Microsoft FHIR-CDS-Sync Agent Cloud Design Pattern

Ref: [Cloud design patterns - Azure Architecture Center | Microsoft Docs]

Table of Contents

Introduction 1

Availability 2

Data Management 2

Data Protection 3

Design and Implementation patterns 4

Management and Monitoring patterns 5

Messaging 5

Performance and Scalability 6

Resiliency 7

Security 8

Security Resources 8

Introduction

The FHIR-CDS-Sync Agent follows the Microsoft Well Architected Framework focusing on the following categories: Availability, Data Management, Design and Implementation, Management and Monitoring, Messaging, Performance and Scalability, Resiliency and Security.

Each pattern listed below describes the problem that the pattern addresses, considerations for applying the pattern, and an example based on Microsoft Azure. Most of the patterns include code samples or snippets that show how to implement the pattern on Azure.

Availability

Availability is measured as a percentage of uptime and defines the proportion of time that a system is functional and working. Availability is affected by system errors, infrastructure problems, malicious attacks, and system load. Cloud applications typically provide users with a service level agreement (SLA), which means that applications must be designed and implemented to maximize availability.

The FHIR-CDS-Sync Agent utilizes the following Availability Patterns

Pattern	Summary
Deployment Stamps	The Sync Agent components can be deployed in multiple regions at one time, relying on separate configuration files to manage endpoints across deployment stamps
Geodes	Components can be deployed into a set of geographical nodes, each of which can service any client request in any region.
Health Endpoint Monitoring	Employing several types of functional checks that can be accessed through exposed endpoints at regular intervals.
Queue-Based Load Leveling	Queues that acts as a buffer between tasks and services that it invokes, to smooth intermittent heavy loads and to maintain referential integrity.
Throttling	Several control functions to manage resources consumed.

To mitigate against availability risks from malicious Distributed Denial of Service (DDoS) attacks, Private Endpoints can be used (with the exception of Dynamics) or customers can implement the native Azure DDoS protection standard service.

Data Management

The FHIR-CDS-Sync Agent houses healthcare data in different Platform as a Service (PaaS) systems which can span several locations and regions for performance, scalability, or availability. The FHIR-CDS-Sync Agent maintains data consistency through business rules.

Data is protected at rest, in transit, and via authorized access mechanisms to maintain security assurances of confidentiality, integrity, and availability. Refer to the Azure Security Benchmark Data Protection Control for more information.

The FHIR-CDS-Sync Agent utilizes the following Data Management Patterns

Pattern	Summary
Cache-Aside	The Sync Agent utilizes several persist mechanisms to protect data before it is loaded into Dynamics.
CQRS	Segregate operations that read data from operations that update data by using separate interfaces.
Event Sourcing	Use an append-only store to record the full series of events that describe actions taken on data in a domain.
Index Table	The FHIR-CDS-Sync Agent utilizes the Azure API for FHIR and Microsoft Dynamics to index fields in data their respective data stores that are frequently referenced by queries.
Static Content Hosting	Deploy static content to a cloud-based storage service that can deliver them directly to the client.

Data Protection

Data Protection involves the discovery, classification, and labeling of customer sensitive data so that you can design the appropriate controls to ensure sensitive information is stored, processed, and transmitted securely by the organization's technology systems.

With Patient Health Information (PHI) and Personal Identification Information (PII) prevalent in the FHIR-CDS-Sync Agent the Sync Agent implements the following security resources.

Resource	Summary
Azure Security Benchmarks	Prescriptive best practices and recommendations to integrate into architectures for securing workloads, data, services, and enterprise environments on Azure.
Security Strategy Guidance	Building and updating a security strategy for cloud adoption and modern threat environment
Security Roles and Responsibilities	Guidance on security roles and responsibilities including definitions of mission/outcome for each organizational function and how each should evolve with the adoption of cloud.
Getting Started Guide for Security	Guidance for planning and implementing security throughout cloud adoption

Design and Implementation patterns

The FHIR-CDS-Sync Agent design encompasses factors such as consistency and coherence in component design and deployment, maintainability to simplify administration and development, and reusability to allow components and subsystems to be used in other applications and in other scenarios.

