Boost up Your Certification Score

UiPath

UiPath-IEPASv1

UiPath Certified Professional Infrastructure Engineer Professional - Automation Suite

Exams Boost
Boost Up Your Career

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Visit us at: https://www.examsboost.com/test/uipath-iepasv1

Latest Version: 6.0

Question: 1

Which command correctly performs an in-place upgrade of Kubernetes and the other infrastructure components?

A. ./bin/uipathctl rke2 upgrade cluster_config.json --versions versions/helm-charts.json
B. ./install-uipath.sh --upgrade -i ./cluster_config.json -o ./output.json -k --accept-license-agreement
C. ./bin/uipathctl manifest apply cluster_config.json --versions versions/helm-charts.json
D. ./configureUiPathAS.sh --upgrade -i ./cluster_config.json -o ./output.json -j server --accept-license-agreement

Answer: A

Explanation:
When executing an in-place upgrade on an Automation Suite cluster on Linux, the upgrade workflow separates the infrastructure layer from the application service layer. Upgrading the underlying Kubernetes distribution (RKE2), container runtime, and foundational infrastructure charts requires executing `./bin/uipathctl rke2 upgrade cluster_config.json --versions versions/helm-charts.json`. This command uses the target version definitions specified in `versions/helm-charts.json` and evaluates the existing parameters inside `cluster_config.json` to sequentially update the control plane, cordoning and draining nodes in a rolling fashion to preserve control-plane quorum. Legacy script parameters (such as `install-uipath.sh --upgrade` or `configureUiPathAS.sh`) were deprecated in favor of modern `uipathctl` subcommands, which orchestrate both infrastructure engine rollouts and Helm management. Once the infrastructure upgrade completes successfully, platform engineers proceed with upgrading the core application services. (Reference: UiPath Automation Suite Upgrade Procedures – Infrastructure and Kubernetes Upgrade Lifecycle).

Question: 2

Which processors are supported for deploying UiPath Automation Suite on Linux?

A. Only AMD processors.
B. Both AMD and Intel processors are supported if architecture requirements are met.
C. Only Intel processors.
D. Only ARM processors.

Answer: B

Explanation:
UiPath Automation Suite on Linux explicitly supports both AMD and Intel 64-bit processors, provided the systems meet core architecture and clock speed requirements. The containerized software suite is compiled for x86_64/AMD64 instruction set architectures. Both enterprise Intel Xeon and AMD EPYC

families provide the microarchitecture capabilities, hardware virtualization features, and vector instruction support required to execute Automation Suite container workloads. ARM-based processor platforms, including AWS Graviton, Ampere Altra, and Apple Silicon, are strictly unsupported due to underlying architectural incompatibilities with compiled product binaries and container base layers. When deploying across virtual machines or physical hosts, engineers must verify that CPU features are exposed transparently by the hypervisor and that minimum aggregate cluster compute thresholds (e.g., 96 cores across multi-node production clusters) are met across Intel or AMD hardware pools. (Reference: UiPath Automation Suite Infrastructure Requirements – CPU Architecture Support).

Question: 3

What does the installer check when it is run with the -k flag?

A. SQL database performance
B. Linux dependencies and infrastructure prerequisites
C. Availability of external registry
D. AI Fabric resource allocation

Answer: B

Explanation:
When executing the Automation Suite installer scripts on Linux platforms, the `-k` flag executes the built-in pre-installation validation check. This validation routine scrutinizes the host environment against foundational Linux prerequisites, checking for mandatory operating system packages (e.g., `lvm2`, `tar`, `curl`), kernel modules, sysctl network settings (such as `net.bridge.bridge-nf-call-iptables`), and disabled swap memory. It also verifies CPU and memory resource baselines, validates mount points, and ensures that firewall configurations permit intra-cluster communication across essential ports. By passing the `-k` parameter prior to committing cluster mutations, infrastructure architects proactively catch prerequisite gaps that would otherwise cause partial installation failures deep within RKE2 or container runtime provisioning. Passing the prerequisite check validates the underlying Linux host as certified and compliant with UiPath infrastructure requirements. (Reference: UiPath Automation Suite Installation Reference – CLI Flags and Host Pre-Requisites).

