

**Sprint 2**

**Turma 3NA-Grupo 76**

1200618 – Jorge Cunha

**Professor:**

Dílio Ribeiro, DAR

**Unidade Curricular:**

ADMINISTRAÇÃO DE SISTEMAS (ASIST)

**Data: 26/11/2023**

**Índice**

[**Índice** 0](#_Toc148222126)

[**Introdução** 1](#_Toc148222127)

[**User Story 1** 2](#_Toc148222128)

[**User Story 2** 3](#_Toc148222129)

[**User Story 5** 7](#_Toc148222130)

[**User Story 6** 7](#_Toc148222130)

# **Introdução**

O presente relatório foi escrito no âmbito do Sprint 2 da unidade curricular Administração de Sistemas.

Neste relatório iremos demonstrar as Us, que nos foram pedidas para desenvolver, como também a sua explicação e como foi desenvolvida. Também apresentaremos imagens que comprovam que as user stories foram adicionadas a máquina virtual.

# **User Story 650**

1. Como administrador do sistema quero que apenas os clientes da rede interna do DEI (cablada ou via VPN) possam aceder à solução

Introdução:

Este relatório descreve a implementação de medidas de segurança para garantir que apenas clientes da rede interna do DEI, seja via conexão cablada ou VPN, tenham acesso à nossa aplicação.

O objetivo é restringir o acesso ao servidor da aplicação para aumentar a segurança e controlar o tráfego.

Metodologia:

A estratégia envolveu o uso do iptables, uma ferramenta de manipulação de tabelas de roteamento do kernel do Linux, para filtrar o tráfego de rede.

A configuração foi projetada para bloquear todo o acesso não autorizado ao servidor e permitir apenas tráfego de IPs específicos.

Etapas de Implementação:

Definição de Política Padrão:

Configuramos a política padrão da cadeia INPUT para DROP.

Isso significa que todos os pacotes que chegam serão descartados por padrão, a menos que correspondam a uma regra definida.

Comando utilizado: iptables -P INPUT DROP.

Configuração de IPs Permitidos:

A gama de IPs permitidos foi definida com base na rede interna do DEI (192.168.43.0/24). Apenas os pacotes originados desta faixa de IP foram permitidos para o porto 4000, que é usado pela nossa aplicação.

Comando utilizado: iptables -A INPUT -s 192.168.43.0/24 -p tcp --dport 4000 -j ACCEPT.

Bloqueio de Acesso Não Autorizado:

Para reforçar a segurança, adicionamos uma regra para bloquear explicitamente qualquer acesso não autorizado ao porto 4000.

Comando utilizado: iptables -A INPUT -p tcp --dport 4000 -j DROP.

Persistência da Configuração:

Para garantir que as regras do iptables permaneçam ativas após reinicializações do sistema, salvamos a configuração em um arquivo de texto.

Comandos utilizados: iptables-save | tee /etc/iptables/rules.v4 para salvar e iptables-restore < /etc/iptables/rules.v4 para carregar.

Conclusão:

Com estas configurações, conseguimos garantir que apenas os clientes da rede interna do DEI possam acessar a aplicação. Este procedimento fortalece significativamente a segurança do nosso sistema, protegendo-o contra acessos não autorizados e possíveis ameaças externas.

Feito por: Jorge Cunha 1200618.

# **User Story**

1. UserStory 810: Como administrador do sistema quero que seja proposta, justificada e implementada uma estratégia de cópia de segurança que minimize o RPO (Recovery Point Objective) e o WRT (Work Recovery Time).

Agendamento dos Backups:

Horários: 08:10, 12:10, 16:00 e as 20:00.

Frequência: Quatro vezes ao dia.

Duração: Aproximadamente 10 minutos por sessão.

Os horários foram escolhidos para coincidir com períodos de baixa atividade acadêmica, minimizando a interferência nas operações diárias.

Armazenamento e Segurança:

Localização: Backups armazenados em locais seguros e replicados para um repositório off-site.

Segurança: Encriptação dos dados recomendada para proteção adicional.

Natureza dos Backups:

Tipo de Backup: Full Backup.

