでは、Cisco IOS XEアプリケーションホスティングのライフサイクルは、トラブルシューティングと構成管理において重要な概念として説明されています。アプリケーションホスティング構成でプロキシ設定などのアプリケーション環境変数が変更された場合、コンテナを単に再起動するだけでは不十分です。
正しい手順は、アプリケーションを「構成済み」状態に戻し、その後「実行中」状態に戻すことです。これには、4段階のライフサイクル実行が必要です（オプションC）。
Stop: 現在実行中のコンテナインスタンスを終了します。
非アクティブ化：ハードウェアリソース（CPU、メモリ、仮想インターフェース）を解放し、重要な点として、以前のランタイム構成を切り離します。
アクティベート：リソースを再割り当てし、新しい構成パラメータ（更新されたプロキシ設定を含む）をコンテナの環境に注入します。
開始: 新しく適用された設定でコンテナを起動します。

質問: **12**
ドラッグアンドドロップ問題

ある組織では、特定のクラウドベースアプリケーションへの接続が断続的に発生する問題が発生しています。図の下部にあるエージェントをドラッグアンドドロップして、接続問題の根本原因を特定してください。すべてのオプションを使用する必要はありません。




正解:




Explanation:

エンドポイントエージェントは、ハイブリッドワーカーのデバイスとラストマイルの状況を可視化します。

Enterprise Agentは、組織のデータセンター内部からクラウドに向けて監視を行います。

Cloud Agentは、パブリックインターネットからSaaSアプリケーションへの外部からの可視性を提供します。

質問: **13**

あなたは、基本認証を使用するWebアプリケーションを対象としたThousandEyesトランザクションテストで断続的に発生する障害を調査しています。この障害は、異なるエージェントや時間帯でランダムに発生します。この問題を解決するために、どのような手順を踏みますか？（該当するものをすべて選択してください）

**A.** 問題を切り分けるために、テスト構成で基本認証を無効にします。

**B.** 異なる場所からアプリケーションに手動でログインして、認証情報の正当性を確認します。

**C.** ThousandEyesのウォーターフォールチャートとHTTPレスポンスコードを分析し、潜在的なボトルネックやエラーを特定します。

**D.** Webアプリケーションベンダーに連絡して問題を報告し、サーバー側の問題の可能性について問い合わせてください。

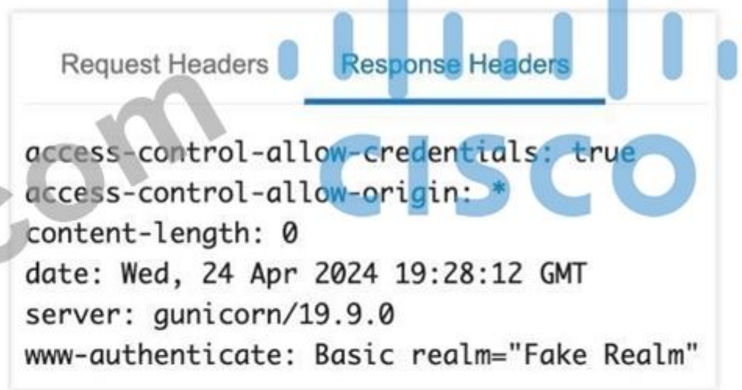
正解: **(**正解を表示します**)**

断続的なパフォーマンス問題のトラブルシューティングは、「エンタープライズネットワーク保証の設計と実装（300-445 ENNA）」カリキュラムの中核をなす要素です。基本認証を使用したトランザクションテストがランダムに失敗した場合、エンジニアは多層的な診断アプローチを用いて、障害の原因が認証情報、ネットワークパス、またはアプリケーションサーバーのいずれにあるかを判断する必要があります。

最初のステップは、認証情報の正確性を確認することです（オプションB）。基本認証では認証情報がヘッダーにエンコードされるため、ユーザー権限の変更やアカウントのロックアウトが発生すると、即座に認証エラーが発生します。さまざまな地域から手動でログインすることで、場所に基づくアクセス制御リスト（ACL）や地域ごとのIdP同期の問題を排除できます。

最もデータ量の多い診断手順は、ThousandEyesのウォーターフォールチャートとHTTPレスポンスコードを分析することです（オプションC）。ウォーターフォールビューを使用すると、エンジニアは障害が最初の401 Unauthorizedチャレンジ中に発生したのか、認証情報が送信された後に発生したのかを確認できます。チャートに「待機時間」が高い、または5xxエラーが表示されている場合は、サーバー側の遅延または不安定性が問題の原因である可能性が高いです。「接続時間」が高い場合は、ネットワーク層の輻輳が問題の原因である可能性があります。
最後に、テレメトリでネットワークパスが正常であることが示されているにもかかわらず、サーバーが断続的にエラーを返したりタイムアウトしたりする場合は、エンジニアはWebアプリケーションベンダーに連絡する必要があります（オプションD）。
ベンダーにThousandEyesの特定の「共有リンク」を提供することで、ベンダーは全く同じパケットレベルおよびブラウザレベルのデータを確認でき、問題がクライアントのネットワークではなくサーバー側のインフラストラクチャにあることを証明できます。認証を無効にする（オプションA）ことは、認証されたワークフローを監視するために特別に設計されたテストの有効なトラブルシューティング手順ではありません。

質問: **14**
証拠資料を検討してください。証拠に基づき、どの対策が問題解決に最も効果的であると考えられますか？




**A.** ターゲットURLを利用可能なAPIエンドポイントに変更します
**B.** HTTPリクエストメソッドをPATCHに変更します
**C.** ファイアウォールルールを変更して、対象ドメインへの接続を許可する。
**D.** 認証情報を変更する
正解: **D** (コメントを発表する)

質問: **15**
最適なデータ収集のためにネットワークエージェントの設置場所を決定する際に、重要な考慮事項は何ですか？
**A.** 自然光へのアクセス
**B.** ネットワークエンドポイントへの近接性
**C.** 会議室の空き状況
**D.** 従業員のワークステーションからの距離
正解: (正解を表示します)
ネットワークエージェントをネットワークエンドポイントの近くに配置することで、最適なデータ収集と分析が保証されます。

質問: **16**
ネットワーク管理者がオフィスサイト内にTLS復号プロキシを導入しました。TLSネゴシエーションのパフォーマンスを示す指標はどれですか？
**A.** ネットワーク遅延
**B.** スループット
**C.** 応答時間

**D.** サーバーの可用性
正解: **(**正解を表示します**)**
TLSネゴシエーションはアプリケーション層の接続設定の一部であり、ThousandEyesはHTTP/HTTPSテストの応答時間メトリックにTLS/SSLハンドシェイクの所要時間を含めています。

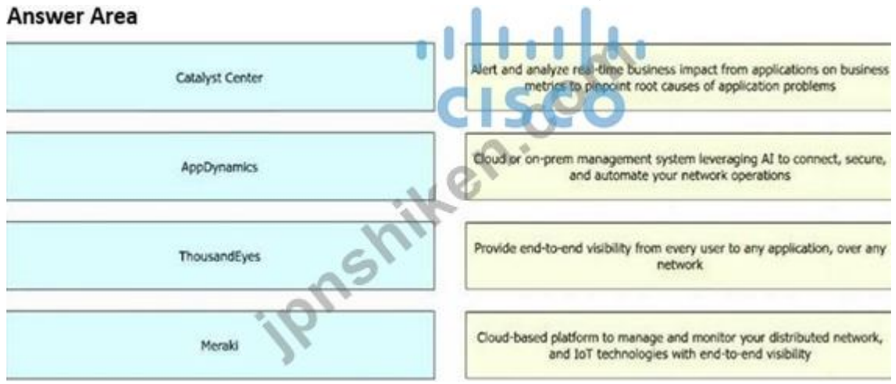


質問: **17**
ネットワーク保証の目的で、Thousand Eyesを使用してどのようなテストを設定できますか？
**A.** インフラテスト
**B.** 音声テスト
**C.** セキュリティテスト
**D.** アプリケーションテスト
**E.** ネットワークテスト
**F.** Webテスト
正解: **B,E,F (**コメントを発表する**)**
Thousand Eyesは、ネットワークテスト、音声テスト、Webテストなど、さまざまなテストに合わせて構成でき、異なるドメインにわたる包括的なネットワーク保証とパフォーマンス監視を可能にします。

質問: **18**
ネットワークエンジニアが、データセンターでホストされているWebアプリケーションのパフォーマンス低下に関する多数の報告を調査しています。根本原因を迅速に特定するには、どのThousandEyesエージェントタイプが最も効果的でしょうか？
**A.** 合成剤
**B.** エンタープライズエージェント
**C.** エンドポイントエージェント
**D.** クラウドエージェント
正解: **(**正解を表示します**)**
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）ガイドラインによると、パブリックまたはデータセンターでホストされているアプリケーションの広範囲にわたるパフォーマンスの問題のトラブルシューティングには、
「外側から内側へ」の視点。報告が広範囲に及ぶ場合、18目標は、問題がグローバルなものか、地域的なものか、データセンターにつながる特定のISPパスに特有のものかを判断することです。
クラウド エージェント (オプション D) は、このタスクに最も効果的なツールです。なぜなら、これらのエージェントは、ティア 1、2、3 の ISP およびクラウド プロバイダーのリージョン内の世界 240 か所以上の拠点で Cisco ThousandEyes によって維持されているからです。19 事前に展開され、すぐに利用できるため、ネットワーク エンジニアは、ソフトウェアをインストールしたりインフラストラクチャを管理したりすることなく、複数のグローバルな場所からデータ センターでホストされているアプリケーションに対してテストを即座に実行できます。これにより、エンジニアは、さまざまな地域間でパフォーマンス メトリック (遅延、損失、ページ読み込み時間) を迅速に比較できます。ロンドンのクラウド エージェントが問題がないと報告している一方で、ニューヨークのエージェントが高いパケット損失を報告している場合、エンジニアは、データ センター自体の障害ではなく、地域の ISP またはピアリングの問題として根本原因をすぐに特定できます。
* エンタープライズエージェント（オプションB）：既存の支店にインストールされている場合は使用可能ですが、インフラストラクチャの所有権と導入時間が必要となります。「内部監視」に適しています。
* エンドポイントエージェント（オプション C）これらは個々のユーザーエクスペリエンスのトラブルシューティングに役立ちますが、広範囲にわたるイベント中にデータセンターアプリケーションに対するグローバルパフォーマンスのベースラインを設定する「最速」の方法ではありません。
* 合成エージェント（オプションA）：前述のとおり、これはすべてのThousandEyesエージェントタイプで使用される基盤技術を説明する一般的な用語です。

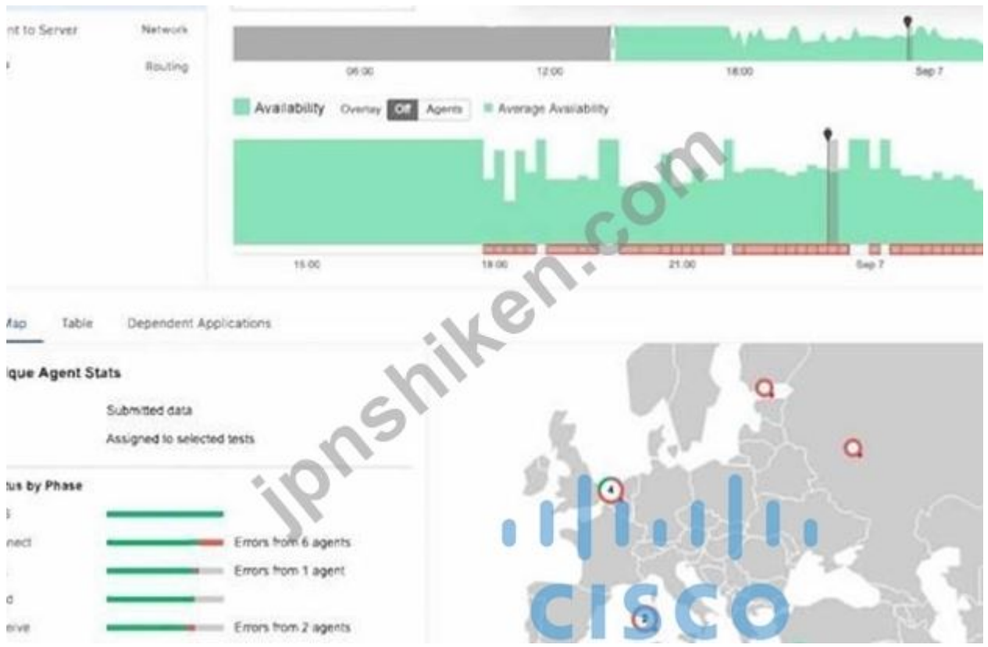
したがって、クラウドエージェントは、広範囲にわたるアプリケーションのパフォーマンス問題に対する迅速な根本原因分析を実行するために必要な、幅広い機能と即時性を提供します。

質問: **19**
ドラッグアンドドロップ問題
左側のCisco Network Assuranceプラットフォームを、右側の対応するビジネスケースにドラッグアンドドロップしてください。
**Answer Area**




正解:
**Answer Area**


質問: **20**
図を参照してください。ウェブサイトの可用性低下を引き起こしているセキュリティインシデントはどれですか？




**A.** 中間者攻撃
**B.** 無効なSSL証明書
**C.** DNSハイジャック
**D.** DDoS攻撃
正解: **D** (コメントを発表する)
ThousandEyesのビューによると、複数のグローバルエージェントで広範囲かつ同時に可用性が低下しており、DNS、接続、SSL、受信といった複数のフェーズに影響が出ていることが示されています。
このパターン（複数の地域にまたがり、複数の接続フェーズに影響を与える）は、DDoS攻撃の特徴であり、サービスを過負荷状態に陥らせ、エージェントがリクエストを完了できないようにする。

質問: **21**
図を参照してください。エンジニアは、銀行のプライベートデータセンターでホストされているオンラインバンキングアプリケーションの顧客体験を監視する必要があります。エンジニアはどのThousandEyesエージェントをデプロイする必要がありますか？

**A.** アプリケーションエージェント
**B.** エンタープライズエージェント
**C.** クラウドエージェント
**D.** エンドポイントエージェント
正解: (正解を表示します)
オンラインバンキングアプリケーションの顧客体験を監視するには、外部のインターネットユーザーが銀行のプライベートデータセンターにアクセスする状況をシミュレートするテストを実施する必要があります。
Cisco ThousandEyesクラウドエージェントはインターネット上でグローバルに稼働し、真の顧客体験を測定するために必要な、適切な外部からの可視性を提供します。

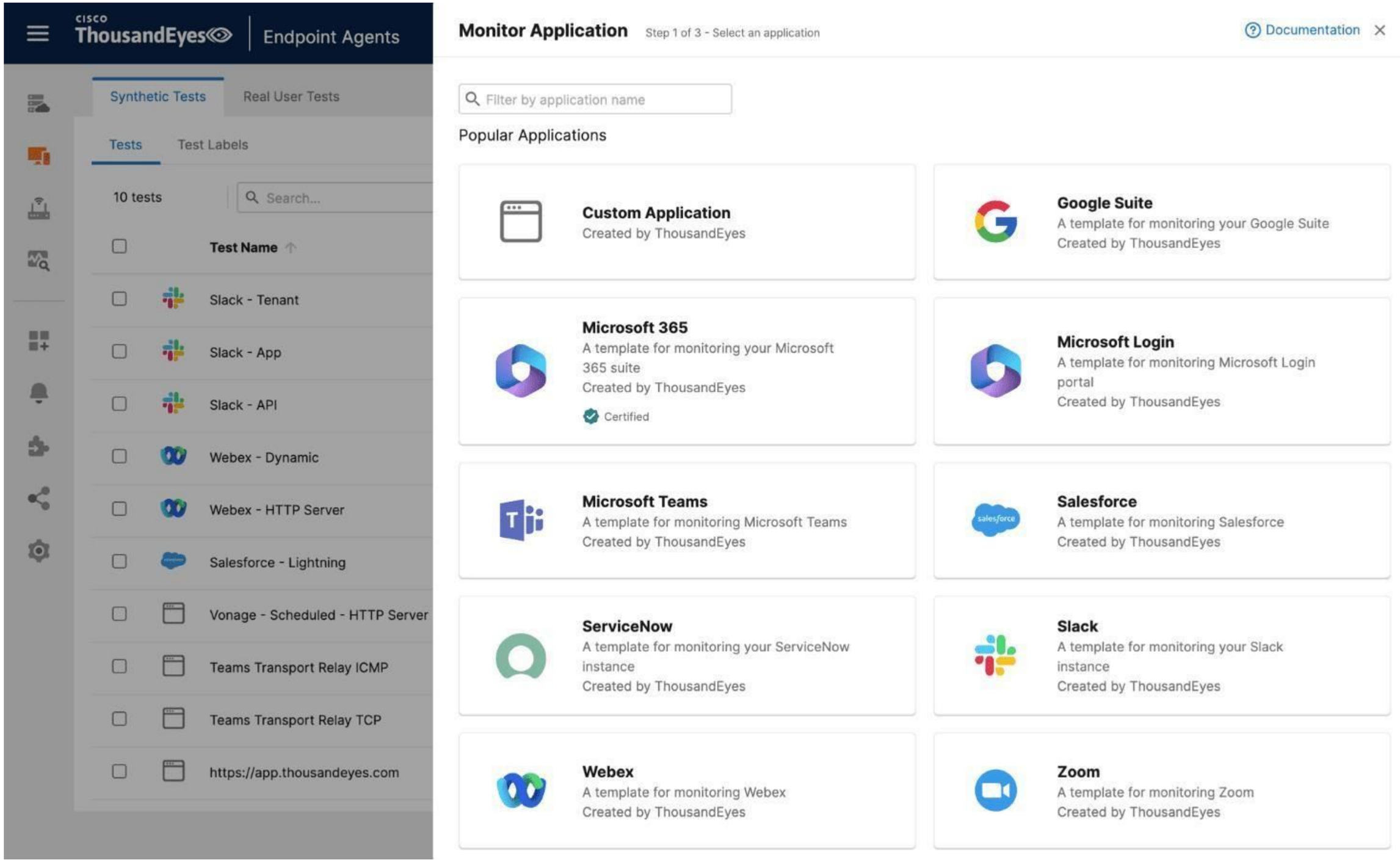
質問: **22**
アーキテクトは、内部ネットワーク、特にアクセス層からクラウドホスト型Webサーバーまでのネットワークパスメトリックを分析する必要があります。1 このタスクに最も適したThousandEyesエージェントはどれですか？
**A.** 合成剤
**B.** エンタープライズエージェント
**C.** クラウドエージェント
**D.** エンドポイントエージェント
正解: (正解を表示します)
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）の枠組みでは、適切なエージェントタイプの選択は、特定の観測に必要な視点に大きく依存します。このシナリオでは、アーキテクトは、企業境界内のユーザーまたはデバイスに最も近いポイントである内部ネットワークアクセス層から、クラウドホスト型の宛先に向けてメトリックを収集する必要があります。
エンタープライズエージェント（オプションB）は、組織が所有および管理するインフラストラクチャに展開するように特別に設計されているため、最も適切な選択肢です。これらのエージェントは、Dockerコンテナを使用してアクセスレイヤーのCisco Catalyst 9300または9400シリーズスイッチに直接インストールできる「インサイドアウト」型の監視ポイントです。アクセスレイヤーにエンタープライズエージェントを展開することで、アーキテクトは内部LANから始まり、エッジ/WANを経由してクラウドホスト型Webサーバーに至るネットワークパス全体を可視化できます。これにより、ローカルの輻輳、ISPピアリングの問題、クラウドプロバイダーの遅延などの問題を特定できます。
その他の選択肢は基準を満たしていません。
* 合成エージェント（オプションA）これは紛らわしい用語です。ThousandEyesのエージェント（クラウド、エンタープライズ、エンドポイント）はすべて、アクティブな合成テストを実行するため、合成エージェントです。
* クラウドエージェント（オプションC）これらはシスコによってグローバルISPデータセンターに事前に展開され、「外部からの視点」14は、外部に公開されている可用性を監視するのに役立ちますが、組織の内部ネットワークやアクセスレイヤーを可視化することはできません。
* エンドポイントエージェント（オプション D）これらはエンドユーザーのマシンにインストールされ、「ユーザー中心」のビューを提供しますが、一般的にはアクセスレイヤースイッチ自体からのインフラストラクチャレベルのパス分析には使用されません。
したがって、エンタープライズエージェントは、アクセス層からクラウドまでの監視において、決定的な選択肢となります。

質問: **23**
どのようなシナリオにおいて、Macデバイスにエンドポイントエージェントをデプロイすることが最も有益でしょうか？
**A.** リアルタイムストリーミングの問題分析
**B.** WANパフォーマンスの監視
**C.** DNSサーバーのパフォーマンス評価
**D.** ウェブ認証テストの実施
正解: (正解を表示します)
Macデバイスにエンドポイントエージェントを導入することは、Web認証テストの実施や、ネットワーク保証におけるWebアプリケーションへの安全なアクセス確保に最も効果的です。

質問: **24**
ネットワーク保証におけるパッシブモニタリングのフレームワークを定義しているRFCはどれですか？
**A.** RFC 791
**B.** RFC 7276
**C.** RFC 7799
**D.** RFC 7880
正解: **C** (コメントを発表する)
RFC 7799は、パッシブモニタリングのフレームワークを定義し、ネットワークアシュアランスにおいてネットワークパフォーマンスに影響を与えることなくネットワークトラフィックをキャプチャおよび分析するためのガイドラインを提供します。

質問: **25**
ネットワーク容量計画の最適化を推奨する際、データ分析に基づいて通常どのような要素が考慮されますか？
**A.** アプリケーションのパフォーマンス
**B.** トポロジーと構成の変更
**C.** サーバーハードウェアのアップグレード
**D.** セキュリティ上の脆弱性
正解: **B** (コメントを発表する)
ネットワーク容量計画の最適化を推奨する際には、通常、データ解析に基づいてトポロジーや構成変更などの要素が考慮されます。これには、ネットワークアーキテクチャの最適化、ルーティングプロトコルの調整、およびトラフィックパターンやビジネス要件の変化に対応してパフォーマンス、信頼性、拡張性を向上させるための追加ネットワークリソースの展開が含まれます。