Decisions made during the design and implementation phase have a huge impact on the quality and the total cost of ownership of cloud hosted applications and services.

The FHIR-CDS-Sync Agent utilizes the following Design and Implementation Patterns

Pattern	Summary
Anti-Corruption Layer	The FHIR-CDS-Sync Agent implements an adapter/converter paradigm between HL7 and FHIR Systems.
Backends for Frontends	Create separate backend services to be consumed by specific frontend applications or interfaces.
CQRS	Segregate operations that read data from operations that update data by using separate interfaces.
External Configuration Store	Move configuration information out of the application deployment package to a centralized location.
Gateway Aggregation	Use a gateway to aggregate multiple individual requests into a single request.
Gateway Offloading	Offload shared or specialized service functionality to a gateway proxy.
Gateway Routing	Route requests to multiple services using a single endpoint.
Pipes and Filters	Break down a task that performs complex processing into a series of separate elements that can be reused.
Sidecar	Deploy components of an application into a separate process or container to provide isolation and encapsulation.
Static Content Hosting	Deploy static content to a cloud-based storage service that can deliver them directly to the client (customer selected option).
Strangler	Incrementally migrate a legacy system by gradually replacing specific pieces of functionality with new applications and services.

Management and Monitoring patterns

Cloud applications run in a remote datacenter where customers do not have full control of the infrastructure or, in some cases, the operating system. This can make management and monitoring more difficult than an on-premises deployment.

The FHIR-CDS-Sync Agent exposes runtime information that administrators and operators can use to manage and monitor the system, as well as supporting changing business requirements and customization without requiring the application to be stopped or redeployed.

The FHIR-CDS-Sync Agent utilizes the following Management and Monitoring Patterns

Pattern	Summary
Anti-Corruption Layer	Implement a façade or adapter layer between a modern application and a legacy system.
External Configuration Store	Move configuration information out of the application deployment package to a centralized location.
Gateway Aggregation	Use a gateway to aggregate multiple individual requests into a single request.
Gateway Offloading	Offload shared or specialized service functionality to a gateway proxy.
Gateway Routing	Route requests to multiple services using a single endpoint.
Health Endpoint Monitoring	Implement functional checks in an application that external tools can access through exposed endpoints at regular intervals.
Sidecar	Deploy components of an application into a separate process or container to provide isolation and encapsulation.
Strangler	Incrementally migrate a legacy system by gradually replacing specific pieces of functionality with new applications and services.

Messaging

The distributed nature of cloud applications requires a messaging infrastructure that connects the components and services, ideally in a loosely coupled manner in order to maximize scalability. Asynchronous messaging is widely used, and provides many benefits, but also brings challenges such as the ordering of messages, poison message management, idempotency, and more.

The FHIR-CDS-Sync Agent utilizes the following Messaging Patterns

Pattern	Summary
Asynchronous Request-Reply	Decouple backend processing from a frontend host, where backend processing needs to be asynchronous, but the frontend still needs a clear response.
Claim Check	Split a large message into a claim check and a payload to avoid overwhelming a message bus.
Choreography	Have each component of the system participate in the decision-making process about the workflow of a business transaction, instead of relying on a central point of control.
Pipes and Filters	Break down a task that performs complex processing into a series of separate elements that can be reused.
Publisher-Subscriber	Enable an application to announce events to multiple interested consumers asynchronously, without coupling the senders to the receivers.
Queue-Based Load Leveling	Use a queue that acts as a buffer between a task and a service that it invokes in order to smooth intermittent heavy loads.
Scheduler Agent Supervisor	Coordinate a set of actions across a distributed set of services and other remote resources.
Sequential Convoy	Process a set of related messages in a defined order, without blocking processing of other groups of messages.