Question: 4

In the context of Automation Suite Platform, how is a server node defined?

A. A server node runs the UiPath products and shared components only.
B. A server node hosts cluster management services that perform important cluster operations, such as workload orchestration, cluster state management, load balance incoming requests, etc.
C. A server node runs special workloads like Task Mining analysis, Document Understanding pipelines that require GPU capability, Automation Suite Robots, etc.
D. A server node can host any of the UiPath products, shared components, or special workloads.

Answer: B

Explanation:
Within the UiPath Automation Suite architecture, a server node is defined as a host that provides the Kubernetes control plane services responsible for cluster management and core operational functions. These essential services include cluster state management via the distributed etcd datastore, API request validation through the `kube-apiserver`, workload scheduling via `kube-scheduler`, controller reconciliation loops via `kube-controller-manager`, and request distribution to platform microservices. In environments where compute resources permit, server nodes may also host certain UiPath product pods and shared platform components; however, this capacity sharing does not alter their primary architectural definition. Server nodes are distinguished from agent nodes (which focus on running business products) and specialized agent nodes (which are isolated for GPU workloads and Automation Suite Robots). Preserving the performance and quorum of server nodes is vital for platform reliability. (Reference: UiPath Automation Suite Architecture Overview – Server Node Capabilities and Responsibilities).

Question: 5

On which mount point is the additional capacity for the temporary registry recommended to be used?

A. /var
B. /opt
C. /tmp
D. /uipath

Answer: D

Explanation:
For offline and air-gapped Automation Suite installations, an internal temporary Docker/OCI registry is used to host container layers and Helm charts during cluster bootstrapping. Because container bundles for the platform require hundreds of gigabytes of disk storage, UiPath recommends placing this additional storage capacity under the `/uipath` mount point. By default, the temporary registry data path is configured as `/uipath/data/registry`. The `/uipath` mount is provisioned over a dedicated, high-capacity, high-performance volume, ensuring that unpacking large container images does not exhaust the root partition (`/`) or system logging directories (`/var`). Placing heavy image data on generic partitions can lead to operating system instability and node failures during setup. (Reference: UiPath Automation Suite Offline Installation Guide – Disk Partitioning and Temporary Registry Storage).

Question: 6

In a deployment across three availability zones, which tool can be used to route traffic to any of the load balancers according to a specified algorithm?

A. Traffic Manager
B. FluentD
C. ArgoCD
D. Prometheus

Answer: A

Explanation:
When deploying UiPath Automation Suite across multi-zone or multi-region topologies utilizing independent regional load balancers, Azure Traffic Manager (or AWS Route 53) provides global DNS-based traffic routing. Azure Traffic Manager operates at the DNS transport layer, evaluating endpoint health and directing client connections to specific load balancer IP addresses based on configured routing methods. Supported algorithms include priority routing for active-passive failover, weighted round-robin for distributing loads proportionally, and geographic routing for latency optimization. The other listed tools serve distinct operational functions: FluentD aggregates cluster logs, ArgoCD automates declarative GitOps platform deployments, and Prometheus collects time-series monitoring metrics. Traffic Manager provides DNS-level endpoint health checking and routing algorithms for multi-load balancer architectures. (Reference: UiPath Automation Suite Cloud Architecture Guide – Multi-Zone DNS and Traffic Management).

Question: 7

When setting up an external OCI-compliant registry for Automation Suite, what information is necessary for the suite to connect to it and pull images?

A. The Fully Qualified Domain Name (FQDN) or IP address of the registry server.
B. The number of CPU cores on the registry server.
C. The physical location of the registry server.
D. The brand of the storage used by the registry.

Answer: A

Explanation:
To enable an Automation Suite cluster to pull container images from an external OCI-compliant container registry, the configuration must declare the network endpoint: the Fully Qualified Domain Name (FQDN) or IP address of the registry server. During cluster bootstrapping and subsequent pod provisioning, the containerd runtime and Kubernetes image pull secrets resolve this FQDN or IP over HTTPS (or HTTP via insecure registry flags) to authenticate and pull container layers. Infrastructure details such as CPU core counts, datacenter locations, or backend storage vendors are abstracted by the registry's OCI API and are irrelevant to client connection configurations. Supplying a valid, network-accessible FQDN or IP address—along with required authentication credentials and CA trust chains—ensures nodes can download container images during installation and pod scheduling. (Reference: UiPath Automation Suite Pre-requisites – OCI Registry Connection Parameters).