Optou-se por backups completos devido ao volume relativamente baixo de dados (máximo de 600 Megabytes) que demorará no máximo 10 minutos.

Isso simplifica o processo de recuperação, pois não depende de backups incrementais ou diferenciais.

Recovery Point Objective (RPO):

RPO Máximo: 4 horas.

Este RPO garante que, no máximo, apenas 4 horas de trabalho serão perdidas em caso de falha do sistema, minimizando o impacto sobre as atividades acadêmicas e administrativas.

Work Recovery Time (WRT): 2h45min até 5 horas, aproximadamente.

Para estimar o tempo necessário para cada etapa no contexto de um WRT (Work Recovery Time), é importante considerar as variáveis específicas do ambiente.

Aqui estão estimativas baseadas em cenários típicos:

Instalação e Configuração do Sistema Operacional:

Tempo estimado: 30 minutos a 1 hora.

Inclui a instalação do SO, atualizações necessárias e configurações básicas.

Instalação e Configuração de um Servidor Nginx:

Tempo estimado: 15 a 30 minutos.

Inclui a instalação do Nginx e a configuração inicial.

Pode ser mais rápido se scripts de automação ou templates de configuração estiverem disponíveis.

Instalação da Base de Dados MongoDB:

Tempo estimado: 20 a 40 minutos.

Inclui a instalação do MongoDB e a configuração inicial.

O tempo pode variar com base na complexidade da configuração desejada.

Restauro da Base de Dados do Backup (600 MB):

Tempo estimado: 5 a 10 minutos.

Dependendo da velocidade da rede e do desempenho do sistema de armazenamento, o restauro de um backup de 600 MB geralmente é rápido.

Restauro e Configuração da Aplicação:

Tempo estimado: 30 minutos a 1 hora.

Este passo pode variar significativamente dependendo da complexidade da aplicação, configurações necessárias e a existência de scripts de automação.

Testes sobre o Restauro da Aplicação e Dados:

Tempo estimado: 30 minutos a 1 hora.

Os testes incluem a verificação da integridade dos dados, funcionalidade da aplicação e testes de performance.

O tempo necessário dependerá do escopo e da profundidade dos testes.

Monitoramento e Revisão:

Implementação de um sistema de monitoramento para acompanhar o sucesso dos backups.

Revisões periódicas da estratégia para adaptá-la às mudanças nas necessidades e no ambiente.

Exemplo do Backup

Uma imagem com texto, captura de ecrã

Descrição gerada automaticamente

Exemplo do Schedule (via Crontab):

Uma imagem com texto, captura de ecrã, Tipo de letra

Descrição gerada automaticamente

Melhoramento do backup

Backups Incrementais ou Diferenciais:

Embora estejamos usando backups completos, a implementação de backups incrementais ou diferenciais pode aumentar a eficiência. Estes tipos de backup armazenam apenas as alterações feitas desde o último backup completo ou incremental, reduzindo o tempo e o espaço de armazenamento necessário.

Testes de Recuperação Regulares:

Realizar testes de recuperação de dados regulares para garantir que os backups são confiáveis e podem ser restaurados com sucesso em caso de emergência.

Encriptação dos Dados:

Adicionar uma camada de segurança através da encriptação de dados, tanto em trânsito (durante a transferência para locais de armazenamento) quanto em repouso (quando armazenados no destino).

Armazenamento Offsite e na Nuvem:

Complementar o armazenamento local com soluções de armazenamento offsite e na nuvem para garantir redundância e proteção contra desastres locais.

Balanceamento de Carga e Distribuição de Recursos:

Implementar soluções de balanceamento de carga para distribuir uniformemente o uso de recursos durante os backups, evitando sobrecarga em sistemas específicos.

Auditorias e Revisões Periódicas:

Realizar auditorias e revisões periódicas dos processos de backup para identificar áreas de melhoria e ajustar a estratégia conforme necessário.

Conclusão:

A estratégia proposta equilibra a proteção dos dados com a eficiência operacional, garantindo a segurança e a integridade dos dados acadêmicos com um impacto mínimo nas atividades diárias da instituição.

Feito Por: Jorge Cunha 1200618.