質問: **26**
展示資料を参照してください。




エンジニアは、従業員の視点からWebアプリケーションを監視する新しいテストを設定するよう指示されました。この要件を満たすために、どのような2つのアクションを実行すべきでしょうか？

**A.** 新しいカスタムアプリケーションモニターを作成します

**B.** 新しいGoogle Suiteモニターを作成する

**C.** モニターに新しいスケジュール済みテストを追加する
**D.** モニターに新しい動的テストを追加
**E.** 新しいテストテンプレートを追加する
正解: **(**正解を表示します**)**
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）カリキュラムでは、社内従業員のデジタルエクスペリエンスを監視するために、ThousandEyesエンドポイントエージェントを活用して、ユーザー固有の視点からのトラフィックをシミュレートまたは記録する必要があります。エンジニアが特定の、場合によっては社内向けまたは非標準のWebアプリケーションを監視する必要がある場合は、エンドポイントエクスペリエンス設定内のカスタムアプリケーションワークフローを使用する必要があります。
ENNA実装標準によれば、最初に必要なアクションは、新しいカスタムアプリケーションモニターを作成することです（オプションA）。ThousandEyesポータルのEndpoint Experience > Test Settings > Synthetic Testsにある「アプリケーションの監視」ボタンをクリックすると、Microsoft 365やWebexなどの一般的なサービス用の事前定義済みテンプレートにアクセスできます。ただし、独自のエンタープライズアプリケーションの場合は、エンジニアは、
「カスタムアプリケーション」では、アプリケーションの名前や関連するドメインまたはURLなど、アプリケーションの識別情報を定義します。
2番目に必要な操作は、モニターに新しいスケジュール済みテストを追加することです（オプションC）。エンドポイントエージェントは、5分ごとや10分ごとなど、事前に定義された定期的な間隔でスケジュール済みテストを実行し、ユーザーの操作を必要とせずに、アプリケーションの可用性、応答時間、ネットワークパスの状態をプロアクティブにチェックします。
カスタムモニターにスケジュールされたHTTPサーバーまたはネットワークテストを追加することで、エンジニアは従業員のマシンから見たアプリケーションのパフォーマンスの一貫したベースラインを確保できます。
誤った選択肢を確認する：
* Google Suite モニター (オプション B): これは Google Workspace 専用のテンプレートであり、カスタム アプリケーションには適していません。
* 動的テスト（オプション D）これらは、Zoom や Microsoft Teams などのコラボレーション ツールでアドホック セッションをキャプチャするために特別に設計されています。これらは通常、標準的なカスタム Web アプリケーションのベースライン設定には使用されません。
* テストテンプレート（オプション E）すべてのモニターはテンプレートに基づいていますが、「新しいテンプレートの追加」は構成操作ではなく、監視設定の結果です。

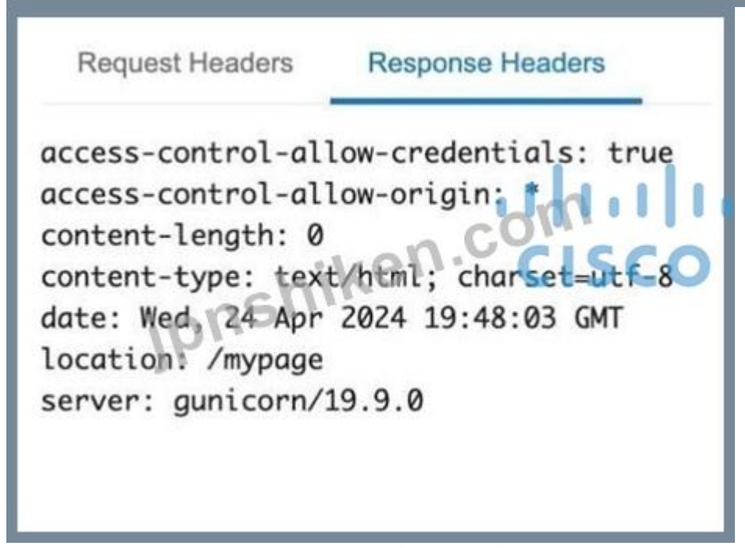
質問: **27**
RFC 7276によると、リアルタイム環境におけるコンプライアンス監査には、どちらの監視手法がより一般的に使用されるでしょうか？
**A.** どちらでもない。RFC 7276ではコンプライアンス監査について議論されていないため。
**B.** アクティブモニタリング
**C.** アクティブ監視とパッシブ監視の両方
**D.** 受動監視
正解: **(**正解を表示します**)**

質問: **28**
証拠資料を検討してください。これらの証拠に基づくと、根本的な問題は何だと考えられますか？


Search by URL or Domain...

Component Type

| Component | Response Code | Domain | Provider | Size (kB) | Duration (ms) | Waterfall |
|---|---|---|---|---|---|---|
| 100 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 433 | |
| 99 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 199 | |
| 98 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 130 | |
| 97 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 219 | |
| 96 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 129 | |
| 95 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 127 | |
| 94 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 273 | |
| 93 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 245 | |
| 92 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 137 | |
| 91 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 288 | |
| 90 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 131 | |
| 89 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 511 | |
| 88 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 129 | |
| 87 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 128 | |
| 86 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 131 | |
| 85 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 127 | |
| 84 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 182 | |
| 83 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 875 | |
| 82 | 302 [ Headers ] | httpbin.org | Amazon.com, I... | 0 | 179 | |
| 81 | No Response [ Headers ] | httpbin.org | Amazon.com, I... | ⚠ | 0 | |


**A.** アプリケーションサーバーの設定ミスがあります
**B.** サーバーからの応答待ちでリクエストがタイムアウトしました
**C.** ネットワーク接続の問題により、目的のURLにアクセスできません。
**D.** サーバー上でDOM要素が見つかりません
正解: **(**正解を表示します**)**

質問: **29**
BGPルーティングを監視するためのアラートルールを設定する際、どのようなイベントが発生するとアラート通知がトリガーされますか？

**A.** CPU使用率が高い
**B.** 低メモリ条件
**C.** 路線広告の変更
**D.** DNSサーバーの障害
正解: (正解を表示します)
BGPルーティングを監視するためのアラートルールを設定する際に、ルートアドバタイズメントの変更によってアラート通知がトリガーされ、ネットワークルーティングパスの潜在的な変更が示されます。

質問: **30**
ネットワーク要素を継続的に調査し、その可用性と応答性を評価する監視方法はどれですか？
**A.** アクティブモニタリング
**B.** 受動監視
**C.** 合成モニタリング
**D.** 動的モニタリング
正解: (正解を表示します)
アクティブモニタリングとは、ネットワーク要素を継続的に監視し、その可用性と応答性をリアルタイムで評価することです。

質問: **31**
TCPプロトコルの動作を監視するために一般的に使用されるアラートルール設定はどれですか？
**A.** CPU使用率が高い
**B.** 有効期限切れのSSL証明書
**C.** 接続タイムアウト
**D.** ディスク容量不足
正解: (正解を表示します)
接続タイムアウトは、TCPプロトコルの動作を監視し、接続障害や遅延などの潜在的なネットワーク問題を検出するために、アラートルールの設定で一般的に使用されます。



質問: **32**
要求されたデータの統合タイプを選択する際、 API」は何の略ですか？
**A.** 分析パフォーマンス指標
**B.** 高度なプロトコル統合
**C.** アプリケーションプログラミングインターフェース
**D.** 自動パフォーマンス指標
正解: (正解を表示します)
API」とはアプリケーションプログラミングインターフェースの略で、異なるソフトウェアアプリケーション間でのデータや機能の交換を容易にし、シームレスな統合と相互運用性を実現します。

質問: **33**

過剰なトラフィックによってネットワークリソースが過負荷状態になり、ネットワークパフォーマンスに影響を与える可能性のあるセキュリティ上の問題はどれですか？
**A.** VLANの設定ミス
**B.** DNS解決エラー
**C.** BGPルーティングの問題
**D.** DDoS攻撃
正解: **D** (コメントを発表する)
DDoS攻撃は、過剰なトラフィックでネットワークリソースを圧倒することでネットワークパフォーマンスに影響を与え、サービスの中断や速度低下を引き起こす可能性があります。

質問: **34**
Thousand Eyesでアプリケーションのパフォーマンスを監視するために設定できるエンドポイントエージェントテストはどれですか？
**A.** ネットワークテスト
**B.** DNSテスト
**C.** ウェブテスト
**D.** 音声テスト
正解: (正解を表示します)
ネットワークテストは、Thousand Eyesで設定することで、アプリケーションのパフォーマンスを監視し、ネットワーク保証における遅延やパケット損失などの要素を評価できます。

質問: **35**
遠隔地のユーザーから音声に関する問題が報告されています。以下の資料から、考えられる原因と今後の対応策を特定できますか？

Current Test: Branch Voice | Settings | Agent: All agents | Run Now | Save | Share | ...

**Views**

VOICE

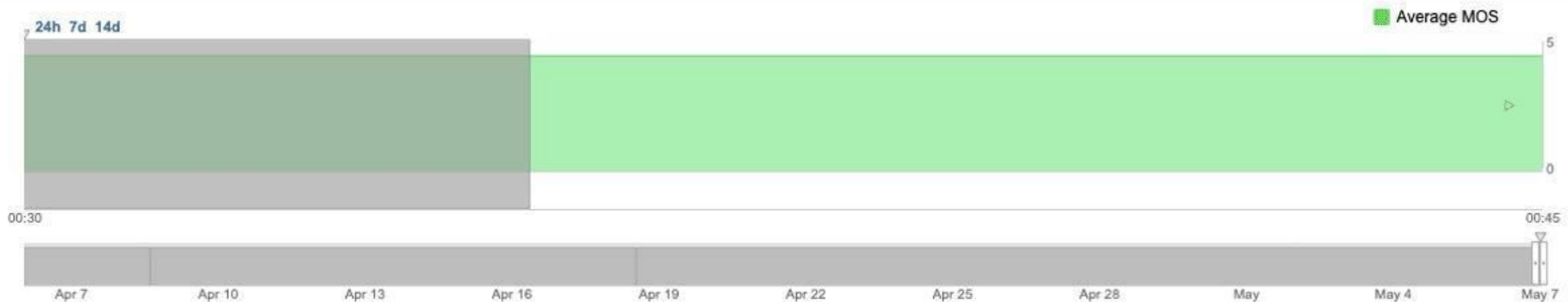
**RTP Stream**

NETWORK

Path Visualization

**Target Agent**
dc50-te-docker-ea53

Metric: **MOS**




Showing data from **Tue, May 7 00:30 - 00:35 EDT** (51 minutes ago)

Latest

Map **Table**

| Agent | Date (EDT) | Target IP | MOS | Packet Loss (%) | Discards (%) | Latency (ms) | PDV (ms) | Received DSCP |
|---|---|---|---|---|---|---|---|---|
| s30-te-olnx32 | 2024-05-07 00:30:05 | 172.17.0.2 | 4.39 | 0 | 0 | 24 | 1 | EF (DSCP 46) |
| s30-te-rhel33 | 2024-05-07 00:30:05 | 172.17.0.2 | 4.39 | 0 | 0 | 24 | 1 | EF (DSCP 46) |
| s20-te-rhel23 | 2024-05-07 00:30:05 | 172.17.0.2 | 4.4 | 0 | 0 | 15 | 1 | EF (DSCP 46) |
| dc60-te-va64 | 2024-05-07 00:30:05 | 172.17.0.2 | 4.4 | 0 | 0 | 12 | 1 | EF (DSCP 46) |

## Branch Voice

Tue, May 7, 2024 14:41 GMT+10 – 15:13 GMT+10

Shared by ThousandEyes Internal - ENNA-samplesv1

Agent

s20-te-rhel23

**Views**

VOICE

RTP Stream

NETWORK

**Path Visualization**

Metric

MOS

24h 7d 14d

Average MOS s20-te-rhel23

5

0

14:45

15:00

14:45

15:00

**Target Agent**

dc50-te-docker-ea53

Showing data from **Tue, May 7 14:50 - 14:55 GMT+10** (38 minutes ago)

Latest

### Path Visualization

7 hops 0 hops

Showing: **1 of 1 Test** **1 of 4 Agents** (Show All)**0 of 0 Servers** Show IP Address labels

Grouping: Agents by **Agent** Interfaces by **IP Address**

Highlighting: **Forwarding Loss > 10 %** ( 0 nodes ) **Link Delay > 100 ms** ( 0 links )

Selecting: Click a node or link **Info** (2)

Highlight nodes that match **all** / any

Search on Network, Country, IP address, Prefix, or Title...

Current Test: Branch Voice | Settings | Agent: s20-te-rhel23 | Run Now | Save | Share | ...

**Views**

VOICE

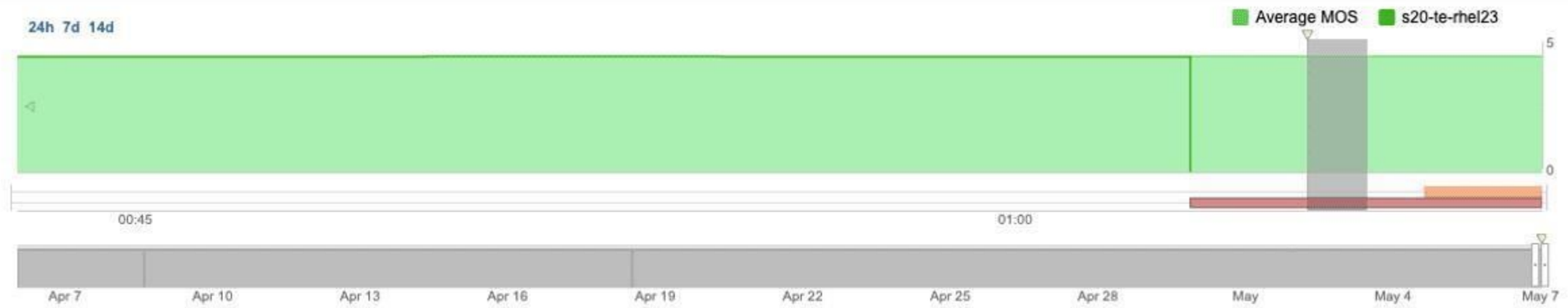
**RTP Stream**

NETWORK

Path Visualization

**Target Agent**
dc50-te-docker-ea53

Metric: **MOS**

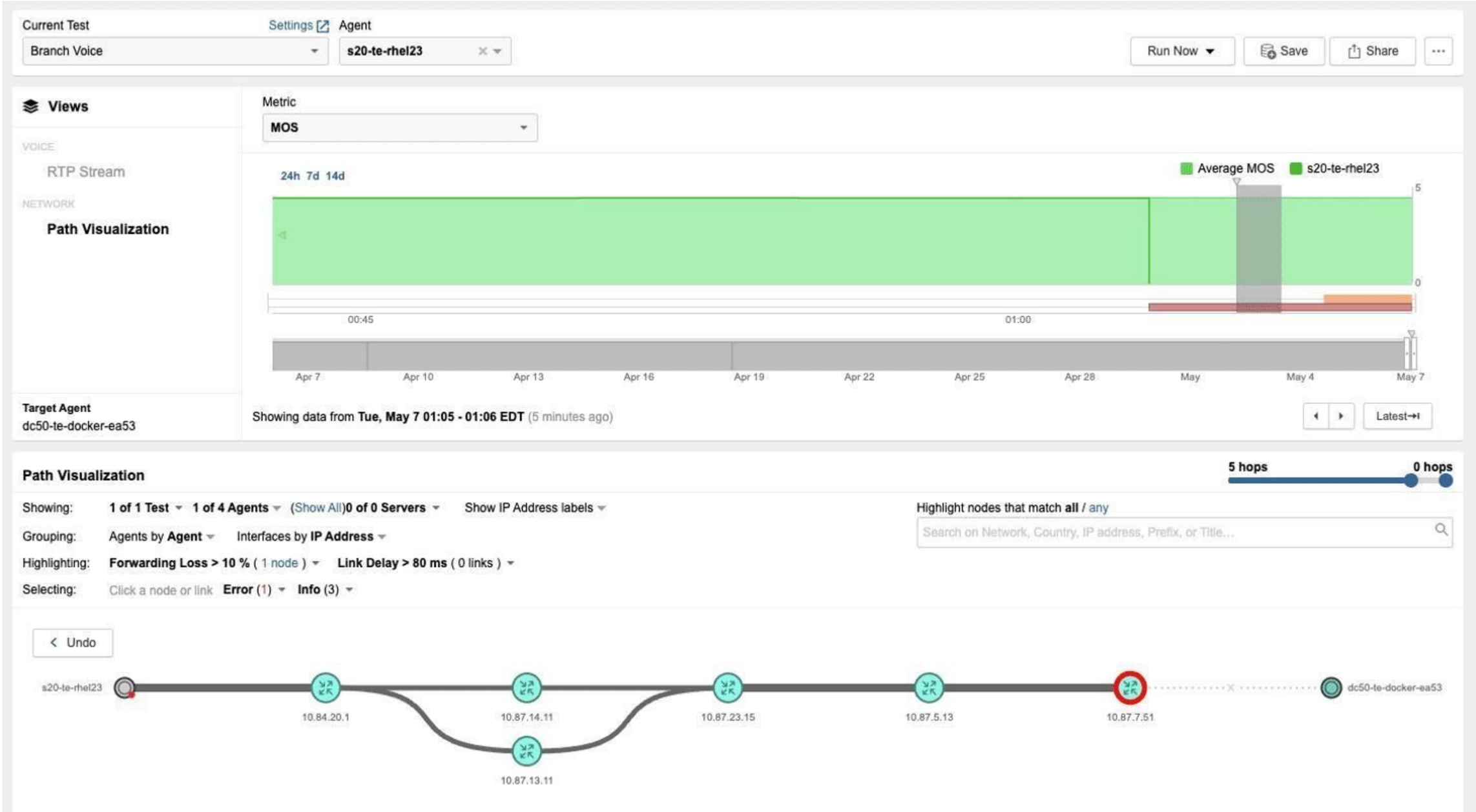



Showing data from **Tue, May 7 01:05 - 01:06 EDT** (4 minutes ago)

Latest

Map **Table**

| Agent | Date (EDT) | Target IP | MOS | Packet Loss (%) | Discards (%) | Latency (ms) | PDV (ms) | Received DSCP |
|---|---|---|---|---|---|---|---|---|
| s30-te-rhel33 | 2024-05-07 01:05:05 | 172.17.0.2 | 4.39 | 0 | 0 | 24 | 1 | EF (DSCP 46) |
| s30-te-olnx32 | 2024-05-07 01:05:05 | 172.17.0.2 | 4.39 | 0 | 0 | 24 | 2 | EF (DSCP 46) |
| dc60-te-va64 | 2024-05-07 01:05:05 | 172.17.0.2 | 4.4 | 0 | 0 | 7 | 1 | EF (DSCP 46) |
| s20-te-rhel23 | 2024-05-07 01:05:06 | 10.84.50.53 | — | — | — | — | — | — |



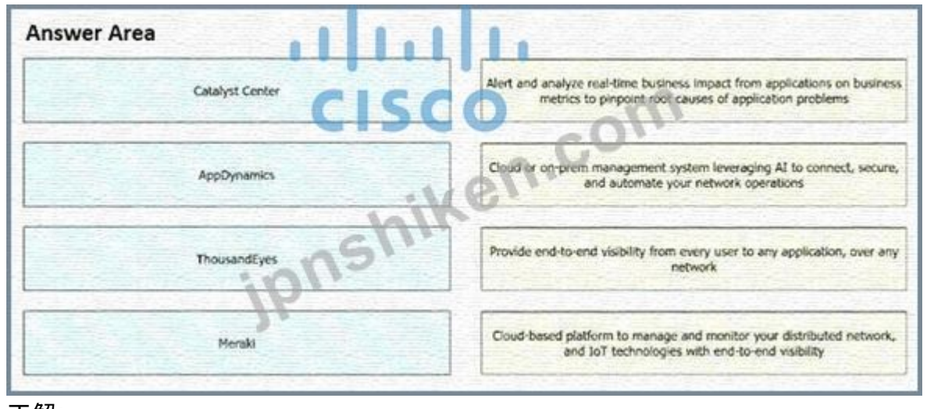

**A.** デバイス10.87.7.51のルーティング変更を確認してください
**B.** RTPテストでは現場のエージェントに関連する結果が返されないため、音声チームに連絡してください。
20（展示資料ではs20と表記）
**C.** 影響を受けた音声経路のジッターと遅延の傾向を分析し、潜在的なネットワーク輻輳を特定します。
**D.** dockerホスト10.84.50.53を確認し、エージェントコンテナが実行されていることを確認します。
正解: **(**正解を表示します**)**

質問: **36**
Thousand Eyes WAN Insightsは、ネットワーク最適化のためにどのような主要機能を提供していますか？
**A.** 機械学習アルゴリズム
**B.** リアルタイム交通状況可視化
**C.** 予測分析
**D.** エンドツーエンド暗号化
正解: **B** (コメントを発表する)
WAN Insightsは、ネットワークの問題を予測し、パフォーマンスを事前に最適化するための予測分析機能を提供します。

質問: **37**
貴社は、アラートしきい値によってイベントが発生した時点で、直ちに通知を受け取りたいと考えています。この通知はITSMシステムに送信され、インシデントが生成されることで、適切な対応が可能になります。
どのような統合方式を採用すべきでしょうか？
**A.** ServiceNowとの連携
**B.** DNAセンター統合
**C.** カスタムWebhook
**D.** アラートAPI
正解: **A** (コメントを発表する)
「エンタープライズ ネットワーク アシュアランスの設計と実装 (300-445 ENNA)」カリキュラムでは、最新のネットワーク アシュアランスの目的は、「可視性」と「アクション」の間のギャップを埋めることです。組織がネットワーク パフォーマンスの異常を処理するための自動化されたワークフローを必要とする場合、最も効率的なアーキテクチャはネイティブ ServiceNow 統合 (オプション A) です。この統合は、ThousandEyes プラットフォーム内の「カスタム構築」またはネイティブ統合として分類され、ServiceNow アカウントへの直接通知の配信を容易にするために特別に設計されています。
ENNAの実装標準によると、ThousandEyesのServiceNow連携はServiceNowのインシデント管理モジュールを利用します。定義済みの警告ルール（例えば、重要なSaaSパスにおけるパケット損失率5%のしきい値など）に違反すると、ThousandEyesはイベントをトリガーし、OAuth認証接続を介して警告データをServiceNowに即座に送信します。ServiceNow内では、このデータを使用して、テスト名、エージェントの場所、違反を引き起こした特定のメトリックなどの関連メタデータを含むインシデントが自動的に生成されます。この自動化により、監視ダッシュボードからチケットシステムに警告の詳細を「コピー＆ペースト」する手動作業が不要になり、平均識別時間（MTTI）が大幅に短縮されます。
カスタムWebhook（オプションC）は、JSONペイロードをREST APIに送信することで同様の結果を得ることができますが、受信側でデータを解析するための追加の開発作業が必要です。ServiceNowのネイティブ統合では、ThousandEyesのアラートフィールドをServiceNowのインシデントフィールドに直接マッピングする事前構成済みのテンプレートが提供され、エンタープライズグレードの導入に最適な「ワンクリック」セットアップを実現します。
オプションBとDは、ITSMインシデント生成という特定の目的には関係ありません。したがって、ITSMへの直接通知とインシデント作成には、ServiceNowネイティブ統合が推奨される方法です。

