Designing and Implementing Enterprise Network Assurance v1.0 (300-445)

Exam Description: Designing and Implementing Enterprise Network Assurance v1.0 (ENNA 300-445) is a 90-minute exam associated with the CCNP Enterprise Certification. This exam certifies a candidate's knowledge of network assurance design and implementation, including platforms and architecture, data collection and implementation, data analysis, and insights and alerts.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

20% 1.0 Platforms and Architecture

1.1 Determine agent types, such as synthetic user agent, scripting agent, and local collection agent to meet network assurance and security requirements

1.2 Determine agent location to meet network assurance and security requirements

1.3 Describe active and passive monitoring (RFC 7276 and RFC 7799)

1.4 Describe ThousandEyes WAN Insights

1.5 Describe the integration between Cisco technologies, such as ThousandEyes, vManage Cisco Catalyst Manager, Webex Control Hub, Meraki, and Endpoint Agent deployment through Secure Client

1.6 Describe setting a metric baseline

1.7 Select the integration type, such as API, alerting thresholds, open telemetry, and ITSM for the requested data

1.8 Select a Cisco network assurance platform based on business requirements, such as application communication, user experience, web, and events

25% 2.0 Data Collection Implementation

2.1 Configure enterprise agent on application servers and network infrastructure devices, including dedicated devices

2.2 Describe endpoint agent deployment at scale across the enterprise on end-user devices (Windows, Mac, and Room OS)

2.3 Configure tests using tools, such as ThousandEyes and Meraki Insights

2.3.a Network such as TCP/UDP, network characteristics, loss, jitter, and latency

2.3.b DNS

2.3.c Voice

2.3.d Web

2.4 Configure endpoint agent tests in ThousandEyes

2.5 Describe the purpose, implementation, and limitations of synthetic web tests

2.6 Implement common web authentication methods, such as basic, digest, bearer tokens, OAuth, SAML, and SSO when testing web applications

30% 3.0 Data Analysis

3.1 Diagnose network issues, such as packet loss, congestion, routing, and jitter using collected data

3.2 Diagnose end-device network issues, such as issues with a default gateway, local network, DNS server, proxy, VPN gateway, wireless, and real-time streaming using collected data

3.3 Diagnose web application performance issues using collected data such as browser waterfalls

3.4 Identify security issues, such as DDoS attacks, DNS hijacking, BGP hijacking, and route leaking affecting network performance

25% 4.0 Insights and Alerts

4.1 Configure alert rules based on network conditions, such as TCP protocol behavior, congestion, error counters, performance, throughput, state of BGP routing table, internet insights, MPLS, VPN, NetFlow, SNMP, and syslog

4.2 Configure alert rules that affect the end-user experience, such as CPU utilization, connectivity types (wired to wireless, Wi-Fi), browser behavior, and VPN

4.3 Select deliverables or metrics such as dashboard and alerts for IT operations, production support, app/dev teams, and executives

4.4 Validate alert configuration and functionality

4.5 Recommend optimization for network capacity planning, such as topology and configuration changes, and QoS based on data interpretation