Performance and Scalability

Performance is an indication of the responsiveness of a system to execute any action within a given time interval, while scalability is ability of a system either to handle increases in load without impact on performance or for the available resources to be readily increased. Cloud applications typically encounter variable workloads and peaks in activity. The FHIR-CDS-Sync Agent is able to scale out (within limits) to meet peaks in demand, and scale in when demand decreases. Scalability concerns not just compute instances, but other elements such as data storage, messaging infrastructure, and more.

The FHIR-CDS-Sync Agent utilizes the following Performance and Scalability Patterns

Pattern	Summary
Cache-Aside	Load data on demand into a cache from a data store

Choreography	Have each component of the system participate in the decision-making process about the workflow of a business transaction, instead of relying on a central point of control.
CQRS	Segregate operations that read data from operations that update data by using separate interfaces.
Event Sourcing	Use an append-only store to record the full series of events that describe actions taken on data in a domain.
Deployment Stamps	Deploy multiple independent copies of application components
Geodes	Deploy backend services into a set of geographical nodes, each of which can service any client request in any region.
Materialized View	Generate prepopulated views over the data in one or more data stores when the data isn't ideally formatted for required query operations (Dynamics only)
Queue-Based Load Leveling	Use a queue that acts as a buffer between a task and a service that it invokes in order to smooth intermittent heavy loads.
Static Content Hosting	Deploy static content to a cloud-based storage service that can deliver them directly to the client (optional)
Throttling	Control the consumption of resources used by an instance of an application, an individual tenant, or an entire service.

Resiliency

Resiliency is the ability of a system to gracefully handle and recover from failures, both inadvertent and malicious.

The nature of cloud hosting, where applications are often multi-tenant, use shared platform services, compete for resources and bandwidth, communicate over the Internet, and run on commodity hardware means there is an increased likelihood that both transient and more permanent faults will arise. The connected nature of the internet and the rise in sophistication and volume of attacks increase the likelihood of a security disruption.

Detecting failures and recovering quickly and efficiently, is necessary to maintain resiliency.

The FHIR-CDS-Sync Agent utilizes the following Resiliency Patterns

Pattern	**Summary**

Bulkhead	Isolate elements of an application into pools so that if one fails, the others will continue to function.
Circuit Breaker	Handle faults that might take a variable amount of time to fix when connecting to a remote service or resource.
Compensating Transaction	Undo the work performed by a series of steps, which together define an eventually consistent operation.
Health Endpoint Monitoring	Implement functional checks in an application that external tools can access through exposed endpoints at regular intervals.
Queue-Based Load Leveling	Use a queue that acts as a buffer between a task and a service that it invokes in order to smooth intermittent heavy loads.
Scheduler Agent Supervisor	Coordinate a set of actions across a distributed set of services and other remote resources.

Security

Security provides confidentiality, integrity, and availability assurances against malicious attacks on information systems (and safety assurances for attacks on operational technology systems). Losing these assurances can negatively impact your business operations and revenue, as well as your organization's reputation in the marketplace. Maintaining security requires following well-established practices (security hygiene) and being vigilant to detect and rapidly remediate vulnerabilities and active attacks.

The FHIR-CDS-Sync Agent utilizes the following Security Patterns

Pattern	**Summary**
Federated Identity	Delegate authentication to an external identity provider.
Gatekeeper	Protect applications and services by using a dedicated host instance that acts as a broker between clients and the application or service, validates and sanitizes requests, and passes requests and data between them.
Valet Key	Use a token or key that provides clients with restricted direct access to a specific resource or service.

Security Resources

With Patient Health Information (PHI) and Personal Identification Information (PII) prevalent in the FHIR-CDS-Sync Agent the Sync Agent implements the following security resources.

Resource	Summary
Azure Security Benchmarks	Prescriptive best practices and recommendations to integrate into architectures for securing workloads, data, services, and enterprise environments on Azure.
Security Strategy Guidance	Building and updating a security strategy for cloud adoption and modern threat environment
Security Roles and Responsibilities	Guidance on security roles and responsibilities including definitions of mission/outcome for each organizational function and how each should evolve with the adoption of cloud.
Getting Started Guide for Security	Guidance for planning and implementing security throughout cloud adoption