質問: **38**
合成Webテストを実施する主な目的は何ですか？
**A.** セキュリティ脆弱性の評価
**B.** ブラウザウォーターフォールの分析
**C.** ネットワークインフラストラクチャのテスト
**D.** Webアプリケーションのパフォーマンス監視
正解: (正解を表示します)
合成Webテストを実施する主な目的は、Webアプリケーションのパフォーマンスを監視し、レイテンシやダウンタイムなどの問題を事前に特定することです。

質問: **39**
サンフランシスコとテキサスの支店から北バージニアのデータセンターまでの通信を監視し、ネットワークパフォーマンスを測定するには、どのテストタイプとターゲットの組み合わせが最も適切でしょうか？
**A.** エージェント対サーバーテストタイプとクラウドエージェント
**B.** クラウドエージェントとHTTPサーバー
**C.** エンタープライズエージェントとエージェント間テストタイプ
**D.** HTTPサーバーとDNSサーバー
**E.** エージェント対サーバーテストタイプとDNSサーバー
正解: **(正解を表示します)**
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）アーキテクチャによると、管理対象拠点間のサイト間接続を監視するには、接続の両端に監視ポイントが必要です。このシナリオでは、組織は支店（サンフランシスコとテキサス）と中央データセンター（北バージニア）間のパフォーマンスを測定する必要があります。
最も適切な組み合わせは、エンタープライズエージェントとエージェント間テストタイプ（オプションC）を使用することです。エンタープライズエージェントは、支店のスイッチやルーター、データセンターのサーバーなど、組織が所有または管理するインフラストラクチャに展開されるソフトウェアプローブです。エージェント間テストは、一方向のメトリックと概算のパスデータしか提供しませんが、エージェント間テストは双方向のネットワークメトリックを提供します。これには、両方向の詳細なスループット、パケット損失、遅延、ジッターの測定値が含まれ、アプリケーションのパフォーマンスに影響を与える可能性のある非対称ルーティングやリンク飽和を特定するために不可欠です。

質問: **40**
左側のCisco Network Assuranceプラットフォームを、右側の対応するビジネスケースにドラッグアンドドロップしてください。


正解:


Explanation:
AppDynamics
カタリストセンター
サウザンドアイズ
メラキ
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）アーキテクチャでは、各プラットフォームは、最新のIT可視化フレームワークにおける、可視化と管理の明確な領域に対応するように配置されています。
AppDynamics（ケース1に該当）は、フルスタックの可観測性とアプリケーションパフォーマンス監視（APM）に特化して設計されています。その独自の特長は、コードレベルの実行やデータベースクエリといった技術的なアプリケーションパフォーマンスを、ビジネス成果やリアルタイムのビジネス指標に直接結びつけることにあります。これにより、アプリケーションの遅延が収益やユーザー満足度にどのような影響を与えるかを組織が正確に把握できるため、ビジネスインパクト分析における主要な選択肢となっています。
Catalyst Center（旧称DNA Center、事例2に該当）は、キャンパスおよび企業ネットワークインフラストラクチャの基盤となるコントローラとして機能します。AIを活用したインサイトにより、ネットワーク運用の自動化、セキュリティポリシーの適用、ローカルデバイスおよびクライアントの健全性モニタリングを一目で確認できる機能を提供します。これは、企業ネットワーク境界「内部」における接続とセキュリティ確保のための決定的な管理システムです。
ThousandEyes（ケース3に該当）は「インターネットインテリジェンス」を提供し、企業が所有していない環境全体にわたるサービス提供チェーンを監視するための重要なソリューションです。クラウド、エンタープライズ、エンドポイントエージェントからなるグローバルネットワークを活用することで、あらゆるユーザーの場所からあらゆるアプリケーション（SaaSまたはクラウド）まで、あらゆるネットワーク（インターネット、ISP、WAN）を介したエンドツーエンドの可視性を提供します。
Meraki（ケース4に該当）は、高度に分散したネットワーク環境とIoT展開の管理向けに設計されたクラウドファーストのプラットフォームです。数千もの拠点にわたるワイヤレスの状態、スイッチング、セキュリティを統合したシンプルなダッシュボードを通じてエンドツーエンドの可視性を提供するため、分散した小売店舗や支店を管理する小規模なITチームに最適です。
各プラットフォームは、企業エコシステム全体にわたる包括的なネットワーク保証を確保するために、異なるデータ収集方法（ThousandEyesではアクティブな合成テスト、Catalyst Centerではパッシブモニタリング／AIテレメトリ）を採用しています。

質問: **41**
ThousandEyesとCiscoテクノロジーの統合は、トラブルシューティングにおいてどのような利点をもたらしますか？
**A.** 手動でのデータ入力が不要になります。
**B.** エンドユーザーにリアルタイムの仮想アシスタンスを提供します。
**C.** ユーザーからのフィードバックに基づいてネットワーク構成の変更を自動化します。

**D.** パフォーマンスの問題を迅速に特定し、解決することを可能にする。11
正解: **(**正解を表示します**)**
Designing and Implementing Enterprise Network Assurance (300-445 ENNA)」認定では、Ciscoの Assurance Stack」の主な価値提案は、平均識別時間 MTTI）と平均解決時間 MTTR）の短縮であると強調しています。Catalyst、Meraki、SD-WANを含むCiscoのポートフォリオ全体にThousandEyesを統合することで、パフォーマンスの問題を迅速に特定して解決できます オプションD）。12 既存のネットワークインフラストラクチャにThousandEyesエージェントを組み込むことで、Ciscoは、パブリックインターネットやSaaS環境など、従来企業が制御していなかったドメインにまたがる エンドツーエンドの可視性」を実現します。13 トラブルシューティング中、このクロスプラットフォームの可視性により、ネットワークエンジニアは、内部ネットワークの状態 Catalyst CenterまたはMeraki Dashboardから）と外部パスの可視化 ThousandEyesから）を即座に関連付けることができます。例えば、ユーザーが Webex ミーティングでビデオ品質の低下を経験した場合、統合により、エンジニアは Webex Control Hub から直接 ThousandEyes パス ビューに クロス起動」できます。14 このピンポイントの精度により、パケット損失や遅延が発生している場所に関する 唯一の真実の情報源」が提供されるため、ネットワーク、アプリケーション、ISP チーム間の 責任のなすりつけ合い」を回避できます。
自動化機能は一部存在するものの オプションC）、その核心的な利点はフィードバックに基づく自動的な構成変更ではなく、手動またはポリシーに基づく修復に必要な実用的な洞察を提供することにある。
同様に、データ収集を効率化する一方で、その究極の目的は、複雑なハイブリッド環境における問題解決のスピードを向上させることである。

質問: **42**
ネットワークエージェントの最適な配置場所を決定する際に、遅延を最小限に抑える上で最も重要な要素は何ですか？
**A.** 外部ベンダーへのアクセス
**B.** マーケティング部門からの距離
**C.** オフィス設備の利用可能性
**D.** エンドユーザーとの近接性
正解: **(**正解を表示します**)**
エンドユーザーの近くにネットワークエージェントを配置することで、遅延を最小限に抑え、効率的なデータ収集を確保できます。

質問: **43**
ネットワーク保証データの解釈に基づくIT運用ダッシュボードの成果物には、どのような指標が推奨されますか？
**A.** パケット損失率
**B.** アプリケーションの遅延
**C.** サーバー稼働時間
**D.** 帯域幅利用率
正解: **(**正解を表示します**)**
アプリケーションのレイテンシは、ネットワーク保証データの解釈に基づき、IT運用向けダッシュボードの成果物として推奨される指標であり、アプリケーションのパフォーマンスとユーザーエクスペリエンスに関する洞察を提供します。

質問: **44**
CPU使用率と接続タイプを監視することでエンドユーザーエクスペリエンスに影響を与えるアラートルール設定はどれですか？
**A.** ユーザーエクスペリエンスアラート
**B.** パフォーマンスアラート
**C.** セキュリティ警告
**D.** しきい値アラート
正解: **A (**コメントを発表する**)**
ユーザーエクスペリエンスアラートルールは、CPU使用率、接続タイプ、およびユーザビリティに影響を与えるその他の要因を監視することで、エンドユーザーのエクスペリエンスに影響を与えます。

質問: **45**
Thousand EyesとMeraki Insightsを使用してテストを設定するプロセスは何と呼ばれますか？
**A.** ネットワークスクリプト
**B.** 合成試験
**C.** エンドポイントの展開
**D.** アクティブモニタリング
正解: **(**正解を表示します**)**
Thousand EyesとMeraki Insightsを使用したテストの設定には、ネットワークパフォーマンスを評価するためにユーザー操作をシミュレートする合成テストが含まれます。

質問: **46**
ブラウザの動作を監視することでエンドユーザーエクスペリエンスに影響を与えるアラートルールの種類は何ですか？
**A.** ユーザーエクスペリエンスアラート
**B.** しきい値アラート
**C.** パフォーマンスアラート
**D.** セキュリティ警告
正解: **(**正解を表示します**)**
ユーザーエクスペリエンスアラートルールは、ブラウザの動作を監視することでエンドユーザーのエクスペリエンスに影響を与え、ネットワーク保証におけるWebアプリケーションの最適なパフォーマンスとユーザビリティを確保します。



質問: **47**
ネットワーク保証ツールで設定されるDNSテストの主な機能は何ですか？
**A.** ネットワークトラフィックを分析する
**B.** セキュリティ上の脆弱性を特定する
**C.** ドメイン名をIPアドレスに解決する
**D.** ネットワーク遅延を監視する
正解: **C (**コメントを発表する**)**
ネットワーク保証ツールに設定されたDNSテストの主な機能は、ドメイン名をIPアドレスに解決し、DNSクエリと応答をシミュレートし、DNSサーバーのパフォーマンスを監視することで、ドメイン名解決の信頼性を確保し、DNS関連の問題を特定し、DNS解決エラーのトラブルシューティングを行うことです。

質問: **48**
ネットワークパフォーマンス分析のための指標ベースラインを設定する最初のステップは何ですか？
**A.** 主要業績評価指標（KPI）を定義する
**B.** ネットワークトラフィックパターンの分析
**C.** アラートしきい値を設定する
**D.** 過去のデータを収集する

正解: **A** (コメントを発表する)
主要業績評価指標（KPI）を定義することは、ネットワークパフォーマンス分析の指標基準を設定するための最初のステップです。

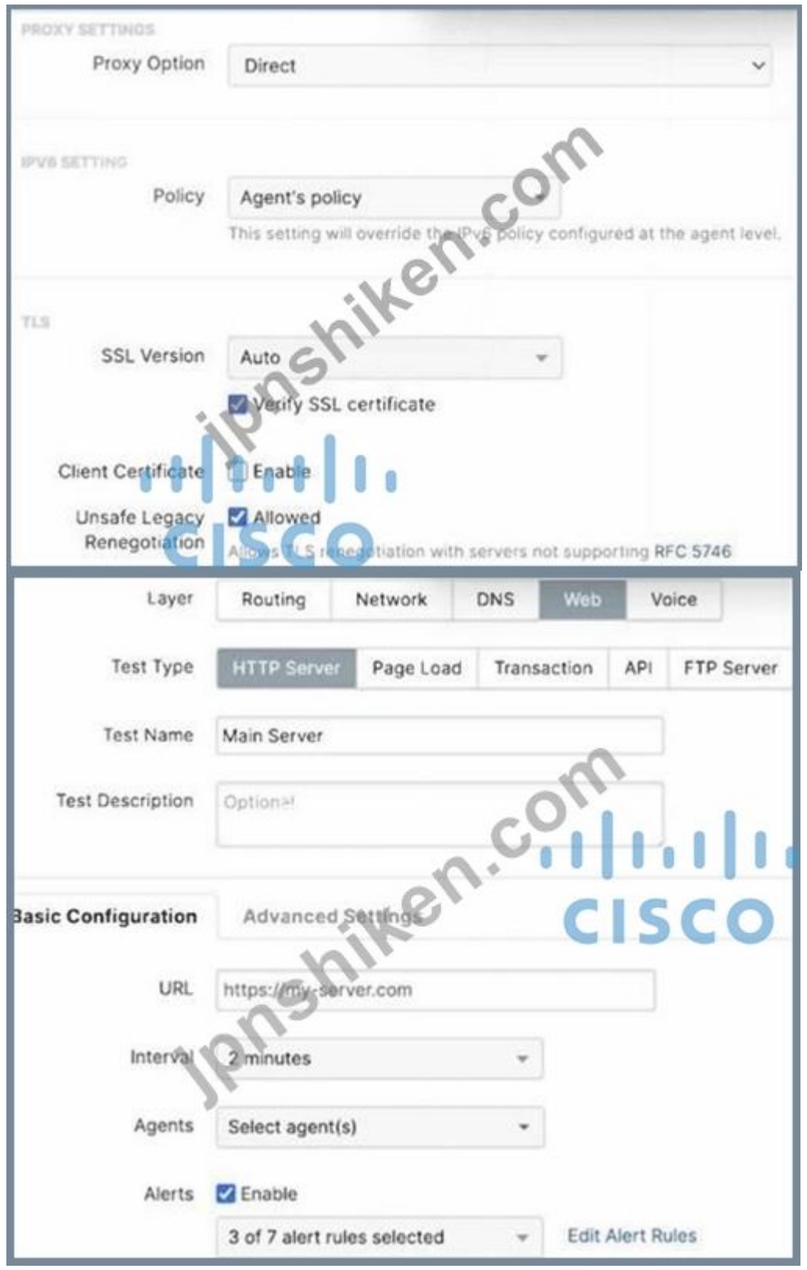
質問: **49**
トポロジー最適化は、ネットワーク容量計画にどのように貢献するのでしょうか？
**A.** ネットワーク効率の最大化
**B.** ネットワークのスケーラビリティを制限する
**C.** ネットワークセキュリティの最小化
**D.** ネットワークの複雑性を低減する
正解: (正解を表示します)
トポロジー最適化は、ネットワーク効率の最大化、データフローの改善、ネットワーク遅延の低減により、ネットワーク容量計画に貢献する。

質問: **50**
Ciscoテクノロジーとサードパーティ製アプリケーション間のシームレスなデータ交換を促進する統合タイプはどれですか？
**A.** テレメトリを開く
**B.** API連携
**C.** アラートしきい値
**D.** SNMP統合
正解: (正解を表示します)
API統合により、シスコのテクノロジーとサードパーティ製アプリケーション間のシームレスなデータ交換が可能になり、相互運用性と拡張性が向上します。

質問: **51**
vManageとThousandEyesの統合の一環として、Cisco SD-WANデバイスには通常どのようなタイプのエージェントがインストールされますか？
**A.** クラウドエージェント
**B.** ブラウザエージェント
**C.** エンタープライズエージェント
**D.** エンドポイントエージェント
正解: **C** (コメントを発表する)
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）カリキュラムでは、ThousandEyesとCisco SD-WANファブリックの統合は、最新の広域ネットワーク可視化の基盤となります。このネイティブ統合で使用される主要なエージェントタイプは、エンタープライズエージェント（オプションC）です。
ENNAの実装ガイドラインによると、ThousandEyes Enterprise Agentsは、Cisco Catalyst 8000 Edge PlatformsやISR 4000シリーズルータなどのサポート対象ハードウェアのCisco IOS XEソフトウェアスタック（バージョン17.6.1以降）上で、コンテナ化されたアプリケーションとして直接実行されます。この展開は、Cisco Catalyst SD-WAN Manager（旧vManage）によって一元的にオーケストレーションされ、Ciscoソフトウェアリポジトリからのdockerベースのエージェントイメージのダウンロードや、ブランチエッジデバイスへの初期設定のプッシュなど、ライフサイクル管理が行われます。
一度導入されると、これらのエンタープライズエージェントは、アンダーレイ伝送とSD-WANオーバーレイの両方のパフォーマンスを測定できる内部監視ポイントとして機能します。エージェントをルーターに配置することで、エンジニアは合成テストを実行し、ミッションクリティカルなSaaSアプリケーションやデータセンターサービスを支店の視点から直接監視できるため、各サイトに別途ハードウェアプローブを設置する必要がなくなります。この「ルーター上のエージェント」アーキテクチャは、設備投資（CapEx）と運用コスト（OpEx）を大幅に削減すると同時に、ISPピアリング、地域的な障害、ファブリックの状態に関する高精度なネットワークインテリジェンスを提供します。

質問: **52**
図を参照してください。エンジニアが、社内ホストのウェブサイトに対してHTTPサーバーテストを設定しています。

テスト結果に「SSL自己署名証明書」が含まれています。テストを正しく動作させるには、どのような設定が必要ですか？




**A.** クライアント証明書を有効にする。
**B.** エージェントプロキシの設定を検証します。
**C.** SSLバージョンの設定を変更します。
**D.** エージェントに証明書チェーンをインストールします。
正解: **(**正解を表示します**)**
このテストでは、SSL証明書の検証が有効になっています。

自己署名証明書またはプライベートCA証明書を使用する内部サーバーの場合、エージェントはそのCAを信頼する必要があります。
エンタープライズエージェントに証明書チェーンをインストールすることで、SSL検証が成功し、「自己署名証明書」エラーを防ぐことができます。

質問: **53**
貴社は、アラートのしきい値によってイベントが発生した時点で、直ちに通知を受け取りたいと考えています。
この通知はITSMに送信され、インシデントが生成されて適切に対応できるようになります。どのような統合方法を使用すべきでしょうか？
**A.** ServiceNowとの連携
**B.** DNAセンター統合
**C.** カスタムWebhook
**D.** アラートAPI
正解: **(**正解を表示します**)**
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）カリキュラムでは、現代のネットワーク保証の目的は、「可視性」と「アクション」の間のギャップを埋めることです。
組織がネットワークパフォーマンスの異常に対処するための自動化されたワークフローを必要とする場合、最も効率的なアーキテクチャは、ServiceNowとのネイティブ統合（オプションA）です。この統合は、ThousandEyesプラットフォーム内の「カスタム構築」またはネイティブ統合に分類され、ServiceNowアカウントへの直接通知の配信を容易にするために特別に設計されています。
ENNA実装標準によると、ThousandEyes ServiceNow統合はServiceNowインシデント管理モジュールを利用します。事前定義されたアラートルール（たとえば、
重要なSaaSパスで5%のパケット損失しきい値を超えると、ThousandEyesはイベントをトリガーし、OAuth認証接続を介してアラートデータをServiceNowに即座に送信します。
ServiceNow内では、このデータを使用してインシデントが自動的に生成されます。インシデントには、テスト名、エージェントの場所、違反を引き起こした特定のメトリックなどの関連メタデータが含まれます。
この自動化により、監視ダッシュボードからチケットシステムにアラートの詳細を「コピー＆ペースト」する手作業が不要になり、平均識別時間（MTTI）が大幅に短縮されます。

質問: **54**
ネットワーク保証におけるスクリプトエージェントの主な機能は何ですか？
**A.** サーバー構成の最適化
**B.** セキュリティログの分析
**C.** ハードウェアの状態監視
**D.** 反復作業の自動化
正解: **(**正解を表示します**)**
スクリプトエージェントは、反復的なタスクを自動化することで、運用効率を高め、安定したネットワークパフォーマンスを確保します。

質問: **55**
ThousandEyes WAN InsightsはCisco SD-WANと統合し、ネットワークパフォーマンスの可視化とパス推奨機能を提供します。WAN Insightsが機能するために不可欠なSD-WAN環境のデータソースはどれですか？（2つ選択してください）
**A.** デバイステンプレートや集中管理ポリシー設定など、vManageからの構成データ。
**B.** vAnalyticsによって収集された過去のネットワークパフォーマンス指標。SD-WANトンネルの損失、遅延、ジッターなどが含まれます。
**C.** SD-WAN内のエンドユーザーデバイスにインストールされたThousandEyesエンドポイントエージェントから収集されたデータ。
**D.** SD-WANデータプレーンからのアプリケーショントラフィックフローデータ。vManageアプリケーションリスト別に分類されています。
**E.** SD-WANエッジルーターからのSyslogメッセージ。トンネル確立に関連するデバイスイベントとエラーを示します。
正解: **B,D (**コメントを発表する**)**
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）のアーキテクチャでは、ThousandEyes WAN InsightsがCisco SD-WAN管理スタックとの緊密な統合に依存していることが規定されています。
予測パスの推奨を生成するために、プラットフォームはネットワークの動作とネットワークを通過するアプリケーションの両方を反映した特定のテレメトリデータを取り込む必要があります。

最初の重要なデータソースは、vAnalytics（オプションB）によって収集された過去のネットワークパフォーマンスメトリクスです。WAN Insightsをアクティブ化する前に、vAnalyticsを有効にして、エッジルータから生のネットワークテレメトリを収集し、データを充実させる必要があります。このデータには、パケット損失、遅延、ジッターなど、各SD-WANトンネルの詳細なメトリクスが含まれます。WAN Insightsはこれらの過去の傾向を分析し、将来のパス品質を予測し、どのトランスポート回線が長期的にアプリケーションのSLAを満たす可能性が最も高いかを判断します。
2 つ目の重要なデータ ソースは、アプリケーションのトラフィック フロー データです (オプション D)。WAN Insights は、ファブリック内で現在アクティブになっているアプリケーションを把握し、推奨事項の優先順位付けを行う必要があります。
Office 365、Webex、またはカスタム社内アプリケーションなどの「ビジネスに不可欠な」サービス。この情報は、SD-WANデータプレーンからフローレコードとして取り込まれ、Cisco Catalyst SD-WAN Manager（vManage）で定義されたアプリケーションリストに基づいて分類されます。