Question: 8

Which AllowedMethods parameters must be configured when creating the CORS policy for the external object store?

A. GET, POST, DELETE
B. POST, DELETE, OPTIONS, HEAD

C. POST, GET, HEAD, DELETE, OPTIONS
D. GET, POST, DELETE, HEAD, PUT

Answer: D

Explanation:
When configuring an external S3-compatible or Azure Blob object store for UiPath Automation Suite, setting up an accurate Cross-Origin Resource Sharing (CORS) policy is mandatory to facilitate secure, direct browser-to-storage and service-to-storage communication. The documented CORS configuration explicitly requires the AllowedMethods parameters to include `GET`, `POST`, `DELETE`, `HEAD`, and `PUT`. These methods correspond directly to essential storage actions executed across the suite's microservices. Specifically, `PUT` and `POST` enable direct multi-part uploads of large automation packages, execution media, and Document Understanding datasets; `GET` enables retrieval of packages and artifacts; `HEAD` allows the service endpoints to verify object presence and metadata headers without downloading payloads; and `DELETE` permits lifecycle cleanup routines to remove deprecated artifacts. Excluding any of these five methods—most notably `PUT` or `HEAD`—results in HTTP 403 Forbidden errors during execution artifact publishing or client downloads in products such as Orchestrator, AI Center, and Data Service. (Reference: UiPath Automation Suite Infrastructure Pre-requisites – Object Store Configuration and CORS Policy Rules).

Question: 9

When configuring a GitOps tool to manage Automation Suite, what is typically required when the Git repository is private?

A. Disabling all security features of the Git repository.
B. Storing the Git repository on the same server as the GitOps tool.
C. Temporarily making the repository public during installation.
D. Configuring access credentials (e.g., SSH key, HTTPS token) for the GitOps tool to authenticate with the repository.

Answer: D

Explanation:
Automation Suite integrates GitOps methodologies (powered by ArgoCD) to automate the deployment, synchronization, and lifecycle management of platform microservices using Git repositories as the source of truth. When utilizing private repositories to protect proprietary configurations and sensitive parameters, the GitOps engine must authenticate to the remote repository. This requires configuring valid access credentials within the GitOps tool, typically using private SSH deploy keys, personal access tokens (PAT), or HTTPS credentials. These credentials allow ArgoCD to clone repositories, read Helm charts, detect branch drift, and apply configurations automatically. Exposing internal company configurations by making repositories public or attempting to co-locate Git servers on cluster nodes violates enterprise security standards. (Reference: UiPath Automation Suite GitOps Deployment Guide – ArgoCD Private Repository Access).

Question: 10

Is UiPath Insights supported on hosts with FIPS 140-2 enabled?

A. Not supported.
B. Yes, fully supported.
C. Supported with limited functionality.
D. Supported only on multi-node setup.

Answer: A

Explanation:
Federal Information Processing Standard (FIPS) 140-2 is a U.S. government computer security standard governing cryptographic modules. Within UiPath Automation Suite, host machines operating with FIPS 140-2 mode enabled are not supported for the UiPath Insights service. Insights utilizes third-party analytics and data visualization runtimes whose cryptographic algorithms and hashing libraries are not certified under or compatible with the strict kernel-level enforcement of FIPS 140-2. When Automation Suite is installed in a FIPS-compliant Linux host environment, the Insights service must be disabled in `input.json` or `cluster_config.json`. Attempting to run Insights with FIPS enabled results in container initialization crashes and service startup failures due to non-compliant cryptographic calls. Organizations requiring FIPS compliance must either exclude Insights from their deployment scope or run Insights in an isolated, non-FIPS environment. (Reference: UiPath Automation Suite Security and Compliance Guide – FIPS 140-2 Compatibility Matrix).

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer

