REST APIs

Q1. What type of relationship is defined as one resource existing only if another parent resource exist-for example, pages in a book?

- [ ] Partial
- [x] dependent
- [ ] associative
- [ ] linked

Q2. Which URL pattern is recommended when working with one resource and a collection of resources?

- [ ] /companies/{id} and /company
- [ ] /company/{id} and /companies
- [x] /companies/{id} and /companies
- [ ] /company/{id} and /company

Q3. When dealing with JSON web Tokens (JWTs), what is a claim?

- [x] data in the token
- [ ] Ownership
- [ ] a permission
- [ ] and integer

Q4. Which REST constraint specifies that knowledge and understanding obtained from one component of the API should be generally applicable elsewhere in the API?

- [x] Uniform Interface
- [ ] Client-Server
- [ ] Stateless
- [ ] Chacheable

Q5. What would you enable to allow a browser on another site to make an AJAX request to your API?

- [ ] HTTP
- [ ] REST
- [ ] OPTIONS
- [x] CORS

Q6. APIs commonly use webhooks to _.

- [x] notify other systems of an event
- [ ] catch error faster
- [ ] improve error logging
- [ ] log additional data

Q7. What is the underlying goal of all APIs?

- [ ] to add new technologies to an organization's infrastructure.
- [x] to share features and functionality with other system.
- [ ] to move infrastructure to the cloud.
- [ ] to appease the latest digital transformation effort.

Q8. Which is a common command-line tool for using or exploring an API?

- [ ] bash
- [x] curl
- [ ] ssh
- [ ] powerShell

Q9. What is the modern specification for describing an API?

- [x] OpenAPI (Swagger)
- [ ] WADL
- [ ] WSDL
- [ ] OAuth

OpenAPI Specification

Q10. Which HTTP verb is normally used to update or create a resource in an API?

- [ ] SUBMIT
- [ ] WRITE
- [x] POST
- [ ] CREATE

HTTP request methods

Q11. What is one benefit of server-side caching in APIs?

- [ ] Mobile app work better.
- [ ] It improves uptime.
- [ ] It offers better security.
- [x] It reduce load on servers.

Q12. Your API resource does not allow deletion, and a client application attempted to delete the resource. What HTTP response code should you return?

- [ ] 409 Conflict
- [ ] 400 Bad Request
- [ ] 406 Not Acceptable
- [x] 405 Method Not Allowed

Response Codes

Q13. What is OpenID Connect?

- [x] an identify layer on top of OAuth 2.0
- [ ] the new name for SAML 3.0
- [ ] a modern replacement for API keys
- [ ] an SSO competitor for OAuth 2.0

What is OpenID Connect?

Q14. What is one benefit of GraphQl over REST approaches?

- [x] flexible querying/responses
- [ ] more stable APIs
- [ ] compatible with more gateways
- [ ] more secure by default

GraphQL vs. REST

Q15. Which REST constraint specifies that there should be no shared context?

- [x] Stateless

- [ ] Client-Server
- [ ] Uniform Interface
- [ ] Cacheable

Q16. What purpose does a User-Agent serve?

- [ ] It identifies the user ID.
- [x] It identifies the client application or SDK.
- [ ] It identifies if the API should expect a user authentication.
- [ ] It identifies if the API should accept microservice traffic.

Q17. If you were to add versioning by using the Accept and Content-Type header, what would be the correct format of the header value?

- [ ] application/json
- [ ] application/json_version2
- [ ] text/html
- [x] application/vnd.myapp.v2+json

Reference

Q18. What is one benefit that OAuth provides over an API key approach?

- [ ] A token is encrypted.
- [ ] A token is encoded.
- [x] A token is scoped to the use case.
- [ ] A token can be shared between systems.

How to easily secure your APIs with API keys and OAuth

Q19. The ability to execute the same API request over and over again without changing the resource's state is an example of _.

- [ ] stateless architecture
- [x] idempotency
- [ ] a uniform interface
- [ ] cacheability

Q20. What component can you use to wrap legacy architectures or protocols into a REST interface for easier consumption and integration?

- [x] API proxy
- [ ] API gateway
- [ ] OpenAPI
- [ ] OAuth authorization server

Q21. What protection does a JSON Web Token (JWT) offer to mitigate tampering with its contents?

- [ ] transport over SSL
- [ ] encrypted payload
- [x] a signature
- [ ] encoded payload

Q22. What OAuth term is used to represent permissions?

- [ ] token
- [x] scope

- [ ] claim
- [ ] back channel

OAuth Scopes

Q23. What additional type of token would you see when using OpenID Connect?

- [x] ID token
- [ ] refresh token
- [ ] access token
- [ ] auth code token

Q24. What should you add to a Cache-Control response header to specify that a response should not be stored in an intermediary cache?

- [ ] no-proxy
- [ ] client-only
- [ ] restricted
- [x] private

reference

Q25. Which OAuth grant type can support a refresh token?

- [x] Authorization Code Grant
- [ ] Client Credentials Grant
- [ ] Implicit Grant
- [ ] Authentication Grant

Reference:

Q26. Using OAuth, what scope would you request for write access to the API?

- [ ] It varies from API to API.
- [x] admin
- [ ] write
- [ ] read-write

Q27. Which property would you use to include subresources directly into a JSON document?

- [ ] _embedded
- [ ] resources
- [x] subresources
- [ ] _links

Q28. What is the best way to track SDK and version usage?

- [x] tracking downloads
- [ ] Accept headers
- [ ] user agents
- [ ] polling users

Q29. Which REST constraint allows for the presence of caching, routing, and other systems between the client and server?

- [x] Layered System
- [ ] Stateless
- [ ] Client-Server

- [ ] `Cacheable`

Q30. Which content is best to include in your documentation?

- [ ] `your tech stack`
- [ ] `reasoning for your naming schema`
- [ ] `your mission statement`
- [x] `sample code`

Q31. What metric tracks overall availability for your API?

- [ ] `Response Time`
- [ ] `Time to First Hello World`
- [ ] `TTL`
- [x] `Uptime`

Q32. What is the recommended method and URL pattern for retrieving a specific user?

- [ ] `GET /user/{id}`
- [x] `GET /users/{id}`
- [ ] `GET /user?id={id}`
- [ ] `GET /users?id={id}`

Q33. What is the purpose of a link relation?

- [ ] `to describe relationships between resources or actions`
- [ ] `to describe subresources related to the current one`
- [x] `to link two resources together`
- [ ] `to describe a resource and its purpose`

Q34. When building SDKs, which languages should you support?

- [ ] Java, Javascript, and .NET
- [ ] and you can support
- [ ] PHP, Python, and Go
- [x] the languages that your target users use

Q35. Which property would you use to include references to other resources in a JSON document?

- [x] `resources`
- [ ] `_embedded`
- [ ] `subresources`
- [ ] `_links`

Q36. What is OAuth?

- [x] an authorization framework for granted delegated access
- [ ] an approach to single sign-on for APIs
- [ ] a method for API authentication
- [ ] HTTP Basic Authentication 2.0

Q37. What should your API documentation describe?

- [ ] JSON
- [ ] HTTP
- [x] common use cases
- [ ] your tech stack

Q38. What is the purpose of an OAuth refresh token?

- [ ] to share user profile information
- [ ] to update an API configuration
- [ ] to keep a web session active
- [x] to retrieve an access token

Understanding Refresh Tokens

Q39. What is Time to First Hello World?

- [x] how long it takes for a developer to do something with your API
- [ ] how long it takes to start a new programming language
- [ ] how long it takes to install your SDK
- [ ] how long it takes to read your documentation

Q40. Which response header tells the client and intermediaries that the response is not to be cached anywhere?

- [ ] Cache-State: none
- [ ] Expires:-1
- [ ] Cache-Control: no-cache
- [x] Cache-Control: no-store

Q41. What component hides the distinctions or boundaries between various microservices from end-client applications?

- [x] `API gateway`
- [ ] `API logging`
- [ ] `a layered system`
- [ ] `API proxy`

Q42. The textbook approach to api versioning is to use _.

- [ ] `common knowledge`
- [ ] `URLs`
- [ ] `no versioning`
- [x] `the Accept header`

Q43. Which is the most secure method to transmit an API key?

- [ ] `URL parameter`
- [x] `Authorization header`
- [ ] `Base64 encoding`
- [ ] `Basic Auth`

Q44. Within Oauth, what component validates the user's identity?

- [ ] `client`
- [ ] `not specified`
- [x] `authorization server`
- [ ] `resource server`

Q45. API traffic that is entirely internal to your organization is normally called _?

- [ ] `inbound traffic`
- [ ] `north-south traffic`
- [x] `internal traffic`

- [ ] east-west traffic

Q46. What is the best approach for requesting JSON instead of XML from an API?

- [ ] Add .json to the URL.
- [ ] APIs do not use XML.
- [ ] Use the Content-Type header.
- [x] Use the Accept header.

Q47. When a user attempts to access a record that is not their own, which HTTP response code is the most appropriate?

- [x] 403
- [ ] 404
- [ ] 401
- [ ] 405

Response Codes

Q48. Which is a benefit of using an API gateway?

- [ ] HTTP verbs
- [ ] JSON payloads
- [ ] HTTP response codes
- [x] rate limiting/throttling

Q49. API testing must be treated as _?

- [ ] red team testing
- [ ] white box testing
- [ ] blue box testing
- [x] black box testing

Q50. Which HTTP verb is used in a CORS preflight request?

- [ ] PUT
- [ ] POST
- [ ] GET
- [x] OPTIONS

Q51. Which response header will tell the client that the response is cached for 1 minute ?