質問: **56**
ThousandEyesとCiscoテクノロジーの統合は、トラブルシューティングにおいてどのような利点をもたらしますか？
**A.** 手動でのデータ入力が不要になります。
**B.** エンドユーザーにリアルタイムの仮想アシスタンスを提供します。
**C.** ユーザーからのフィードバックに基づいてネットワーク構成の変更を自動化します。
**D.** パフォーマンスの問題を迅速に特定し、解決することができます。
正解: **(**正解を表示します**)**
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）認定資格では、Ciscoの「Assurance Stack」の主な価値提案は、平均識別時間（MTTI）と平均解決時間（MTTR）の短縮であると強調されています。Catalyst、Meraki、SD-WANを含むCiscoのポートフォリオ全体にThousandEyesを統合することで、パフォーマンスの問題を迅速に特定して解決できます（オプションD）。
シスコは、ThousandEyesエージェントを既存のネットワークインフラストラクチャに組み込むことで、
従来企業が制御していなかったパブリックインターネットやSaaS環境などのドメインにまたがる「エンドツーエンドの可視性」。トラブルシューティング中、このクロスプラットフォームの可視性により、ネットワークエンジニアは内部ネットワークの状態（Catalyst CenterまたはMeraki Dashboardから）と外部パスの可視化（ThousandEyesから）を即座に関連付けることができます。たとえば、Webexミーティングでユーザーがビデオ品質の低下を経験すると、統合によりエンジニアは
Webex Control Hub から ThousandEyes パス ビューに直接「クロス ローンチ」します。このピンポイントの精度により、ネットワーク、アプリケーション、ISP チーム間の「責任のなすりつけ合い」を回避し、
パケット損失や遅延が発生している場所に関する「唯一の信頼できる情報源」。
自動化機能は一部実装されているものの（オプションC）、その核心的な利点はフィードバックに基づく自動的な構成変更ではなく、手動またはポリシーベースの修復に必要な実用的な洞察を提供することにある。同様に、データ収集を効率化する一方で、その究極の目的は複雑なハイブリッド環境における問題解決の迅速化にある。

質問: **57**
BGPルーティングデータを分析することで、ネットワークパフォーマンスに影響を与えるどのセキュリティ上の問題を特定できますか？
**A.** ルートリーキング
**B.** DDoS攻撃
**C.** DNSハイジャック
**D.** BGPハイジャック
正解: **(**正解を表示します**)**
BGPハイジャックは、BGP（ボーダーゲートウェイプロトコル）ルーティングデータを分析することで特定できる、ネットワークパフォーマンスに影響を与えるセキュリティ問題です。BGPハイジャックは、権限のない第三者が所有していないIPアドレスプレフィックスをアナウンスし、それらのアドレス宛てのトラフィックを不正な宛先に転送することで発生し、ネットワークの混雑やパフォーマンスの低下につながります。

質問: **58**

あなたは、基本認証を使用するWebアプリケーションを対象としたThousandEyesトランザクションテストで断続的に発生する障害を調査しています。この障害は、異なるエージェントや時間帯でランダムに発生します。この問題を解決するために、どのような手順を踏みますか？（該当するものをすべて選択してください）

**A.** ウェブアプリケーションのベンダーに連絡して問題を報告し、サーバー側の問題の可能性について問い合わせてください。

**B.** 問題を切り分けるために、テスト構成で基本認証を無効にします。

**C.** 異なる場所からアプリケーションに手動でログインして、認証情報の正当性を確認します。

**D.** ThousandEyesのウォーターフォールチャートとHTTPレスポンスコードを分析し、潜在的なボトルネックやエラーを特定します。

正解: **(**正解を表示します**)**

断続的なパフォーマンス問題のトラブルシューティングは、「エンタープライズネットワーク保証の設計と実装（300-445 ENNA）」カリキュラムの中核をなす要素です。基本認証を使用したトランザクションテストがランダムに失敗した場合、エンジニアは多層的な診断アプローチを用いて、障害の原因が認証情報、ネットワークパス、またはアプリケーションサーバーのいずれにあるかを特定する必要があります。

最初のステップは、認証情報の正当性を確認することです（オプションB）。基本認証では認証情報がヘッダーにエンコードされるため、ユーザー権限の変更やアカウントのロックアウトが発生すると、即座に認証エラーが発生します。

さまざまな地理的な場所から手動でログインを実行することで、場所に基づくアクセス制御リスト（ACL）や地域的なIdP同期の問題を排除するのに役立ちます。

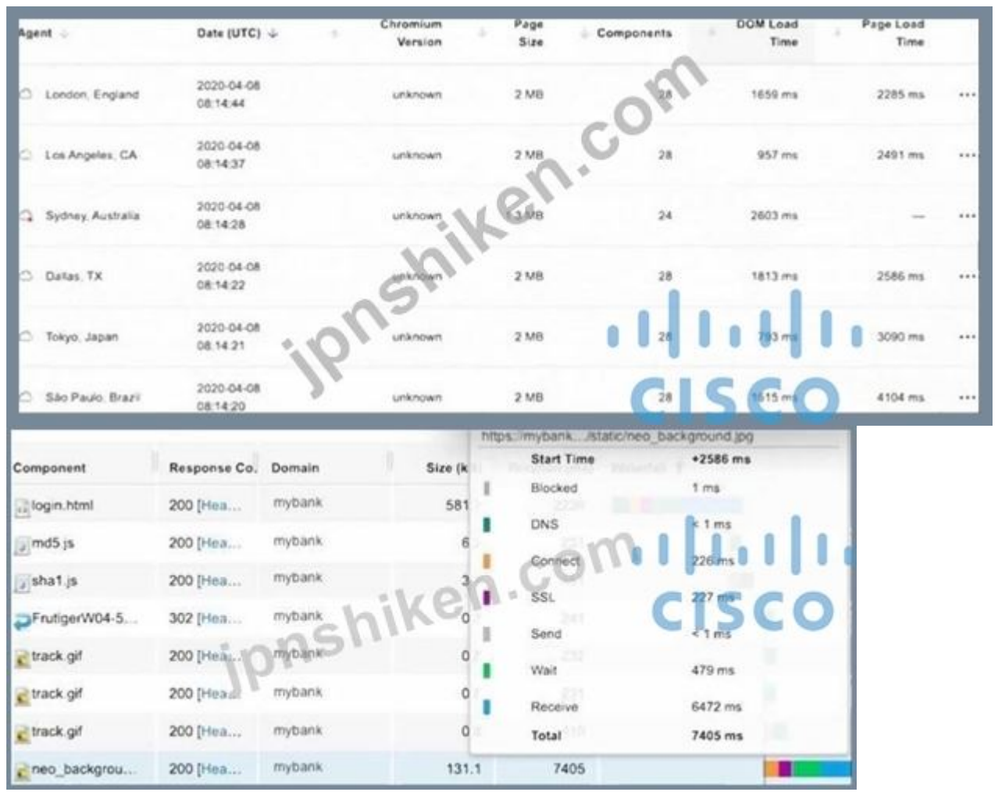
最もデータ量の多い診断手順は、ThousandEyesのウォーターフォールチャートとHTTPレスポンスコードを分析することです（オプションC）。ウォーターフォールビューを使用すると、エンジニアは障害が最初の401 Unauthorizedチャレンジ中に発生したのか、認証情報が送信された後に発生したのかを確認できます。チャートに「待機時間」が高い、または5xxエラーが表示されている場合は、サーバー側の遅延または不安定性が問題の原因である可能性が高いです。「接続時間」が高い場合は、ネットワーク層の輻輳が問題の原因である可能性があります。

最後に、テレメトリでネットワークパスは正常と示されているにもかかわらず、サーバーが断続的にエラーを返したりタイムアウトしたりする場合は、エンジニアはWebアプリケーションベンダーに連絡する必要があります（オプションD）。ベンダーに特定のThousandEyes「共有リンク」を提供することで、ベンダーは全く同じパケットレベルおよびブラウザレベルのデータを確認でき、問題がクライアントのネットワークではなくサーバー側のインフラストラクチャにあることを証明できます。認証を無効にする（オプションA）ことは、認証されたワークフローを監視するために特別に設計されたテストの有効なトラブルシューティング手順ではありません。

質問: **59**

図を参照してください。Cisco ThousandEyes は、銀行の Web サイトが読み込めないというアラートを送信しました。

シドニーのクラウドエージェントから10秒の回答です。ウェブサイトの障害の根本原因は何ですか？




**A.** Frutigerフォントオブジェクトを読み込む際に、無限HTTP 302リダイレクトループが発生しました。
**B.** シドニークラウドエージェントでCPU飽和問題が発生しました。
**C.** HTTPサーバー上にlogin.htmlオブジェクトが存在しません。
**D.** シドニークラウドエージェントと銀行ウェブサイト間で帯域幅の問題が発生しました。
正解: **D** (コメントを発表する)
ウォーターフォール図から判断すると、重大な遅延は、大きなneo_background.jpgオブジェクトの受信フェーズ中に発生します。
受信時間: 6472 ms
- 合計読み込み時間: 7405 ms
DNS、接続、SSL、送信にかかる時間は正常です。
受信時間が長い場合は、リダイレクト、CPUの問題、またはオブジェクトの欠落ではなく、データ転送速度が遅いことを示しています。
これは、シドニーのクラウドエージェントと銀行サイト間の経路における帯域幅のスループットの問題を明確に示している。

質問: **60**
ネットワーク監視エンジニアは、Linuxパッケージとしてインストールされたエージェントからの平均パケット損失を表示するウィジェットを作成するよう指示されました。選択すべきデータソースと測定方法はどれでしょうか？
**A.** エンドポイントエージェントとメディアン
**B.** クラウド＆エンタープライズエージェントと平均
**C.** ルーティングと標準偏差
**D.** デバイスとnパーセンタイル

正解: (正解を表示します)
エンタープライズ ネットワーク保証の設計と実装 (300-445 ENNA) では、ダッシュボード ウィジェットを適切なテレメトリ データ ソースと統計的尺度にマッピングする必要があります。エージェントが組織のインフラストラクチャに Linux パッケージとしてインストールされると、エンタープライズ エージェントとして分類されます。
このウィジェットの正しい構成は、クラウドとエンタープライズエージェント、および平均 オプションB）です。
* データソース: Linux ベースのエージェントはエンタープライズエージェントであるため、ThousandEyes ダッシュボードの設定メニューでクラウドエージェントと同じデータソースカテゴリを共有します。
* 測定:要求された 平均」パケット損失を表示するには、平均値（算術平均が適切な統計的尺度です。
その他の選択肢は不適切です。
* オプション A:エンドポイント エージェントは、Windows/macOS ユーザー デバイスにインストールされるもので、通常はインフラストラクチャ監視に使用される標準的な Linux サーバー パッケージではありません。中央値は平均値ではなく、中央値を示します。
* オプション C:ルーティングは BGP データを参照しており、合成ネットワーク テストと同じ方法でパケット損失を報告しません。
* オプション D: Devices は SNMP を介して監視されるハードウェアを指し、annth Percentile は単純な平均ではなく、特定の統計的カットオフ (95 パーセンタイルなど) を指します。

質問: **61**
ネットワークアシュアランスで収集したデータを使用して特定できる、ネットワークパフォーマンスに影響を与えるセキュリティ上の問題はどれですか？
**A.** TCPハンドシェイクの失敗
**B.** DDoS攻撃
**C.** SQLインジェクション攻撃
**D.** DNS解決失敗
正解: (正解を表示します)
DDoS攻撃はネットワークパフォーマンスに影響を与えるセキュリティ上の問題であり、ネットワーク保証において収集されたデータを用いて特定することで、脅威に対する予防的な対策が可能になります。



質問: **62**
スイッチにThousandEyesエージェントをデプロイするには、どのような方法がありますか？（該当するものをすべて選択してください）
**A.** アプリケーションホスティング
**B.** カタリストセンター（旧DNAセンター）
**C.** Catalyst SD-WAN Manager（旧称vManage）
**D.** ThousandEyesポータルの 「エンタープライズ＆クラウドエージェント」セクションから
**E.** 上記のすべて
正解: (正解を表示します)
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）アーキテクチャでは、スイッチングインフラストラクチャへのThousandEyes Enterprise Agentの展開は、さまざまな管理スタイルとネットワーク規模に対応できるよう、非常に柔軟に設計されています。最新のCiscoスイッチ、特にCatalyst
9300 および 9400 シリーズは、Cisco IOS XE Application Hosting フレームワークを介して、スイッチのハードウェア上でコンテナ化されたアプリケーションを直接実行することをサポートします。1 Application Hosting (オプション A) は、Cisco IOS XE コマンドライン インターフェイス (CLI) を使用した手動方式を指します。エンジニアは、pp-hosting コマンドを使用して、Docker ベースの Enterprise Agent をインストール、構成、および管理できます。2 これにより、コンテナのリソース割り当てとネットワークをきめ細かく制御できます。Catalyst Center (オプション B) は、GUI 駆動型の自動化されたワークフローを提供し、キャンパス ファブリック全体にエージェントを大規模に展開します。3 これにより、複数のスイッチへのインストールとアクティベーションを同時に処理することで、ライフサイクル管理が簡素化されます。SD-

WAN ファブリックのエッジ デバイスとして機能するスイッチの場合、Catalyst SD-WAN Manager (オプション C) は、集中管理されたポリシーとテンプレートを使用して展開をオーケストレーションし、デバイス構成の一部としてエージェントをプッシュできるようにします。最後に、ThousandEyesポータル（オプションD）はテストの管理プレーンであると同時に、前述のどのデプロイ方法においても、Dockerイメージとアカウントグループトークンを取得する場所でもあります。
どの方法も最終的な結果は同じです。つまり、アクセス層またはコア層から直接始まるネットワークパスの詳細な可視性を提供するために、「オンボックス」で実行されるエンタープライズエージェントが実現されます。したがって、上記のすべて（オプションE）が正解です。これは、300-445 ENNA公式ガイドラインに従って、スイッチベースの展開で利用可能な手動、自動、およびオーケストレーションによる方法を網羅しているためです。

質問: **63**
無線接続に関する収集データを用いて診断される一般的な問題は何ですか？
**A.** ネットワークの混雑
**B.** チャネル干渉
**C.** パケット損失
**D.** DNSサーバーの障害
正解: **(**正解を表示します**)**
チャネル干渉は、無線接続に関する収集データを用いて診断される一般的な問題であり、ネットワーク保証における信号品質とネットワークパフォーマンスに影響を与える。

質問: **64**
ネットワークチームは、Webex RoomOSエンドポイントエージェントを導入し、Webex Control HubをThousandEyesと統合しました。VoIPチームは、Webex Control Hubビューからどのようなメトリックを収集できるかを知りたいと考えています。VoIPチームは、ネットワークデータをどこで確認すればよいでしょうか？
**A.** デバイス
**B.** ネットワークパス
**C.** ユーザー
**D.** 設定
正解: **B (**コメントを発表する**)**
「エンタープライズ ネットワーク アシュアランスの設計と実装 (300-445 ENNA)」カリキュラムによると、ThousandEyes と Webex Control Hub の統合により、コラボレーション サービスのトラブルシューティング エクスペリエンスが効率化されます。VoIP チームが、遅延、損失、ジッターなどの ThousandEyes ネットワーク テレメトリにアクセスするには、Control Hub の [トラブルシューティング] タブ内の [ネットワーク パス (オプション B)] セクションに移動する必要があります。15 ネットワーク パスの視覚化は、ThousandEyes Endpoint Agent データが Webex インターフェイスに取り込まれた結果です。16 会議中にユーザーまたは RoomOS デバイスで音声またはビデオの品質が低下すると、Control Hub のトラブルシューティング ビューに、参加者の詳細の下に「ネットワーク パス」の行が表示されます。
17この行をクリックすると、VoIPチームはコラボレーションデバイスからWebexメディアノードまでの全経路のホップごとの内訳を確認できます。このビューでは、パフォーマンスが問題となる特定のホップが強調表示されます。
遅延（400ms超）または損失（5%超）に関する事前定義された閾値に基づいて、「不良」（赤）、「普通」（黄）、「良好」（緑）のいずれかに分類されます。
「デバイス」（オプションA）ではエージェントをアクティブ化し、「ユーザー」（オプションC）では特定の参加者を選択できますが、実際のテレメトリ指標とネットワーク経路の視覚化は、ネットワークパスビューにのみ表示されます。この統合により、VoIPチームはWebex環境を離れて初期トリアージを行う必要がなくなり、「ネットワークパス」ダッシュボードから直接、問題が支店のローカルなものか、サービスプロバイダーのネットワークの奥深くにあるものかを識別できるようになります。

質問: **65**
ネットワーク保証における合成ユーザーエージェントの主な機能は何ですか？
**A.** サーバーログの分析
**B.** シミュレーションされたトラフィックの生成

**C.** 物理ハードウェアの監視
**D.** ファイアウォールの設定
正解: (正解を表示します)
合成ユーザーエージェントは、ネットワークのパフォーマンスを評価し、潜在的な問題を特定するために、シミュレーションされたトラフィックを生成します。

質問: **66**
ネットワーク管理者は、コア ルーターの CPU 使用率の基準値を確立したいと考えています。この目的に最も適したデータ ソースはどれでしょうか？
**A.** ThousandEyesテストによるDNS解決時間
**B.** ThousandEyesテストによるHTTPサーバーの応答時間
**C.** ルーターから収集されたSNMPデータ
**D.** ThousandEyesテストによるネットワークパスの可視化
正解: (正解を表示します)
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）フレームワークにおいて、ベースライン設定とは、異常の検出を可能にするために、ネットワークインフラストラクチャの「正常な」パフォーマンスプロファイルを確立するプロセスです。コア ルータの CPU 使用率など、物理デバイスの内部状態を指標とする場合、SNMP（Simple Network Management Protocol）が業界標準のデータ ソースとなります。SNMPは、デバイスの制御プレーンとハードウェアのパフォーマンスを直接可視化します。Cisco Catalyst Centerやサードパーティ製のNMSなどの監視システムは、ルータの管理情報ベース（MIB）から特定のオブジェクト識別子（OID）をポーリングすることで、CPUサイクル、メモリ割り当て、温度に関する詳細なデータを収集できます。この「内部から外部へ」のテレメトリは、さまざまなトラフィック負荷時のルータの実際のリソース消費を反映するため、ベースライン設定に不可欠です。
一方、ThousandEyesテスト（オプションA、B、D）は「外部から内部へ」の合成データを提供します。DNS解決時間（オプションA）、HTTP応答時間（オプションB）、パス可視化（オプションD）はエンドツーエンドのサービス提供とネットワークトランジットの健全性を測定するのに優れていますが、ルーターの内部ハードウェアの状態は報告しません。たとえば、ルーターのCPU使用率が99%（クラッシュの可能性を示唆）であっても、データプレーン（ASIC）がパケットを効率的に転送している場合は、ThousandEyesパステストで「グリーン」パスが表示される可能性があります。したがって、CPUなどのハードウェア固有のメトリックの信頼できるベースラインを確立するには、SNMPデータ（オプションC）が選択肢の中で唯一適切なソースとなります。

質問: **67**
ネットワーク分析において、エンドデバイスのネットワーク問題を診断する主な目的は何ですか？
**A.** ネットワークセキュリティの脆弱性の評価
**B.** サーバーパフォーマンス指標の分析
**C.** 接続問題の特定と解決
**D.** ネットワークトラフィックパターンの監視
正解: (正解を表示します)
エンドデバイスのネットワーク問題を診断する主な目的は、ネットワーク内の個々のデバイス（コンピュータ、スマートフォンなど）に影響を与える接続問題を特定して解決し、ネットワークリソースとサービスへのシームレスなアクセスを確保することです。

質問: **68**
ネットワーク保証において、TCPプロトコルの動作を監視するために使用されるアラートルールの構成タイプは何ですか？
**A.** 州ベースのルール
**B.** エラーカウンターに基づくルール
**C.** 混雑状況に基づくルール
**D.** パフォーマンスに基づくルール
正解: **D** (コメントを発表する)

パフォーマンスベースのルールは、ネットワーク保証においてTCPプロトコルの動作を監視するために使用されます。ラウンドトリップタイム（RTT）、再送信率、TCP接続確立時間などのメトリックに閾値を設定することで、異常を検出し、パフォーマンスの逸脱が発生した場合にアラートをトリガーします。

質問: **69**
収集したデータを使用してネットワークの問題を診断する際の最初のステップは何ですか？
**A.** 影響を受けるデバイスの特定
**B.** パフォーマンス指標の分析
**C.** パケットトレースの解析
**D.** ネットワーク異常の特定
正解: **(**正解を表示します**)**
収集したデータを用いてネットワークの問題を診断する最初のステップは、パフォーマンス指標を分析して、通常のネットワーク動作からの逸脱を特定することです。

