Ministério da Educação e Ciência

Linhas Guia de Resolução

U.C. 21108

Sistemas Distribuídos

e-Fólio B – Linhas Guia de Resolução

-- INSTRUÇÕES --

Este documento apresenta linhas guia, referenciando o manual da cadeira, para a resolução do e-fólio B.

Nota que não é apresentada uma resolução completa. São documentados os diversos itens que podem ser incluídos tendo em conta os diversos critérios.

Critérios

Os critérios considerados estão documentados na tabela abaixo.

% Item	ID Critério	Cotação	Descrição Critério
25%	C1.1	40%	Indentifica/apresenta suporte para transações e operações atómicas
	C1.2	20%	Identifica aspetos de segurança quanto ao armazenamento dos dados
	C1.3	40%	Identifica/apresenta os mecanismos de acesso aos dados dos pacientes
25%	C2.1	40%	Identifica/discute mecanismos para atribuição de alarmes com severidade alta.
	C2.2	40%	Identifica/discute mecanismos de filas de espera para alarmes
	C2.3	20%	Identifica/discute mecanismos para implementar tempo de resposta
20%	C3.1	50%	Identifica/apresenta os mecanismos de nomes (ex: DNS)
	C3.2	50%	Identifica/apresenta configurações de DNS para serviços críticos (duplicar registos)
20%	C4.1	80%	Identifica/apresenta mecanismo para guardar os dados de forma segura (e.g. campos sensíveis)
	C4.2	20%	Apresenta configurações para implementar AAA (Autenticação, Accounting e Autorização) com LDAP
10%	Geral	100%	Clareza na apresentação do relatório

C1

Explicar a necessidade de suporte de transações e operações atómicas, nomeadamente para algumas situações, como:

1- Atualização dos dados dos pacientes. Garantir que este processo é feito de forma controlada e atómica. Esta operação pode incluir itens como a atualização do estado clínico, dos exames efetuados, ou de outros campos.

Referir o tipo de lock desejável e porquê. Por exemplo, usar o two-phase locking…
Referir a utilização de campos de estado para controlo do estado da informação.

Descrever os aspetos de armazenamento dos dados, em que os campos sensíveis devem ser guardados de forma encriptada. O envio dos dados entre frontend e SGBD deve também usar mecanismos seguros de encriptação. O acesso aos dados deve ser controlado através de mecanismos de login/password, de certificados.

Alguns aspetos que podem ajudar na questão de segurança são a utilização de logs, para efeitos de auditing. Ou até mesmo aspetos de segurança física, como o controlo físico ao datacenter dos servidores, a utilização de tecnologia RAID para a redundância de dados e tolerância a falhas.

C2

A gestão de alarmes com diferentes níveis de severidade pode ser recorrer a diversas abordagens:

1- Usar filas de mensagens, conforme descrito no capítulo 6. A nível prático pode-se ter:
    a. Uma fila de mensagens para severidade alta
    b. Uma fila de mensagens para severidade média
    c. Uma fila de mensagens para severidade baixa

1. Recorrer a base de dados em que o registo dos alarmes é feito em diferentes tabelas, ou numa tabela com o campo de severidade. A aplicação frontend ao atribuir um alarme a um medico altera o status do alarme para atribuído
2. Recorrer a um Sistema publish subscribe com tópicos específicos.
    d. Tópico para severidade alta
    e. Tópico para severidade média
    f. Tópico para severidade baixa

Esta funcionalidade pode ser complementada com serviço email ou outro Sistema de notificações nas aplicações mobile PorHealth.

A funcionalidade de verificar o tempo de resposta pode ser implementada incluindo timestamp nas próprias mensagens, e implementando um processo controlador que verifica o nível de severidade.

C3
O serviço de nomes para a rede deve usar o DNS, para assegurar o acesso à Internet e Intranet. Os registos no DNS devem ser configurados de forma hierarquica, tendo em conta as diversas filiais.
Por exemplo, o domínio base do Sistema PorHealth pode ser: porhealth.com.pt

Configuração DNS / politicas de configuração	**Descrição /Exemplos**
Serviços comuns ficam diretamente associado ao domínio base.	Estes serviços incluem: • www → frontend da aplicação • m → versão mobile do frontend da aplicação. • mail, smtp, mx → Serviço de email • alarms → Sistema de gestão de alarmes
Os serviços críticos devem ter configuração para alta disponibilidade no DNS	Estes serviços podem incluir: • www → • m → • Alarms → A configuração para alta disponibilidade depende do software de resolução de nomes (e.g. Bind, PowerDNS) mas a lógica é ter diversos IPs associados ao mesmo nome e do tipo de registo A. Exemplo: www IP1, IP2, IP3
Filiais devem ser consideradas um subdomínio. Os serviços específicos de cada	filia11.porhealth.com.pt filia12.porhealth.com.pt

filial devem funcionar dentro deste subdomínio	… Serviços específicos devem ficar acessíveis em: www.filial1.porhealth.com.pt.

C4

O serviço de nomes dos utilizadores do Sistema PorHealth, deve recorrer a mecanismos tipo LDAP para possibilitar a administração da informação dos utilizadores do sistema de uma forma centralizada e escalável.

Algumas regras, políticas de configuração são detalhadas na tabela abaixo:

Nome Política	**Descrição**
Campos sensíveis	Guardados de forma encriptada
Super administrador	Só o super administrador é que tem acesso ao Sistema LDAP em que devem ser implementados mecanismos seguros de autenticação (e.g. autenticação two-factor).
Administradores	Podem adicionar utilizadores e fazer reset à palavra passe
Autenticação de users	Deve ter suporte para a autenticação de utilizadores
Accounting	Deve ter suporte para accounting, para saber quanto tempo o user esteve logado num dado serviço
Autorização	Deve ter suporte para regras de autorização, ou seja, a role do user e as respetivas permissões
Validade dos dados	Deve ter suporte para ativar e desativar determinadas contas.