- [ ] Expires: 1 minute
- [x] Cache-Control: max-age=60
- [ ] Expires: 1 January 2020
- [ ] Cache-Expires: max-age=60

Cache Control Header

Q52. What is the concept that allows an API client to explore an API via links embedded in payloads?

- [ ] hypermedia
- [x] link relations
- [ ] parsing
- [ ] browsing

Q53. To create a new resource, what HTTP response code should you receive?

- [ ] 405

- [x] `201`
- [ ] `204`
- [ ] `202`

Response Codes

Q54. Which is an example of Code on Demand?

- [ ] AWS Lambda
- [ ] downloading open-source software
- [ ] Serverless
- [x] JavaScript on a webpage

Code on Demand

Q55. Which URL pattern should you follow for accessing a subresource attached to a specific resource?

- [ ] /companies/employees/{companyId}/{employeeId}
- [ ] /company/{companyId}/employees/{employeeId}
- [x] /companies/{companyId}/employees/{employeeId}
- [ ] /companies/{companyId}/employee/{employeeId}

Resource Naming

Q56. Which REST constraint essentially prohibits the use of cookies?

- [x] Stateless
- [ ] Cacheable
- [ ] Layered System
- [ ] Uniform Interface

Q57. Which HTTP verb is used to delete a resource?

- [ ] FLUSH
- [x] DELETE
- [ ] CLEAR
- [ ] DESTROY

Q58. Which verb is *not* considered idempotent?

- [ ] DELETE
- [ ] GET
- [ ] PUT
- [x] POST

Idempotency

Q59. Which REST constraint specifies that each request should stand on its own and not have a specific required order?

- [ ] Uniform Interface
- [ ] Cacheable
- [x] Stateless
- [ ] Client-Server

REST Architectural Constraints

Q60. When you get a 429 response code, what should you do next?

- [ ] Check you JSON structure.

- [x] Slow down your requests.
- [ ] Check the API uptime status.
- [ ] Check you API key.

Q61. When exploring record sets, what is the best approach for pagination?

- [ ] date-based filtering
- [x] next/previous cursors
- [ ] page size and filters
- [ ] database IDs

Q62. What is *not* a method for API authentication or authorization?

- [ ] OAuth
- [x] biometrics
- [ ] API Keys
- [ ] username and password

Q63. Which HTTP response code usually means the requested work is still processing and may or may not result in an error later?

- [ ] 200 OK
- [ ] 204 No Content
- [ ] 201 Created
- [x] 202 Accepted

Q64. When validating a JWT, what are some of the claims that you must confirm? (Select all that apply.)

```
A. The exp (expiration) has not passed.
B. The algorithm is sufficient.
C. The signature matches the payload.
D. The token was Base64 encoded.
E. The iss (issuer) is the auth server you expect.
F. There is a refresh token.
G. The cid (client ID) is the client you expect.
H. The token was encrypted.
```

- [x] A,B,E,H
- [ ] B,C,F,G
- [ ] A,D,G,H
- [ ] A,C,E,G

Q65. API traffic that enters and leaves your organization is normally called _?

- [ ] `east-west traffic`
- [ ] `inbound traffic`
- [x] `north-south traffic`
- [ ] `external traffic`

North-South vs East-West Traffic

Q66. Which OAuth grant type is appropriate for mobile apps?

- [x] Authorization Code with PKCE
- [ ] Client Credentials
- [ ] Device

- [ ] Resource Owner Password

OAuth 2.0 for Native and Mobile Apps

Q67. Which datetime format is the easiest or most predictable to parse and process?

- [ ] `YY-M-D hh:mm:ss+TZ`
- [ ] `YY-M-D h:mm:ss`
- [x] `YYYY-MM-DDThh:mm:ssZ`
- [ ] `YYYY-M-D hh:mm:ss`

The 5 laws of API dates and times

Q68. Which header is *not* used in cache management?

- [x] Rate-Limit
- [ ] Expires
- [ ] Etag
- [ ] Cache-Control

Cache-Control Expires Etag Rate limiting your RESTful API

Q69. A client application uses a filter or a search in your API correctly but there are zero results. What is the best response code?

- [ ] 204 No Content
- [ ] 400 Bad Request
- [x] 200 OK
- [ ] 404 Not Found

Response Status Codes

Q70. Which HTTP verb is normally used to retrieve or create a resource in an API?

- [ ] `RETRIEVE`
- [ ] `FORM`
- [x] `GET`
- [ ] `READ`

Q71. To create a new resource, what HTTP response code should you receive?

- [ ] `200`
- [ ] `405`
- [x] `201`
- [ ] `204`

HTTP request methods

Q72. You are developing a RESTful API for a new project on GitHub. Security is a top priority, and you want to ensure that only authorized users can access specific endpoints. Which of the following mechanisms should you use to achieve this goal?

- [ ] API rate limiting
- [x] OAuth 2.0
- [ ] Basic Authentication
- [ ] HTTP Basic Auth