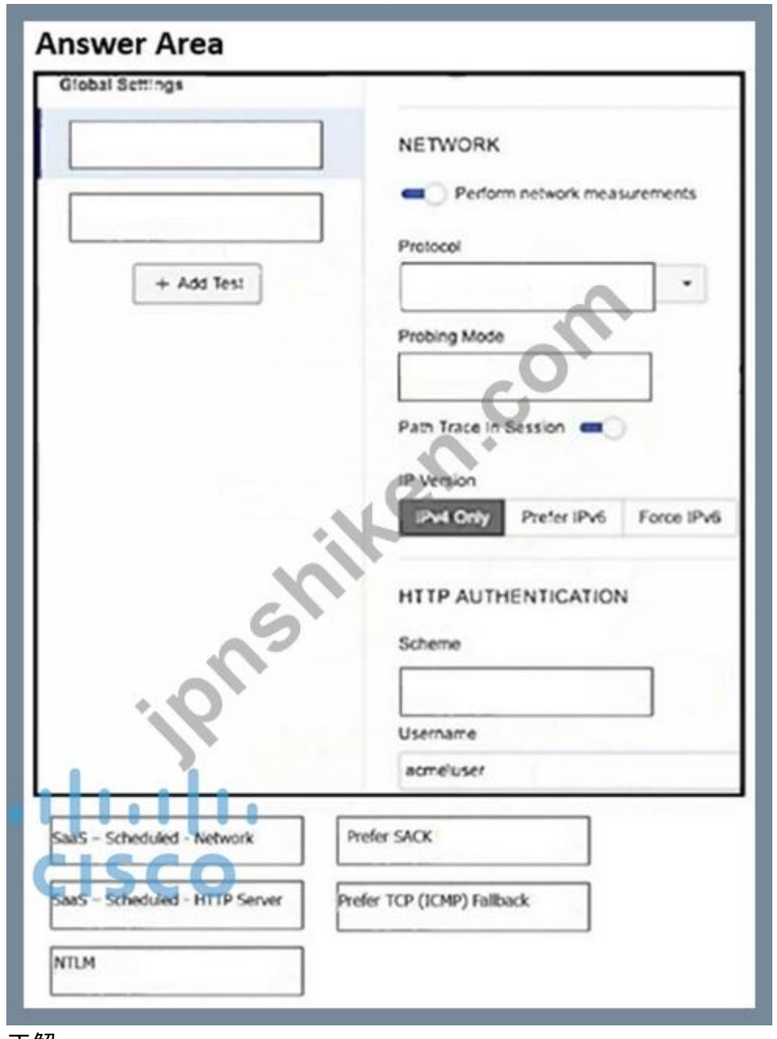
質問: **70**
ウェブアプリケーションのパフォーマンス問題を診断する際、ブラウザウォーターフォールは主にどのような点の特定に役立ちますか？
**A.** ネットワーク暗号化強度
**B.** ファイアウォールのスループット
**C.** SSL証明書の有効性
**D.** 最初のバイトに到達するまでの時間（TTFB）
正解: **(**正解を表示します**)**

質問: **71**
アラートルールの検証は、ネットワークの信頼性向上にどのように貢献するのでしょうか？
**A.** ハードウェアの冗長性を削減する
**B.** ネットワークの複雑性の増大
**C.** アラートの正確性を確保する
**D.** データ収集の制限
正解: **(**正解を表示します**)**
アラートルールの検証は、アラートの正確性と信頼性を確保することでネットワークの安全性を高め、ネットワークの問題や脆弱性をタイムリーに検出・解決することを可能にします。

質問: **72**
パケットロスなどのネットワーク問題を診断する際、通常、どのような収集データが分析されますか？
**A.** ユーザー認証ログ
**B.** パフォーマンス指標
**C.** ネットワークトラフィックログ
**D.** サーバー構成
正解: **(**正解を表示します**)**
パケット損失などのネットワーク問題を診断する際には、ルーター、スイッチ、ファイアウォールといったネットワーク機器から収集されたパフォーマンス指標が一般的に分析されます。これらの指標には、ラウンドトリップタイム（RTT）、ジッター、パケット損失率などが含まれ、異常を特定し、ネットワークパフォーマンスの問題をトラブルシューティングするために用いられます。

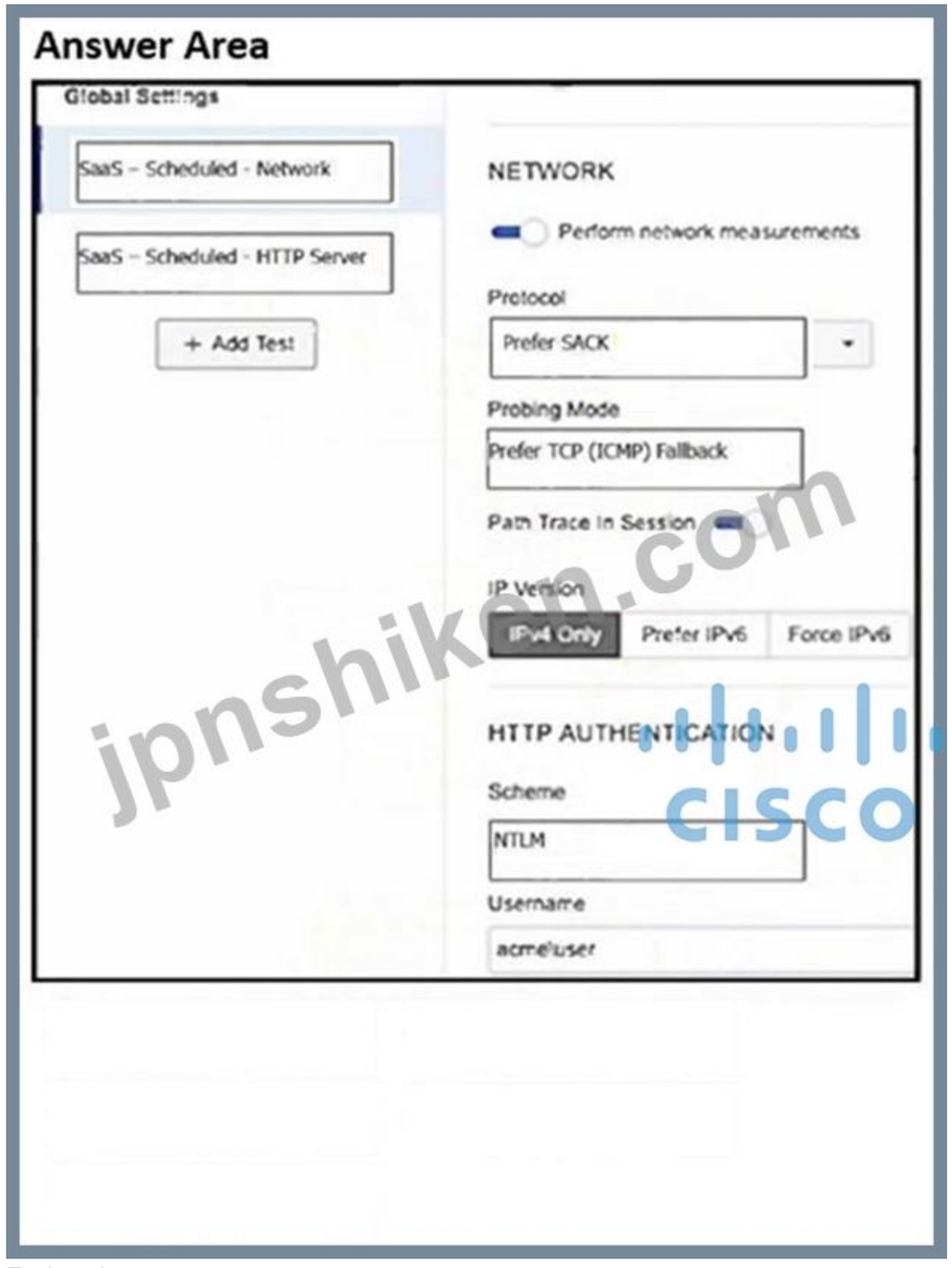
質問: **73**

ドラッグアンドドロップ問題
エンジニアがエンドユーザー向けにマルチテストテンプレートを展開しています。要件には、Cisco ThousandEyes Endpoint Agentからターゲットへの単一のTCPセッションの確立、セキュア認証のテスト、およびTCPパストレースが含まれます。下部にあるオプションをテスト構成テンプレートのボックスにドラッグアンドドロップしてください。




正解:

## Answer Area






Explanation:

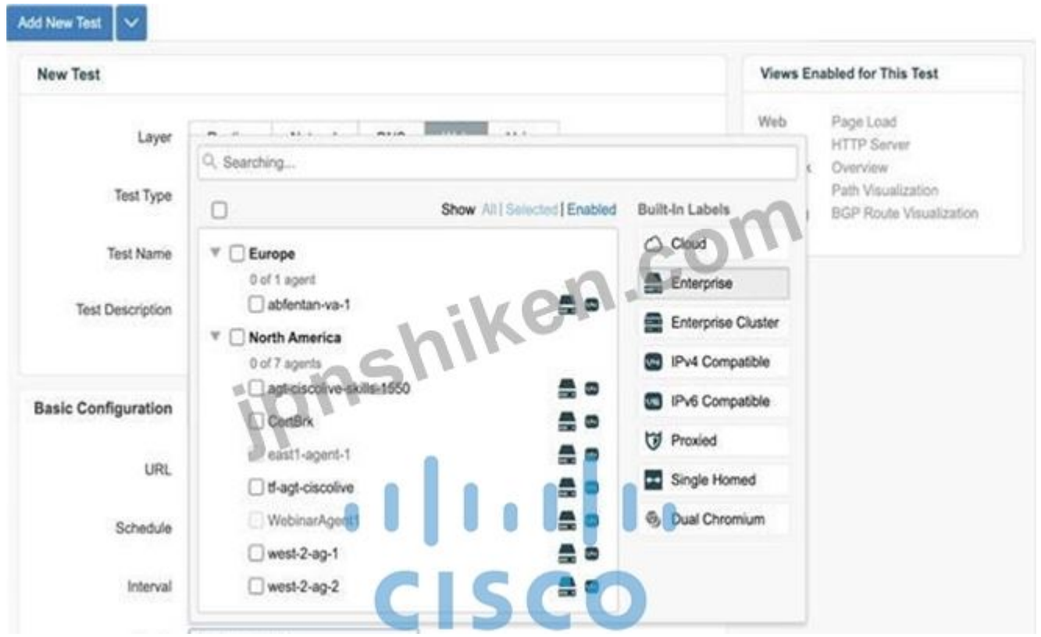
SaaSスケジュールHTTPサーバーテストは、ThousandEyesエンドポイントエージェントからターゲットアプリケーションへの単一のTCPセッションを提供します。これをSaaSスケジュールネットワークテストと組み合わせることで、対応するネットワーク測定値が追加されます。

プロトコルを「Prefer SACK」（SSL）に設定すると、セッションがHTTPSを使用して確立されることが保証されます。

「TCP（ICMP）フォールバック優先」は、プローブ方法としてTCPを使用することで、ターゲットへのTCPベースのパス追跡を可能にします。

HTTP認証方式としてNTLMを使用することで、対象アプリケーションに対する安全なユーザー認証を検証できます。

質問: **74**
エンジニアがページ読み込みテストの設定を行い、east1-agent-1 に実行を割り当てようとしていますが、そのエージェントが一覧に表示されません。指定されたエージェントが表示されない理由は何でしょうか？




**A.** エージェントが実行されていません
**B.** エージェントが無効になっています
**C.** エージェントはまだ登録中です
**D.** エージェントはページ読み込みテストをサポートしていません
正解: **D** (コメントを発表する)
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）の枠組みにおいて、特定のテストタイプに適したエージェントを選択することは、重要な構成手順です。ThousandEyesプラットフォームは、基盤となるハードウェアおよびソフトウェア環境に応じて、異なるエージェントバイナリと機能を使用します。具体的には、ページロードテストとトランザクションテストでは、Webコンテンツをレンダリングし、DOM関連のメトリックを測定できるように、エージェントにブラウザエンジン（Chromium）がインストールされ、正常に動作している必要があります。
ENNAの実装ガイドラインによると、すべてのエンタープライズエージェントがこれらのブラウザベースのテストをサポートしているわけではありません。図には、エンジニアが「east1-agent-1」を検索している「新規テスト」設定画面が表示されています。「west-2-ag-1」などの他のエージェントは表示されますが、指定されたエージェントはページ読み込みテスト（オプションD）をサポートしていないため表示されません。このような現象は、特定のCisco Catalyst 9000スイッチやCisco ISR 4000シリーズルータなど、リソースに制約のあるハードウェアにエンタープライズエージェントが展開されている場合によく発生します。これらのハードウェアでは、メモリやCPUの制限により、Chromiumブラウザパッケージがサポートされていないか、有効になっていないためです。

質問: **75**
スイッチにThousandEyesエージェントをデプロイするには、どのような方法がありますか？（該当するものをすべて選択してください）
**A.** アプリケーションホスティング
**B.** カタリストセンター（旧DNAセンター）
**C.** Catalyst SD-WAN Manager（旧称vManage）

**D.** ThousandEyesポータルの「エンタープライズ＆クラウドエージェント」セクションから
**E.** 上記のすべて
正解: **(**正解を表示します**)**
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）アーキテクチャでは、スイッチングインフラストラクチャへのThousandEyes Enterprise Agentの展開は、さまざまな管理スタイルやネットワーク規模に対応できるよう、高い柔軟性を備えるように設計されています。最新のCiscoスイッチ、特にCatalyst 9300および9400シリーズは、Cisco IOS XEアプリケーションホスティングフレームワークを介して、コンテナ化されたアプリケーションをスイッチのハードウェア上で直接実行することをサポートしています。

質問: **76**
収集したデータを用いてエンドデバイスのネットワーク問題を診断する主な目的は何ですか？
**A.** 接続問題の解決
**B.** サーバーパフォーマンスの最適化
**C.** デバイスのコンプライアンスを確保する
**D.** ネットワークの脆弱性の特定
正解: **A (**コメントを発表する**)**
収集したデータを用いてエンドデバイスのネットワーク問題を診断する主な目的は、デバイスのパフォーマンスやユーザーエクスペリエンスに影響を与える接続問題を特定し、解決することです。



質問: **77**
ThousandEyesエンドポイントエージェントを使用してMicrosoft Teamsを監視したい場合、このタイプのアプリケーション監視で利用できるテストにはどのようなものがありますか？
**A.** 予定されているテスト
**B.** 動的テスト
**C.** スケジュールされたテスト、動的なテスト、および実際のユーザーテスト
**D.** 定期テストと動的テスト
正解: **D (**コメントを発表する**)**
コラボレーション監視のベストプラクティスである「Designing and Implementing Enterprise Network Assurance (300-445 ENNA)」によると、Microsoft Teams (Webex および Zoom も含む) は、スケジュールされたテストと動的テストの組み合わせ (オプション D) を使用して監視されます。
* スケジュールされたテスト: これらは、Microsoft Teams インフラストラクチャの到達可能性とパフォーマンスを事前に監視するために使用されます。Teams テンプレートには通常、teams.microsoft.com および login.microsoftonline.com へのスケジュールされた HTTP サーバー テストと、Teams トランスポート リレー (worldaz.tr.teams.microsoft.com など) へのネットワーク レイヤー テストが含まれています。これにより、ユーザーが通話中かどうかに関わらず、接続性の継続的なベースラインが提供されます。
* 動的テスト :これはコラボレーション監視のための独自の機能です。エンドポイントエージェントがTeamsアプリケーションがリアルタイムメディアセッション（音声またはビデオ通話）を開始したことを検出すると、その通話に使用されている特定のIPアドレスとポートに対して動的テストが自動的にトリガーされます。これにより、ITチームはセッションがアクティブな間、実際の通話トラフィックの正確なネットワークパス（ホップごとの遅延や損失を含む）を確認できます。
リアルユーザーテスト（オプションC）は、WebベースのSaaSアプリの場合とは異なり、Teamsの監視には通常使用されません。ほとんどのユーザーはブラウザではなくTeamsデスクトップクライアントを使用するため、RUMブラウザ拡張機能ではデスクトップアプリケーションの内部シグナリングやメディアストリームの豊富なテレメトリをキャプチャできません。そのため、ダイナミックテストによる専用の「自動セッションテスト」と、スケジュールテストによるプロアクティブなヘルスチェックを組み合わせることで、Microsoft Teamsの完全な保証戦略が実現します。

質問: **78**
ネットワーク保証において、地域債権回収業者の目的は何ですか？
**A.** 近くのデバイスからデータを収集します
**B.** 遠隔診断の実施
**C.** グローバルネットワークの動向分析
**D.** クラウドベースアプリケーションの管理
正解: **(**正解を表示します**)**
ローカル収集エージェントの目的は、同じネットワークセグメント内の近隣デバイスからデータを収集し、ローカルのトラフィックパターンを詳細に監視および分析できるようにすることです。

質問: **79**
ネットワーク保証における合成テストの主な目的は何ですか？
**A.** サーバーログの分析
**B.** ハードウェアの状態監視
**C.** ユーザーインタラクションのシミュレーション
**D.** ネットワークの脆弱性の特定
正解: **(**正解を表示します**)**
合成テストの主な目的は、アプリケーションに対するユーザーの操作をシミュレートし、ネットワーク保証におけるプロアクティブな監視とパフォーマンス最適化を可能にすることです。

質問: **80**
ネットワーク保証において、アラートの設定と機能を検証する目的は何ですか？
**A.** 規格への準拠を確保する
**B.** 競合他社とのベンチマーク
**C.** 偽陽性の特定
**D.** ネットワークパフォーマンスのテスト
正解: **C (**コメントを発表する**)**
アラートの設定と機能を検証することで、誤検知を特定し、ネットワーク保証における効率的なインシデント対応のために正確なアラートを確実に発信できるようになります。

質問: **81**
添付資料を参照してください。


ネットワークエンジニアが、従業員のエンドポイントのパフォーマンスに影響を与えることなく、SaaSアプリケーションのネットワークを監視するためにCisco ThousandEyesエージェントをデプロイしています。ブランチAからネットワークメトリックを取得するには、どのThousandEyesエージェントをデプロイする必要がありますか？

**A.** エンドポイントエージェント
**B.** アプリケーションエージェント
**C.** エンタープライズエージェント
**D.** クラウドエージェント
正解: **(**正解を表示します**)**
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）の枠組みにおいて、適切なThousandEyesエージェントタイプを選択することは、可視性の要件とインフラストラクチャの制約とのバランスを取る上で非常に重要です。ブランチAの場合、主な目的は、従業員のエンドポイントへのパフォーマンスへの影響を厳密に回避しながら、SaaSアプリケーションのネットワーク層メトリクス（遅延、パケット損失、ジッターなど）とパスの可視化を取得することです。
エンタープライズエージェント（オプションC）は、企業ネットワーク環境内部からの「インサイドアウト」監視用に設計されているため、最適な選択肢です。これらのエージェントは軽量なソフトウェアプローブであり、Dockerコンテナまたは仮想マシンを使用して、Cisco Catalyst 9300/9400スイッチやCatalyst 8000エッジプラットフォームなどの既存のネットワークインフラストラクチャに展開できます。エージェントをブランチルーターまたは専用のローカルサーバーにホストすることで、エンジニアはSaaSプロバイダーの宛先に対して合成テストを実行できます。このアプローチにより、従業員個々のワークステーション（エンドポイント）にソフトウェアをインストールしたり、リソースを消費したりすることなく、ブランチAから必要なネットワークの視点を得ることができます。
他のエージェントタイプは、このシナリオの特定の制約を満たしません。
エンドポイントエージェントは、ユーザーデバイス（Windows/macOS）に直接インストールされ、「ラストマイル」の可視性を提供します。しかし、エンドポイントのCPUとメモリを使用するため、エンドポイントのパフォーマンスに影響を与えないという要件と矛盾します。
* クラウドエージェントは、シスコが世界中のISPデータセンターで管理しています。クラウドエージェントは「外部から内部への」可視性を提供しますが、内部ブランチネットワークの特性や、ブランチAの内部ローカルエリアネットワークからの特定のパスを把握することはできません。
* アプリケーションエージェントは非標準的な用語であり、ThousandEyesアーキテクチャ内には独立したエージェントタイプとして存在しません。
したがって、支店インフラ内にエンタープライズエージェントを導入することで、ネットワークエンジニアは従業員のデバイスに一切負荷をかけることなく、高精度のネットワークメトリクスを取得できるようになります。
ThousandEyesの紹介
このビデオでは、CCNPレベルのエンタープライズネットワーク保証戦略において、ThousandEyesエージェントがどのように機能するかについて、重要な概要を説明します。

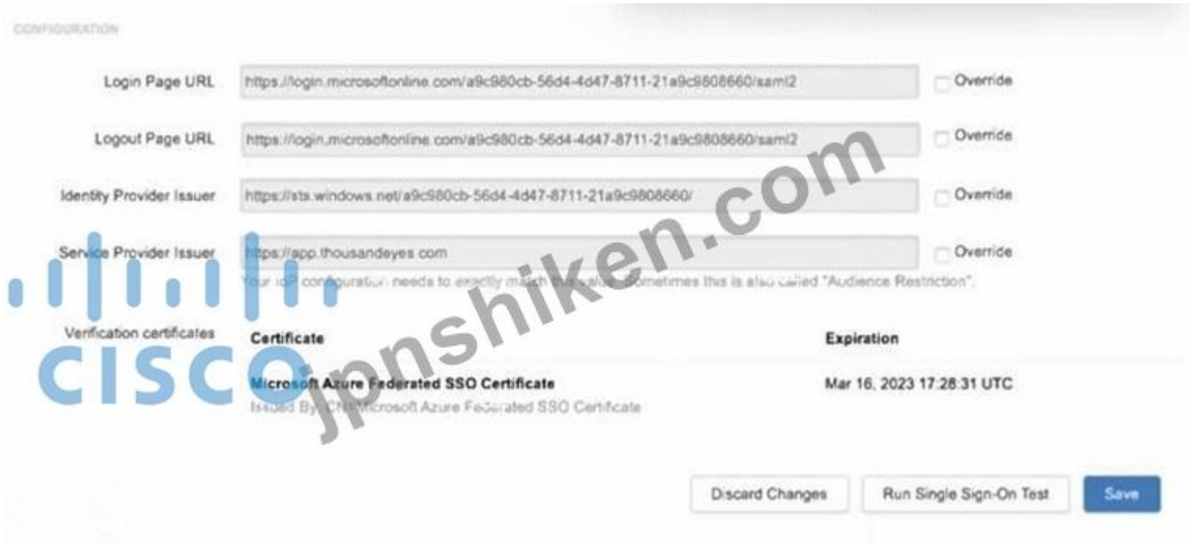
質問: **82**
ネットワークパフォーマンス監視のための指標ベースラインを設定する最初のステップは何ですか？
**A.** パフォーマンス基準値の設定
**B.** 主要業績評価指標の定義
**C.** ネットワークトラフィックの分析
**D.** 歴史データの収集
正解: **(**正解を表示します**)**
指標の基準値を設定する最初のステップは、ネットワーク保証におけるネットワークパフォーマンスを測定および監視するための主要業績評価指標（KPI）を定義することです。

質問: **83**
どの統合タイプが、シスコのテクノロジーとサードパーティのITSMプラットフォーム間でシームレスなデータ交換を可能にしますか？
**A.** SNMP
**B.** オープンテレメトリ
**C.** API
**D.** アラートしきい値
正解: **(**正解を表示します**)**
API統合により、シスコのテクノロジーとサードパーティのITSMプラットフォーム間でのシームレスなデータ交換が可能になり、ネットワーク保証における自動化と相互運用性が促進されます。

質問: **84**
社内ネットワークに接続されているすべてのエンドポイントエージェントを自動的に含むエンドポイントラベルを作成したいと考えています。エージェントの名前が 「agentname-network」という形式の場合、ホスト名フィールドにはどのようなフィルタを使用すればこれを実現できますか？
**A.** -企業
**B.** エージェント名-
**C.** エージェント*コーポレート
**D.** ワイルドカード設定は利用できません
正解: **A (**コメントを発表する**)**
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）フレームワークでは、エンドポイントエージェントの大規模な展開を管理するには、エージェントラベルによる効率的な分類が必要です。エージェントラベルは、場所、OS、命名規則などの特定の属性に基づいて、ターゲットを絞ったテストの割り当てやデータフィルタリングを行うためにエージェントをグループ化するために使用されます。ThousandEyes は、ラベルフィルタ内でワイルドカード (特に * 記号) を使用することで、動的かつスケーラブルなグループ化を可能にしています。このシナリオでは、組織は agentname-network という命名規則を採用しています。固有の agentname プレフィックスに関係なく、「corporate」ネットワークに接続されているすべてのエージェントをキャプチャするには、エンジニアはホスト名またはエージェント名のフィールドでフィルタ *-corporate (オプション A) を使用する必要があります。アスタリスクは任意の文字列のプレースホルダーとして機能し、末尾が "-corporate" のエージェントが ThousandEyes プラットフォームに登録されるとすぐにラベルに自動的に追加されるようにします。

質問: **85**
ネットワーク保証において、Webアプリケーションのテスト時に一般的に使用される認証方法はどれですか？
**A.** 基本
**B.** NTLM
**C.** SAML
**D.** OAuth
正解: **(**正解を表示します**)**
基本認証は、ネットワーク保証におけるWebアプリケーションのテストで一般的に使用されます。これは、認証のためにHTTPリクエストヘッダーにユーザー認証情報（ユーザー名とパスワード）を送信するもので、WebリソースやAPIへのアクセスにおいて、シンプルで広くサポートされている認証メカニズムを提供します。

質問: **86**
図を参照してください。エンジニアは、図に示されている構成を使用して、Cisco ThousandEyes SSOをMicrosoft Entra IDを使用するように構成する必要があります。構成を完了するには、どの機能をオーバーライドするように設定する必要がありますか？



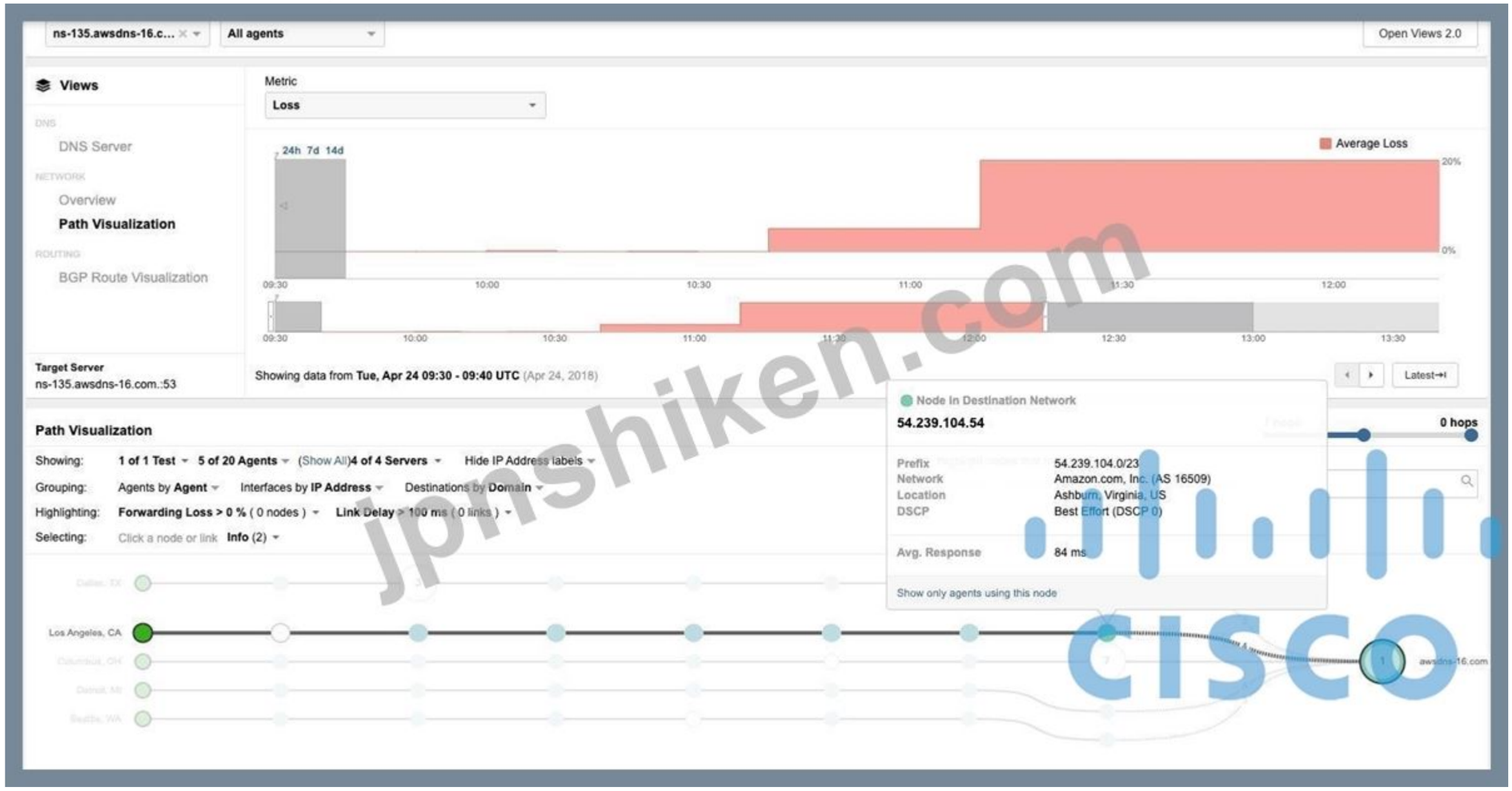


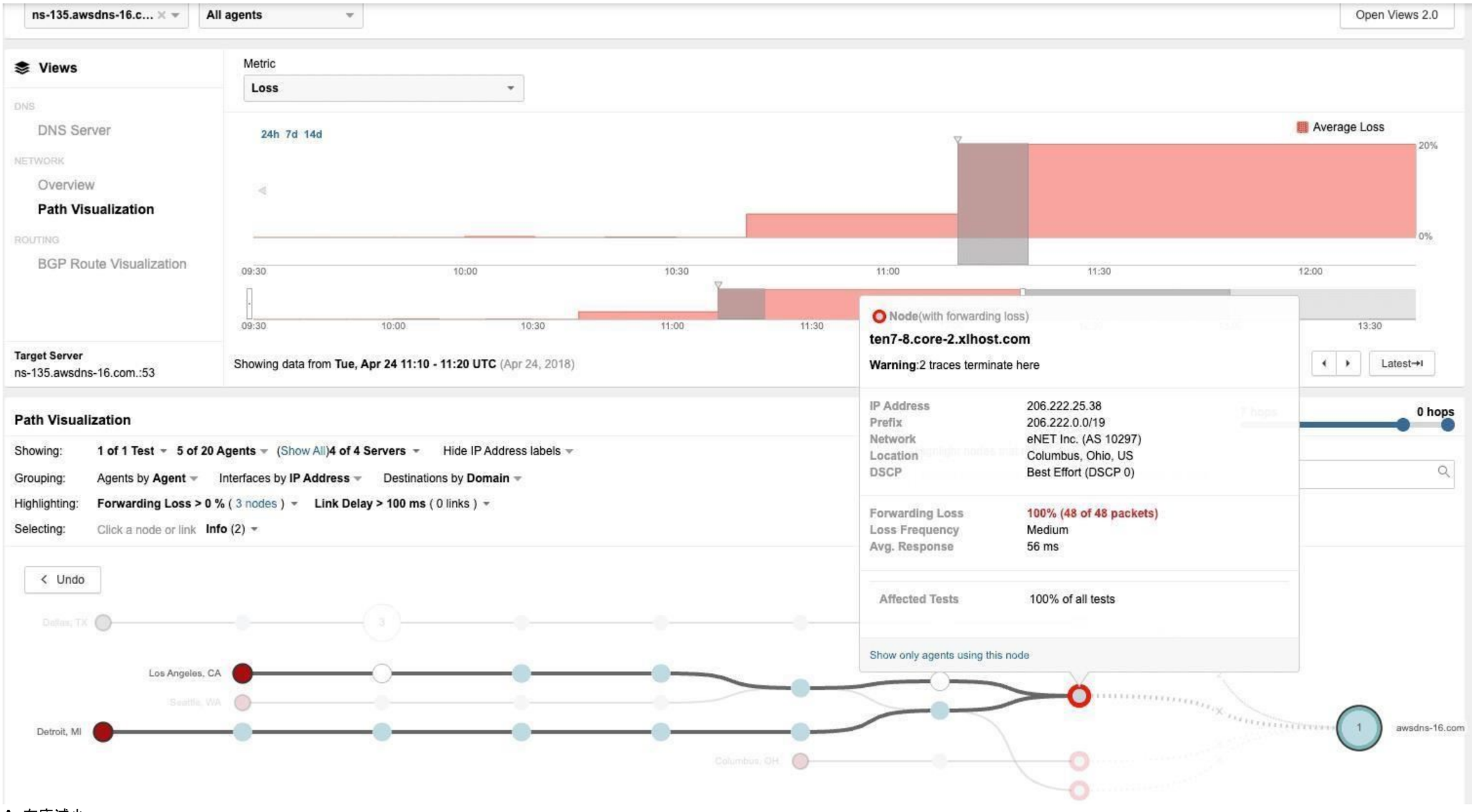
**A.** サービスプロバイダー発行者
**B.** ログアウトページのURL
**C.** ログインページURL
**D.** アイデンティティプロバイダー発行者
正解: **(**正解を表示します**)**
Cisco ThousandEyes SSOをMicrosoft Entra ID（Azure AD）と統合する場合、サービスプロバイダー発行者（エンティティIDまたはオーディエンス制限とも呼ばれる）は、ThousandEyesとEntra IDの間で完全に一致している必要があります。
この値は通常、デフォルトでは一致しないため、オーバーライドを有効にして、Azure が想定するエンティティ ID に手動で設定する必要があります。

質問: **87**
ある企業が、自社のウェブアプリケーションのパフォーマンスに断続的な低下が見られることに気づいており、それがユーザーエクスペリエンスに影響を与えている。
従業員のノートパソコンのCPU使用率が高いことが原因ではないかと疑われており、その原因はバックグラウンドプロセスにある可能性がある。この問題の原因としてエンドポイントのCPUパフォーマンスが関係しているかどうかを特定するには、ThousandEyesのアラートタイプと条件の組み合わせのうち、どれが最も効果的だろうか？
**A.** 実ユーザーテスト > ネットワークテストとパストレース、エンドツーエンドパケット損失
**B.** スケジュールされたテスト > エンドポイントパストレース、パス長 > #
**C.** リアルユーザーテスト > エンドポイント、CPU使用率 # %
**D.** スケジュール済みテスト > エンドポイントエンドツーエンド（サーバー）、メモリ負荷 # %
正解: **(**正解を表示します**)**
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）カリキュラムでは、エンドユーザーのマシンにおけるパフォーマンスの問題を特定するには、アプリケーション層のエクスペリエンスデータとローカルシステムのテレメトリを組み合わせる必要があります。アーキテクトが、CPU使用率の高さなど、ローカルハードウェアの制約がデジタルエクスペリエンスを低下させていると疑う場合、エンドポイントエージェントが最適な監視ポイントとなります。
正しい組み合わせは「リアルユーザーテスト」>「エンドポイント」、CPU使用率#%（オプションC）です。このアラート設定は、以下のいくつかの理由から効果的です。
* ターゲットを絞った可視性: ハードウェアのボトルネックが存在すると疑われるユーザーのデバイス (エンドポイント) を直接監視します。
* リアルタイムコンテキスト :リアルユーザーテスト（RUM）を利用することで、エージェントは実際のユーザーアクティビティ（Webアプリケーションの閲覧など）中にパフォーマンスデータを収集します。これにより、CPUスパイクがアクティブなアプリケーションの使用状況と相関していることが保証され、ユーザーエクスペリエンスへの影響を代表的に把握できます。

* しきい値アラート :この機能は、定義されたパーセンテージしきい値 # %）を超えるCPU使用率を監視します。これにより、アプリケーションの動作が遅くなったり、ブラウザがフリーズしたりする原因となるCPU負荷が問題のあるレベルに達した場合にのみ、ITチームに通知されます。
この特定のトラブルシューティング目標に対して、代替手段は効果が低い。
* オプションA :ネットワーク損失を監視しますが、ローカルCPUのボトルネックを特定することはできません。
* オプションB :パス長 ホップ数）を監視します。これは、ローカルハードウェアのパフォーマンスとは無関係なルーティング指標です。
* オプション D: スケジュールされたテスト中にメモリ負荷を監視します。メモリも要因の一つですが、このシナリオで特に疑われるのは CPU 使用率であり、スケジュールされたテストでは、実際のユーザーがブラウザを操作する際の負荷の影響を常に正確に捉えられるとは限りません。

質問: **88**
展示物を注意深く確認してください。どの詳細が、ネットワークの問題がBGPハイジャックによって引き起こされた可能性を示唆していますか？






**A.** 在庫減少
**B.** AS 16509 を AS 10297 に変更
**C.** HTTPサーバー応答遅延
**D.** パケット損失
正解: **B** (コメントを発表する)

エンタープライズネットワーク保証の設計と実装（300-445 ENNA）カリキュラムでは、BGPハイジャックなどのルーティング異常を特定することが、外部ネットワーク保証の重要な側面となっています。BGPハイジャックとは、自律システム（AS）が、自身が所有していないプレフィックスを不正にアナウンスし、正当な所有者宛てのトラフィックが誤った方向にルーティングされる現象です。
図3.4-1（障害発生前）と図3.4-2（障害発生中）を比較すると、ルーティングパスに明確な変化が見られます。ベースラインビュー（図3.4-1）では、ロサンゼルスエージェントからのトラフィックは宛先ネットワーク54.239.104.0/23に到達し、これはAmazon.com, Inc.（AS 16509）に正しく関連付けられています。
しかし、障害発生時（図3.4-2）には、経路可視化により、トラフィックが別のネットワークであるeNET Inc.（AS 10297）にリダイレクトされていることが示されています。この新しい場所では、トラフィックはノードten7-8.core-2.xlhost.comで100%の転送損失に遭遇します。
自律システム（AS）番号が16509から10297（オプションB）に変更されたことが、BGPハイジャックの最も具体的な指標となります。可用性の低下（オプションA）、応答の遅延（オプションC）、パケット損失（オプションD）などの症状はThousandEyesテレメトリで明確に確認できますが、これらの症状は一般的なものであり、物理的なリンク障害や輻輳など、他のさまざまな問題によっても発生する可能性があります。ASパスの変更、特にターゲットのIPプレフィックスを正当にホストしていないASへの変更は、ルーティング乗っ取りを根本原因として特定するために必要なフォレンジック証拠となります。この可視化により、ネットワーク管理者は内部トラブルシューティングを省略し、アップストリームプロバイダとの外部修復に直ちに集中できます。

質問: **89**
WindowsユーザーIT向けにThousandEyesエンドポイントエージェントを拡張性、セキュリティ、かつ影響を最小限に抑えて展開するには、どの戦略が最も効果的でしょうか？
**A.** 各デバイスにエンドポイントエージェントを手動でインストールします
**B.** サイレントインストールをサポートする集中型ソフトウェア展開ツール（GPO、Intuneなど）を使用してエンドポイントエージェントを展開します。
**C.** 従業員にエンドポイントエージェントのダウンロードリンクをメールで送信し、各自のデバイスにインストールするよう依頼する。
**D.** 従業員がログインしてエンドポイントエージェントをダウンロードできるWebポータルを提供する
正解: **B** (コメントを発表する)
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）のベストプラクティスによると、エンドポイント保証の展開を成功させる目標は、ITスタッフとエンドユーザー双方の負担を最小限に抑えつつ、カバレッジを最大化することです。これを実現するための最も効果的な戦略は、サイレントインストールをサポートする集中型ソフトウェア展開ツール（GPO、Intuneなど）を使用することです（オプションB）。
集中型展開ツールを使用すると、管理者は単一の管理コンソールから ThousandEyes Endpoint Agent を数千台のマシンに同時にプッシュできます。サイレントインストールパラメータ (MSI パッケージの /quiet または /qn など) を使用すると、エージェントはユーザーの操作やセットアップウィザードの表示を必要とせずにバックグラウンドでインストールされます。
「最小限の混乱」アプローチにより、業務運営の中断を防ぎます。
さらに、集中管理ツールは「安全な」導入方法を提供します。なぜなら、ITチームはインストールされるエージェントのバージョンを管理し、エージェントがThousandEyesダッシュボードに登録するために必要なアカウントグループトークンが正しく埋め込まれていることを確認できるからです。

質問: **90**
エンジニアは、APIを監視するために認証設定を必要とするテストを作成する必要がある。
テストでは、トークンを取得するために、クライアント認証情報パラメータを含むPOSTリクエストを送信する必要があります。取得したトークンは、リソースを取得する権限を得るために、GETリクエストで送信する必要があります。要件を満たすには、何をする必要がありますか？（2つ選択してください）




**A.** HTTPサーバーテストでクライアント認証情報に基本認証を使用するように設定します。
**B.** HTTPサーバーテストで、クライアント認証情報にNTLM認証を使用するように設定します。
**C.** HTTPサーバーテストでクライアント認証情報にOAuth認証を使用するように設定します。
**D.** パラメータはHTTPサーバーのOAuth認証ではサポートされていません。代わりにトランザクションスクリプトを使用してください。
**E.** パラメータはHTTPサーバーのOAuth認証ではサポートされていません。代わりにAPIテストを使用してください。
正解: **(**正解を表示します**)**
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）カリキュラムでは、最新のAPIを監視するには、特定のクライアント認証情報パラメータを使用したOAuth 2.0などの複雑な認証フローを処理する必要があることがよくあります。提供されている図は、標準的なHTTPサーバーテストで使用できるHTTP認証オプション（なし、基本認証、NTLM、Kerberos、OAuth）を示しています。
ENNA実装標準によると、HTTPサーバーテストタイプはOAuth（オプションC）をサポートしていますが、そのネイティブ実装には制限があります。具体的には、既存のトークンまたは単純なトークン更新フローを使用するように設計されており、多くのエンタープライズクライアント認証シナリオでトークンを取得するために必要な最初のPOSTリクエストへのカスタムパラメータの挿入はサポートしていません。BasicおよびNTLM（オプションAおよびB）は、単純なユーザー名/パスワードヘッダーに依存するレガシープロトコルであり、前述の複数ステップのトークン交換プロセスを容易にすることはできません。
2段階フロー（トークン取得のためのPOST、続いてリソース取得のためのGET）の要件を満たすには、エンジニアはより柔軟なテストタイプを使用する必要があります。
トランザクションスクリプト（オプションD） これにより、エンジニアはThousandEyesトランザクションライブラリを使用してカスタムJavaScriptを記述し、POSTリクエストをプログラムで処理し、結果として得られるJSONトークンを解析し、そのトークンを後続のGETリクエストのヘッダーに渡すことができます。

APIテスト オプションE） これらはAPI監視専用に設計されており、変数の定義や、ある呼び出しの出力（トークン）が次の呼び出しの入力となる複数ステップのリクエストをネイティブにサポートしています。これらの高度なテストタイプを活用することで、エンジニアは標準的なHTTPサーバーテストでは対応できない複雑な認証要件にも適切に対処できます。

質問: **91**
図を参照してください。ネットワークエンジニアは、HTTPサーバーがサーバーエラーを返した場合にトリガーされるアラートを設定するよう指示されています。指定された要件を満たすには、どのようなアラート条件を設定すべきでしょうか？

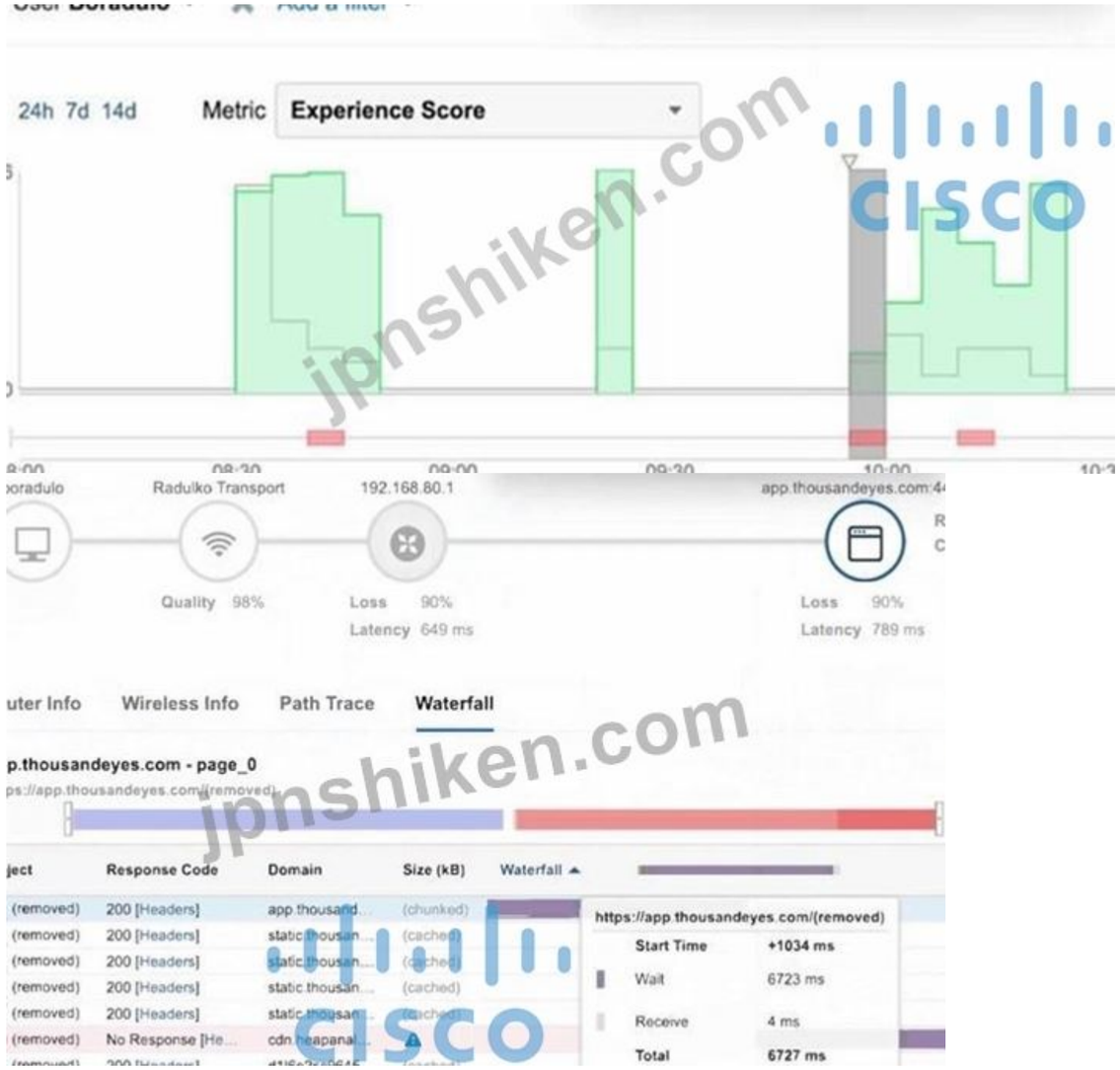

**A.** エラータイプは任意です
**B.** 待機時間は動的（新機能）感度は中程度
**C.** 応答時間 ≥ 静的500ms
**D.** 応答コードはサーバーエラー（5XX）です
正解: **(**正解を表示します**)**
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）フレームワークでは、標準的なネットワークノイズと対応が必要なアプリケーション層の障害を区別するために、効果的なアラートルールを設定することが重要です。Web - HTTPサーバーのテストでは、ThousandEyesを使用することで、エンジニアはネットワークレベルのメトリック（接続時間など）とアプリケーションレベルの指標（HTTP応答コードなど）の両方を監視できます。
要件は、HTTP サーバーがサーバー エラーで応答したときにアラートをトリガーすることです。HTTP プロトコルでは、サーバー エラーは 5XX シリーズのステータス コード (例:

500 内部サーバーエラー、503 サービス利用不可、504 ゲートウェイタイムアウト）。この要件を満たすには、エンジニアは、メトリックがレスポンスコードに設定され、条件値がサーバーエラー(5XX)であるロケーションアラート条件を構成する必要があります(オプション D)。



質問: **92**
エンジニアは、ユーザーがOneDriveにログインしてファイルをダウンロードするワークフローを実行するテストを作成する必要があります。このテストには再試行メカニズムを実装する必要があります。エンジニアはスクリプト作成の経験が限られています。
エンジニアはどのような行動を取る必要があるのか？
**A.** Office365 > OneDrive - ファイルのダウンロードテンプレートからスクリプトを作成します
**B.** ThousandEyes Recorder IDEをインストールし、ユーザーフローを記録します。
**C.** サンプルスクリプトについては、トランザクションスクリプトの例リポジトリを確認してください。
**D.** 上記のすべて
正解: **D (**コメントを発表する**)**
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）カリキュラムでは、トランザクション監視は、複雑な複数ステップのユーザーワークフローを検証するために不可欠です。スクリプト作成の経験が限られているエンジニアがOneDriveのファイルダウンロードプロセスを監視する必要がある場合、ThousandEyesエコシステムは、堅牢なトランザクションテストの作成を簡素化する複数のツールを提供します。
正しいアプローチは、利用可能なすべてのリソースを活用することであり、オプションDが決定的な答えとなります。まず、ThousandEyes Recorder IDE（オプションB）は、スクリプト作成の知識がないエンジニアにとって重要なツールです。このツールを使用すると、エンジニアはローカルマシンのブラウザ環境で、OneDriveへのアクセス、ログイン、ダウンロードの開始といった実際のワークフローを実行でき、同時にツールがすべてのクリックとキーボード入力を記録します。Recorderは、ThousandEyesトランザクションライブラリを使用して、対応するJavaScriptコードを自動的に生成します。
第二に、このプラットフォームは、Office 365やOneDriveなどの事前構築済みスクリプトテンプレート（オプションA）を提供します。
これには、これらの特定のサービスに関する基本ロジックとベストプラクティスが含まれます。3つ目は、GitHub の officialtransaction-scripting-examplesrepository (オプション C) が、コードスニペットのメンテナンスされたソースであることです。これは、一時的なネットワーク障害によってテストが「失敗」を報告せず、アラートをトリガーする前にアクションを再試行することを保証する再試行メカニズムなどの高度なロジックを実装するのに特に役立ちます。
提供された図に示すように、一般的なスクリプトでは、@thousandeyes と selenium-webdriver のインポート文を使用してブラウザを制御します。基本的なフローにはレコーダー、サービス固有のニュアンスにはテンプレート、再試行などのロジック強化にはサンプルスクリプトを組み合わせることで、エンジニアは高度なコーディングスキルがなくても、非常に信頼性の高い保証テストを展開できます。したがって、これら 3 つのアクションはすべて、ENNA 実装フレームワーク内で強く推奨され、有効です。

質問: **93**
図を参照してください。在宅勤務中の従業員から、アプリケーションのパフォーマンスが時々低下するという報告がありました。NOCオペレーターはCisco ThousandEyesを開き、従業員のEndpoint Agentのパフォーマンスメトリックを調査します。問題は何でしょうか？




**A.** Wi-Fi信号強度が低い
**B.** ISPネットワークの問題
**C.** ユーザーのルーターで帯域幅を過剰に使用しています
**D.** アプリケーションサーバーのパフォーマンスが低い
正解: **(**正解を表示します**)**
エンドポイントエージェントのビューでは、従業員とISPゲートウェイ間のパケット損失率が非常に高く（約90%）、レイテンシも非常に高い（約650〜780ミリ秒）ことが示されています。
ユーザーのWi-Fi接続品質は良好（約98%）であり、トラフィックがアプリケーションサーバーに到達すると、正常に応答します。
これは、パフォーマンスの低下がWi-Fi、ユーザーのルーター、またはアプリケーションサーバーではなく、ISPネットワーク経路で発生していることを裏付けています。

質問: **94**
IT運用ダッシュボードを分析した結果、どのエージェントのHTTP接続時間が優れているか？
**A.** カリフォルニア州サンノゼ (AT&T)

**B.** メキシコ、メキシコシティ（テルメックス）
正解: **B** (コメントを発表する)
IT運用ダッシュボードでは、エージェントごとにパフォーマンス指標が表示され、詳細なトラブルシューティングが容易になります。最新の指標テーブルを確認すると、メキシコシティ（TelMex）エージェントの接続時間は0.51ミリ秒で、サンノゼ（カリフォルニア州）エージェントの対応する時間よりも大幅に短く（つまり「優れている」）ことがわかります。接続時間はTCPの3ウェイハンドシェイクにかかる時間を測定するもので、値が小さいほどネットワーク層の確立が速いことを示します。

質問: **95**
受動監視が能動監視に比べて持つ主な利点は何ですか？
**A.** パッシブモニタリングは、合成条件下でのネットワークのパフォーマンスを測定できます。
**B.** 受動監視は、ネットワークにトラフィックを追加することなく、ネットワークパフォーマンスに関するリアルタイムデータを提供することができます。4
**C.** パッシブモニタリングでは、テストトラフィックを生成してユーザーの行動をシミュレートできます。
**D.** パッシブモニタリングは、特定のネットワークサービスやプロトコルのパフォーマンスを直接測定できます。
正解: **B** (コメントを発表する)
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）アーキテクチャにおいて、重要な設計上の考慮事項は、監視ソリューションが本番環境に与える影響です。パッシブ監視（オプションB）の主な利点は、非侵襲性であることです。データプレーンに余分な「合成」オーバーヘッドを挿入することなく、ネットワークパフォーマンスとトラフィック構成に関する洞察を提供します。
Cisco Meraki Insight (MI)、NetFlow、SNMPなどのパッシブな手法は、既存のユーザートラフィックまたはデバイス自身の制御プレーンによって生成されるテレメトリに依存しています。たとえば、Meraki Insightは、個別のプローブを送信するのではなく、Meraki MXアプライアンスを自然に通過するHTTP/Sフローを分析してアプリケーションのパフォーマンススコアを導き出します。5これにより、監視ツール自体が帯域幅を消費したり、ネットワークの輻輳を引き起こしたりすることがなくなります。これは、帯域幅が制限されているブランチ環境や利用率の高いリンクでは特に重要です。
対照的に、アクティブモニタリング（オプションAとC）では、意図的に合成トラフィックを生成する必要があり、トラフィック量が多すぎる場合やネットワークが既に容量に達している場合は、結果が歪む可能性があります。アクティブモニタリングは、プロアクティブなトラブルシューティング（ユーザーからの苦情が出る前にパフォーマンスを測定する）に不可欠ですが、パッシブモニタリングは、実際のネットワーク上で何が起こっているかを捉えるため、実際のユーザーエクスペリエンスとインフラストラクチャ利用状況の長期的な履歴分析には最適な方法です。オプションDは両方のタイプに共通する機能です。どちらのタイプも特定のサービスを測定できますが、ネットワーク負荷に対して透過性を保ちながら測定できるのはパッシブモニタリングのみです。したがって、トラフィックを追加しないことが、パッシブアプローチの決定的な利点となります。

質問: **96**
ウェブアプリケーションとの合成的なユーザーインタラクションを実行する役割を担うエージェントの種類は何ですか？
**A.** 合成ウアー剤
**B.** 現地集金代行業者
**C.** スクリプトエージェント
**D.** クラウド統合エージェント
**E.** 仮想化エージェント
**F.** リモート管理エージェント
正解: (正解を表示します)
合成ユーザーエージェントとスクリプトエージェントは、ネットワーク保証におけるWebアプリケーションとの合成ユーザーインタラクションを実行し、パフォーマンス監視とテストを容易にする役割を担います。

質問: **97**
エンジニアがeBGPピアとのネットワーク輻輳問題を調査しています。外部ネットワークの輻輳が激しい場合、影響を受けるメトリックはどれですか？（2つ選択してください。）
**A.** BGP到達可能性
**B.** パケット損失

**C.** レイテンシー
**D.** HTTPの可用性
**E.** BGP収束時間
正解: (正解を表示します)
外部ネットワークの混雑が激しい場合、キューが蓄積されパケットがドロップされるため、主にパケット損失と遅延に影響が出ます。これらの指標は混雑状況を直接反映しますが、BGPの到達可能性と収束性は、セッション自体が失敗しない限り影響を受けません。

質問: **98**
ThousandEyesエンドポイントエージェントを使用してMicrosoft Teamsを監視したい場合、このタイプのアプリケーション監視で利用できるテストにはどのようなものがありますか？
**A.** 予定されているテスト
**B.** 動的テスト
**C.** スケジュールされたテスト、動的なテスト、および実際のユーザーテスト
**D.** 定期テストと動的テスト
正解: (正解を表示します)
コラボレーション監視に関する「エンタープライズネットワーク保証の設計と実装（300-445 ENNA）」のベストプラクティスによると、Microsoft Teams（WebexおよびZoomも含む）は、スケジュールされたテストと動的テストの組み合わせを使用して監視されます（オプションD）。

質問: **99**
ThousandEyesは、アラートによってトリガーされるイベント通知を即座に受信するための、複数のネイティブ統合機能を提供しています。
ThousandEyesプラットフォーム内で直接利用できる統合機能はどれですか？該当するものをすべて選択してください。
**A.** ServiceNow
**B.** PagerDuty
**C.** MS Teams
**D.** Splunk
**E.** AWS
**F.** AppDynamics
**G.** Webex
**H.** スラック
正解: (正解を表示します)
エンタープライズネットワーク保証の設計と実装（ENNA 300-445）のアーキテクチャによると、ThousandEyesはアラート通知専用に設計された、すぐに使えるネイティブな統合機能群を提供します。これらの統合機能は、[管理] > [統合]または[アラートルール] > [通知]タブで設定でき、プラットフォームがさまざまなコラボレーションツール、IT運用ツール、および監視ツールにイベントデータを即座に送信できるようにします。
検証済みのネイティブ通知統合リストは以下のとおりです。
* ServiceNow (A):インシデント管理とチケット発行ワークフローの自動化を容易にします。
* PagerDuty (B): ThousandEyes アラートに基づいて、インシデントの自動エスカレーションとオンコールルーティングを可能にします。
* MS Teams (C) および Slack (H): アラートの詳細とパーマリンクをチームコラボレーション用の指定されたチャネルに直接プッシュすることで、リアルタイムのチャットオペレーションを実現します。
* Splunk (D): Cisco ThousandEyes App for Splunk を利用してアラートデータを取り込み、SIEM またはログ記録プラットフォーム内で履歴分析と相関分析を行います。
* AppDynamics (F): アラート通知をAppDynamicsインスタンスに直接送信し、アプリケーション所有者がネットワークの問題とAPMメトリクスを関連付けることができるようにします。12
* Webex (G): Webex Control Hub および特定の Webex スペースと統合して、コラボレーション パフォーマンスの統一された可視性を提供します。34 AWS (オプション E) は、このコンテキストではネイティブのアラート通知先ではありません。代わりに、ThousandEyes は、チャットや ITSM ツールなどのイベント通知の受信器として機能するのではなく、「Cloud Insights」（VPC フロー ログの取り込み）および「テスト

推奨事項」のために AWS と統合します。これらのネイティブ統合を利用することで、エンタープライズ チームは、パフォーマンスのしきい値を超えた瞬間に適切なステークホルダーが希望するコミュニケーション チャネルを通じて通知されるようにし、組織全体の応答時間を大幅に改善します。

質問: **100**
セキュリティ上の目的でネットワークエージェントの設置場所を決定する際に考慮すべき重要な要素は何ですか？
**A.** 重要インフラへの近接性
**B.** 会議室の空き状況
**C.** 自然光へのアクセス
**D.** 従業員のワークステーションからの距離
正解: (正解を表示します)
重要インフラの近くにネットワークエージェントを配置することで、セキュリティ監視と脅威検出能力が強化されます。

質問: **101**
展示資料を参照してください。


このネットワークエージェントからサーバーへのテストにおいて、テストトラフィックがファイアウォールによって悪意のあるものとして検出されないようにするには、どの設定を有効にする必要がありますか？
**A.** パストレースモード: セッション中
**B.** プロトコル: TCP
**C.** ポート: 5000
**D.** プローブモード: 強制SYN
正解: (正解を表示します)

エンタープライズネットワーク保証の設計と実装（300-445 ENNA）アーキテクチャにおいて、アクティブな合成監視における重要な課題は、テストプローブが中間セキュリティアプライアンスによって破棄されることなく、ユーザーのトラフィックを正確に反映するようにすることです。標準的なネットワークテストでは、パフォーマンスメトリック（遅延/損失）の測定とパス検出（ホップバイホップの可視化）に別々の接続を使用することがよくあります。この動作は、ステートフルファイアウォールや侵入防御システム（IPS）によって、疑わしいまたは悪意のあるスキャン活動としてフラグ付けされる可能性があります。
これを軽減するには、エンジニアは「パス トレース モード: セッション内 (オプション A)」を有効にする必要があります。このモードが有効になっている場合、ThousandEyes はパフォーマンス測定用に確立されたまったく同じ TCP セッションを使用してパス検出を実行します。アクティブな確立済みセッション内にパス検出プローブを埋め込むことで、トラフィックはファイアウォールに対して、TTL 値が異なる独立した一連のプローブではなく、正当な継続的な通信ストリームの一部として認識され、「なりすまし対策」や「スキャン」アラートがトリガーされるのを防ぎます。
代替案の検討：
* プロトコル：TCP（オプションB）：一般的にTCPはICMPよりもファイアウォールに優しいですが、図では既にTCPが選択されています。問題はプロトコル自体ではなく、セッションに対するパス検出プローブの処理方法です。
* ポート: 5000 (オプション C): ポートを 5000 のような非標準の値に変更すると、80 のような標準の Web ポートと比較して、デフォルトのファイアウォール ポリシーによってトラフィックが監視またはブロックされる可能性が高くなります。
* プロービング モード: SYN を強制 (オプション D): SYN パケットを強制することは、特定のタイプのロード バランサーをバイパスするために使用される手法ですが、パス ディスカバリ プローブがステートフル インスペクション エンジンによって別の悪意のあるスキャンと見なされるという根本的な問題には対処していません。
したがって、セッションパスのトレースモードを有効にすることは、セキュリティが強化された環境全体で一貫した可視性を確保するための最も効果的な方法です。

質問: **102**
Thousand Eyesのどのテストが、DNS解決のパフォーマンスを評価するために特別に設計されていますか？
**A.** 音声テスト
**B.** ウェブテスト
**C.** DNSテスト
**D.** ネットワークテスト
正解: (正解を表示します)
Thousand EyesのDNSテストは、DNS解決のパフォーマンスを評価し、ネットワーク保証における遅延や応答時間の問題を特定するために特別に設計されています。

質問: **103**
図を参照してください。ユーザーパフォーマンスの低下を引き起こしている損失はどこにありますか？


**A.** ISPエッジ
**B.** デフォルトゲートウェイ
**C.** 宛先ネットワーク
**D.** ワイヤレス接続
正解: (正解を表示します)
経路可視化により、ユーザーのデフォルトゲートウェイである192.168.1.1ノードで95%以上の転送損失が発生していることが強調されています。
上流ノードではすべて損失が見られず、パフォーマンスの問題はゲートウェイに起因していることが確認されました。

質問: **104**
重要なネットワークリンクにおけるインターフェース利用率の基準値を確立するためにデータを収集する期間を選択する際に、重要な考慮事項は何ですか？
**A.** ネットワークトラフィック量が最も少ない時間帯を選択します。
**B.** 期間が組織の会計年度と一致していることを確認する。
**C.** ピーク時とオフピーク時の両方の交通パターンを捉え、代表的なビューを作成します。
**D.** 分析する必要のあるデータ量を最小限に抑えるために、期間を制限する。
正解: **(**正解を表示します**)**
正確なベースラインを設定することは、エンタープライズネットワーク保証の設計と実装（300-445 ENNA）手法の要です。ベースラインは、異常検出や容量計画に役立つよう、ネットワークの標準的な運用サイクル全体における「典型的な」動作を表す必要があります。重要なリンク上のインターフェース使用率を監視する場合、ピーク時とオフピーク時の両方のトラフィックパターンを把握することが不可欠です（オプションC）。
ほとんどの企業ネットワークは、日周期と呼ばれる周期的なトラフィックパターンを示します。これは、業務時間中（ピーク時）に利用率が急上昇し、夜間や週末（オフピーク時）には大幅に低下するというものです。エンジニアがトラフィック量の最も少ない時間帯（オプションA）のみでデータを収集した場合、ベースラインが非現実的に低くなり、通常の業務トラフィックが戻った際に「誤検知」アラートが発生する可能性があります。逆に、ピーク時のデータのみを収集すると、オフピーク時に発生するバックグラウンド同期タスクやバックアップウィンドウが隠されてしまう可能性があります。
エンジニアは、代表的な期間（通常は1週間または1か月）を選択することで、月曜朝の「ログオン集中」、週半ばの安定状態、週末のメンテナンスなどの変動を考慮したベースラインを確保します。この包括的なビューにより、保証プラットフォーム（Cisco Catalyst CenterやThousandEyesなど）は標準偏差を計算し、動的なしきい値を設定できます。利用率がこれらの過去の代表的な基準から逸脱した場合、システムは予測可能な日々の急増ではなく、真の異常に基づいてアラートをトリガーできます。会計年度に合わせる（オプションB）ことは技術的なパフォーマンスとは無関係であり、データを制限する（オプションD）とベースラインの統計的妥当性が損なわれます。

質問: **105**
MPLSネットワーク監視のアラートによく含まれる指標は何ですか？
**A.** CPU温度
**B.** VPNトンネルの状態
**C.** ネットワークスループット
**D.** サーバー稼働時間
正解: **(**正解を表示します**)**
VPNトンネルの状態は、潜在的なVPN接続の障害や中断を検出し、MPLSネットワーク全体で信頼性の高いデータ伝送を確保するために、MPLSネットワーク監視のアラートによく含まれています。

質問: **106**
Room OSデバイスにエンドポイントエージェントをデプロイすることが最も有益なシナリオはどれでしょうか？
**A.** リアルタイムストリーミングの問題を診断する
**B.** DNSサーバーのパフォーマンス評価
**C.** WANパフォーマンスの監視
**D.** Webアプリケーションのパフォーマンス分析
正解: **A (**コメントを発表する**)**
Room OSデバイスにエンドポイントエージェントを導入することは、リアルタイムストリーミングの問題を診断する上で最も有益であり、包括的な監視とトラブルシューティングを可能にする。

質問: **107**
Ciscoのネットワーク保証プラットフォームを選択する際、アプリケーション間の通信に関して優先すべき点は何ですか？
**A.** 拡張性
**B.** サーバーハードウェア
**C.** ユーザーエクスペリエンス
**D.** ネットワークスループット
正解: **(**正解を表示します**)**
アプリケーション間の通信においては、ネットワーク保証における最適なパフォーマンスと使いやすさを確保するために、Ciscoのネットワーク保証プラットフォームを選択する際に、ユーザーエクスペリエンスを最優先に考慮する必要があります。

質問: **108**
エンドユーザーデバイスのCPU使用率を監視するために、どのようなアラートルール構成が使用されますか？
**A.** 過去のデータ分析
**B.** しきい値に基づくアラート
**C.** 異常検知
**D.** リアルタイム交通分析
正解: **(**正解を表示します**)**
しきい値ベースのアラートは、エンドユーザーデバイスのCPU使用率を監視するために使用されます。CPU使用率が事前に定義されたしきい値を超えた場合にアラート通知がトリガーされ、潜在的なパフォーマンスの問題を示します。

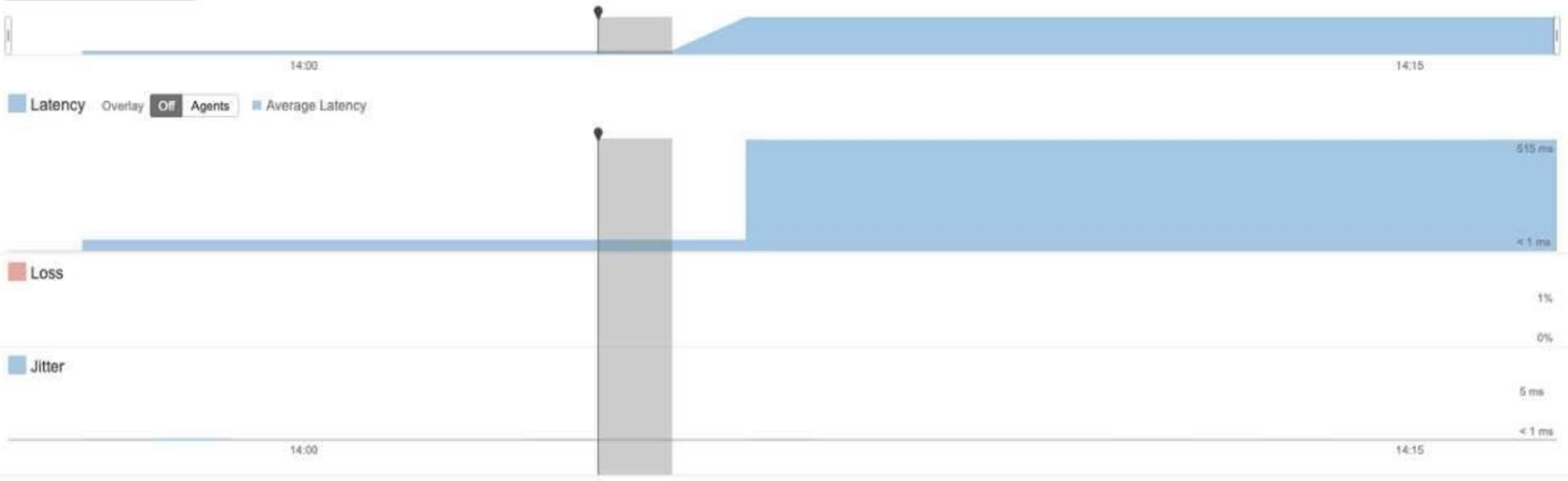
質問: **109**
遠隔地の企業拠点（図表ではs30と表記）のユーザーが、データセンターでホストされている重要なエンタープライズアプリケーションに問題が発生しています。この拠点はMPLSネットワークを介して本社キャンパスに接続されています。

Reachability to MPLS Hub | 10.87.13.11 ICMP | Agents: **s30-te-rhel33** × | Servers: **All** | Reset | Open Views 1.0 | Submit Feedback

Agent to Server | Network

Metrics: **Latency + 2**

Tue, May 7 14:04 – 14:05 GMT+10 (1 hour ago) < > >| 24h 7d 14d




Path Visualization | Map | Table

Show 1 of 1 agents | IP Address Labels

Group Agents by Agent | Interfaces by IP Address | Destinations by No Grouping

Highlight All | Search Network, Country, IP Address, Prefix or Title

Select Click a node or link | Info (1)

1 hop 1 hop

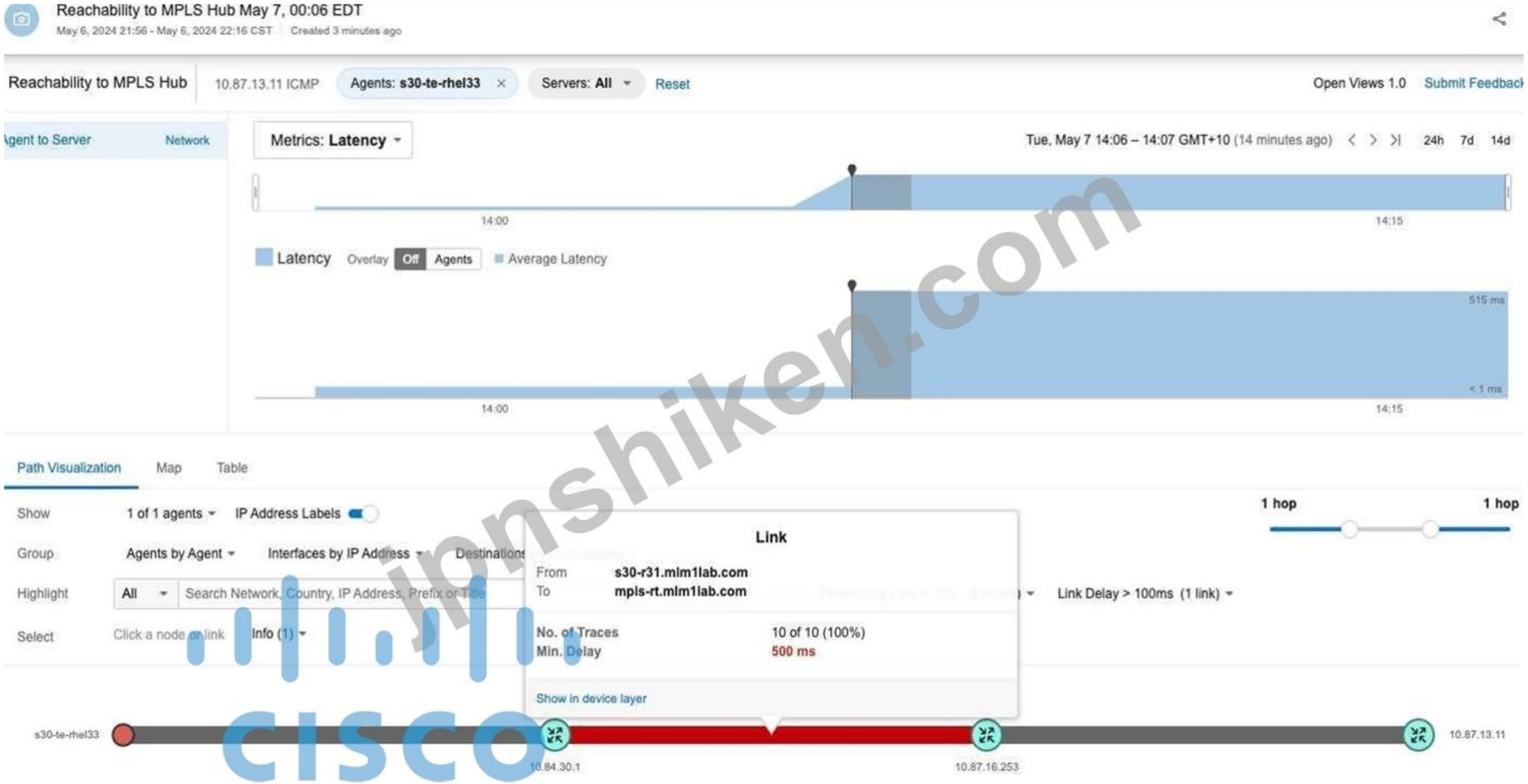
oss > 10% (0 nodes) | Link Delay > 100ms (0 links)

**Link**

From **s30-r31.mlm1lab.com**
To **mpls-rt.mlm1lab.com**

| | |
|---|---|
| No. of Traces | 10 of 10 (100%) |
| Min. Delay | 40 ms |

Show in device layer




以下の図は、問題発生前後のネットワークの状態を示しています。提示された情報に基づき、問題の最も可能性の高い原因は何ですか？また、ネットワーク運用エンジニアとして、次にどのような対策を講じますか？

**A.** 伝送メディアチームにエスカレーションし、10.84.30.1 と光ファイバー間の接続を確保します。
10.87.16.53 を確認しました。

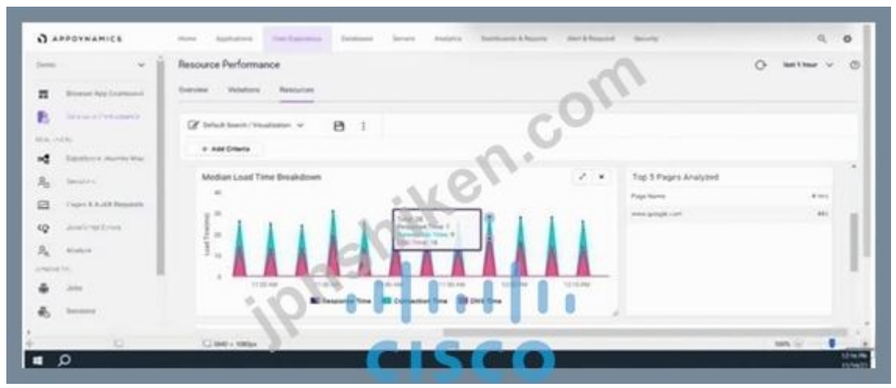
**B.** MPLSネットワーク機器のルーティングテーブルに最近変更がないか確認してください。

**C.** このサイトの帯域幅使用状況を確認してください。

**D.** エンタープライズアプリケーションを所有するチームに連絡を取り、サーバーのレビューを依頼してください。

正解: (正解を表示します)

質問: **110**
図を参照してください。エンジニアは、Cisco AppDynamics を使用してアプリケーションのパフォーマンスの問題をトラブルシューティングする必要があります。アプリケーション接続で発生した問題はどれですか？




**A.** 11月14日午前11時41分におけるDNS応答時間は18ミリ秒でした。
**B.** 10月14日午前11時56分の応答時間は443ミリ秒でした。
**C.** 11月14日午前11時41分の接続時間は9msでした。
**D.** 11月14日午前11時56分にロード時間は28ミリ秒でした。
正解: **C** (コメントを発表する)
グラフのツールチップには、選択したタイムスタンプ（11月14日午前11時41分）の正確な指標が表示されます。
接続時間は9ミリ秒と表示されます。これは、トラブルシューティング中に観測された接続関連の指標を直接的に示しています。

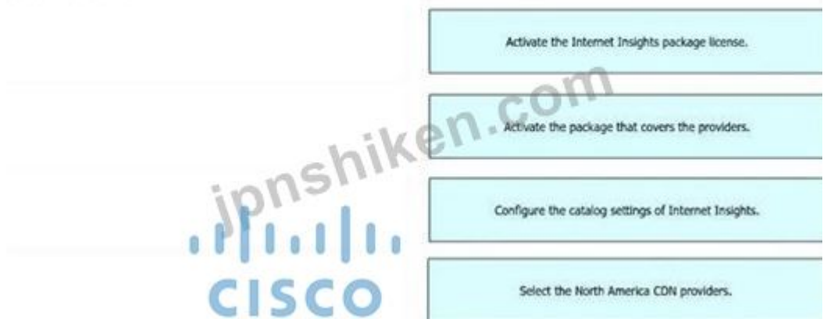
質問: **111**
ドラッグアンドドロップ問題
Cisco ThousandEyesで北米コンテンツ配信ネットワーク（CDN）プロバイダー向けのインターネットインサイトを有効にするには、左側の手順を右側の順序にドラッグアンドドロップしてください。

**Answer Area**

| | |
|---|---|
| Configure the catalog settings of Internet Insights. | Step 1 |
| Activate the package that covers the providers. | Step 2 |
| Select the North America CDN providers. | Step 3 |
| Activate the Internet Insights package license. | Step 4 |

正解:

**Answer Area**




Explanation:
まず、Internet Insightsのライセンスを有効にしてから、適切なパッケージ（例CDN/ネットワーク障害）をアクティブ化する必要があります。
その後、カタログ設定を構成し、最後に監視対象となる特定の地域別CDNプロバイダーを選択します。

質問: **112**
図を参照してください。ThousandEyesとGrafanaの間で、どのタイプの統合を設定すべきでしょうか？

```
curl -i -XPOST https://api.thousandeyes.com/v7/stream \
-H "Content-Type: application/json" \
-H "Authorization: Bearer $BEARER_TOKEN" -d '{
"type": "",
"tagMatch": [
{
"key": "TestKey",
"value": "TestValue",
"objectType": "test"
}
],
"streamEndpointUrl": "https://example.org",
"customHeaders" : {
"test": "value"
}
}'
```

**A.** opentelemetry
**B.** カスタムウェブフック
**C.** プッシュAPI
**D.** poll-api
正解: **C** (コメントを発表する)
この例は、テストメトリクスを外部システムにプッシュするために使用される ThousandEyes Streaming (Push) API である /v7/stream に送信される POST リクエストを示しています。
GrafanaとThousandEyesの連携では、ダッシュボード用のデータを継続的に受信するために、このプッシュAPIが利用されます。

質問: **113**
図を参照してください。河川ではどのような問題が発生しましたか？


**A.** 11月8日のエージェント -サーバー間のテストでは、パケット損失率が1%でした。

**B.** 11月4日、ウェブサーバーは利用可能な帯域幅の95.6%を使用していました。

**C.** 11月7日のエージェント -サーバー間のテストでは、パケット損失率が1%でした。

**D.** 11月7日、ウェブサーバーは利用可能な帯域幅の95.6%を使用していました。

正解: (正解を表示します)

ストリーム内のツールチップには、選択した時点の値が表示されます。

- 可用性 :100%

損失 :1%

帯域幅利用率 :95.6%

タイムラインで強調表示されている部分は、11月4日や11月ではなく、11月7日に対応しています。

8. したがって、11月7日に観測された問題は1%のパケット損失です。

質問: **114**

Ciscoテクノロジーとサードパーティプラットフォーム間でのシームレスなデータ交換を促進する統合タイプはどれですか？

**A.** FTP

**B.** CLI

**C.** SNMP

**D.** REST API

正解: (正解を表示します)

REST APIの統合により、シスコのテクノロジーとサードパーティのプラットフォーム間でのシームレスなデータ交換が可能になり、相互運用性とデータに基づいた意思決定が実現します。

質問: **115**

ネットワーク保証において、アラートしきい値を選択することの意義は何ですか？

**A.** セキュリティ脆弱性の特定

**B.** 事前定義された条件に基づいてアラートをトリガーする

**C.** リアルタイム交通状況の監視

**D.** 自動レポートの生成

正解: (正解を表示します)

ネットワーク保証においてアラートのしきい値を選択することで、事前に定義された条件に基づいてアラートをトリガーすることができ、ネットワークの問題をタイムリーに検出して対応することが可能になります。

質問: **116**
あなたは、基本認証を使用するWebアプリケーションを対象としたThousandEyesトランザクションテストで断続的に発生する障害を調査しています。この障害は、異なるエージェントや時間帯でランダムに発生します。この問題を解決するために、どのような手順を踏みますか？（該当するものをすべて選択してください）
**A.** 問題を切り分けるために、テスト構成で基本認証を無効にします。
**B.** 異なる場所からアプリケーションに手動でログインして、認証情報の正当性を確認します。
**C.** ThousandEyesのウォーターフォールチャートとHTTPレスポンスコードを分析し、潜在的なボトルネックやエラーを特定します。
**D.** Webアプリケーションベンダーに連絡して問題を報告し、サーバー側の問題の可能性について問い合わせてください。
正解: **B,C,D (コメントを発表する)**
断続的なパフォーマンス問題のトラブルシューティングは、「エンタープライズネットワーク保証の設計と実装（300-445 ENNA）」カリキュラムの中核をなす要素です。基本認証を使用したトランザクションテストがランダムに失敗した場合、エンジニアは多層的な診断アプローチを用いて、障害の原因が認証情報、ネットワークパス、またはアプリケーションサーバーのいずれにあるかを特定する必要があります。
最初のステップは、認証情報の正当性を確認することです（オプションB）。基本認証では認証情報がヘッダーにエンコードされるため、ユーザー権限の変更やアカウントのロックアウトが発生すると、即座に認証エラーが発生します。
さまざまな地理的な場所から手動でログインを実行することで、場所に基づくアクセス制御リスト（ACL）や地域的なIdP同期の問題を排除するのに役立ちます。
最もデータ量の多い診断手順は、ThousandEyesのウォーターフォールチャートとHTTPレスポンスコードを分析することです（オプションC）。ウォーターフォールビューを使用すると、エンジニアは障害が最初の401 Unauthorizedチャレンジ中に発生したのか、認証情報が送信された後に発生したのかを確認できます。チャートに「待機時間」が高い、または5xxエラーが表示されている場合は、サーバー側の遅延または不安定性が問題の原因である可能性が高いです。「接続時間」が高い場合は、ネットワーク層の輻輳が問題の原因である可能性があります。
最後に、テレメトリでネットワークパスは正常と示されているにもかかわらず、サーバーが断続的にエラーを返したりタイムアウトしたりする場合は、エンジニアはWebアプリケーションベンダーに連絡する必要があります（オプションD）。ベンダーに特定のThousandEyes「共有リンク」を提供することで、ベンダーは全く同じパケットレベルおよびブラウザレベルのデータを確認でき、問題がクライアントのネットワークではなくサーバー側のインフラストラクチャにあることを証明できます。認証を無効にする（オプションA）ことは、認証されたワークフローを監視するために特別に設計されたテストの有効なトラブルシューティング手順ではありません。

質問: **117**
エンドユーザーエクスペリエンスに影響を与えるVPN接続の問題を監視するために、どのようなアラートルール構成が使用されますか？
**A.** スループットベースのルール
**B.** 接続性に基づくルール
**C.** パフォーマンスに基づくルール
**D.** 州ベースのルール
正解: **B (コメントを発表する)**
接続性に基づくルールは、VPN接続確立時間、パケット損失率、レイテンシのしきい値を設定することで、エンドユーザーエクスペリエンスに影響を与えるVPN接続の問題を監視し、接続障害、中断、または劣化を検出して、即時の調査と解決のためのアラートをトリガーします。

質問: **118**
図を参照してください。あるエンジニアは、世界中に支店を持つ物流会社に勤務しており、Cisco ThousandEyesを使用して、AWSでホストされているアプリケーションにおける従業員のデジタルエクスペリエンスを監視しています。
エンジニアは、アプリケーションが適切な時間内に応答しない場合にアラートが発動するようにアラートルールを設定しています。エンジニアはアラートルールを設定しましたが、過去1週間に支店の接続に複数の問題が発生したにもかかわらず、アラートは発動しませんでした。アラートを発動させるには、設定のどの部分を変更する必要がありますか？


**A.** 同じ」1エージェントを「いずれかの」1エージェントに変更します。
**B.** 「すべての」条件を「任意の」条件に変更します。
**C.** 「エージェント1人」を「エージェントの10%」に変更します。
**D.** 「エラーが発生しています」という警告条件を削除します。
正解: **D** (コメントを発表する)
このアラートはアプリケーションの応答速度の低下を検出するように設計されていますが、ルールでは以下の両方が必要です。
- エラーが発生しており、
- 合計時間 ≥ 4000 ms
アプリケーションの動作が単に遅いだけでHTTPエラーを返さない場合、最初の条件は満たされないため、アラートは発生しません。
「エラーが発生しています」を削除すると、応答時間が遅い場合のみアラートがトリガーされるようになります。

質問: **119**
Thousand23Eyes WAN InsightsはCisco SD-WANと統合し、ネットワークパフォーマンスの可視化とパス推奨機能を提供します。WAN Insightsが機能するために不可欠なSD-WAN環境のデータ ソースはどれですか？ 2つ選択してください）
**A.** vManageからの構成データ、デバイステンプレート、集中型ポリシー設定など。28
**B.** vAnalyticsによって収集された過去のネットワークパフォーマンス指標。SD-WANトンネルの損失、遅延、ジッターなどが含まれます。
**C.** SD-WAN内のエンドユーザーデバイスにインストールされたThousandEyesエンドポイントエージェントから収集されたデータ。
**D.** SD-WANデータプレーンからのアプリケーショントラフィックフローデータ。vManageアプリケーションリスト別に分類されています。
**E.** SD-WANエッジルーターからのSyslogメッセージ。トンネル確立に関連するデバイスイベントとエラーを示します。
正解: **B,D** (コメントを発表する)
エンタープライズネットワーク保証の設計と実装（300-445 ENNA）のアーキテクチャでは、ThousandEyes WAN InsightsがCisco SD-WAN管理スタックとの緊密な統合に依存していることが規定されています。予測パスの推奨を生成するために、プラットフォームはネットワークの動作とネットワークを通過するアプリケーションの両方を反映した特定のテレメトリデータを取り込む必要があります。
最初の重要なデータソースは、vAnalytics（オプションB）によって収集された過去のネットワークパフォーマンスメトリックです。WAN Insightsをアクティブ化する前に、エッジルータから生のネットワークテレメトリを収集して強化するために、vAnalyticsを有効にする必要があります。34このデータには、パケット損失、遅延、ジッターなど、すべてのSD-WANトンネルの詳細なメトリックが含まれます。35WAN Insightsは、これらの過去の傾向を分析して、将来のパス品質を予測し、どのトランスポート回線が長期にわたってアプリケーションのSLAを満たす可能性が最も高いかを判断します。
2 つ目の重要なデータ ソースは、アプリケーションのトラフィック フロー データ (オプション D) です。WAN Insights は、ファブリック内で現在アクティブになっているアプリケーションを把握し、Office 365、Webex、またはカスタム内部アプリなどの「ビジネスに不可欠な」サービスの推奨事項を優先する必要があります。38 この情報は、SD-WAN データ プレーンからフロー レコードとして取り込まれ、Cisco Catalyst SD-WAN Manager (vManage) で定義されているアプリケーション リストに基づいて分類されます。
オプションAとEは、一般的な管理には役立つものの、WAN Insights予測エンジンで使用される生のテレメトリ入力ではない構成データまたはログデータです。オプションCは、WAN InsightsがSD-WANファブリックの計算にThousandEyesエージェントベースの合成データではなく、インフラストラクチャテレメトリを明示的に使用するため、誤りです。WAN Insightsは、vAnalyticsのパフォーマンスメトリックとアプリケーションフローデータを組み合わせることで、最新のネットワーク保証の特長である「予測パス推奨」を提供できます。