UniSENAI

DEFESA CIBERNÉTICA
PROJETO APLICADO I

DOCUMENTAÇÃO TÉCNICA DO PROJETO APLICADO:

Soluções de Monitoramentos para Integridade de Backup.

EQUIPE:

GABRIEL COSME SANTOS DA SILVA

MELQUISEDEQUE DA SILVA

RÔMULO COSTA PEREIRA DA SILVA

VINICIUS OCKER FAGUNDES

PROFESSOR RESPONSÁVEL:

ISKAILER INAIAN RODRIGUES

2024

SUMÁRIO

1. Equipe e Planejamento das atividades.....3
1.1 Integrantes e funções
1.2 Cronograma do Projeto
2. Problema escolhido e Descrição.....3
2.1 Contextualização
2.2 Descrição do Problema
2.3 Impacto
2.4 Justificativa
3. Necessidades do Cliente/Usuário e Validação.....4
3.1 Perfil do Cliente/Usuário
3.2 Necessidades Identificadas
3.3 Método de Validação
3.4 Conclusões Obtidas
4. Necessidades do Cliente/Usuário e Validação.....5
4.1 Zabbix (Monitoramento)
4.2 Veeam Backup (Backup Avançado)
5. Diagrama e Descrição da Solução Proposta 5
5.1 Descrição do fluxo:
6. Conclusão e Próximos Passos.....6
6.1 Conclusão
6.2 Próximos Passos

1. Equipe e Planejamento das Atividades

1.1 Integrantes e Funções

Melquisedeque da Silva – Coordenação técnica.

Gabriel Cosme da Silva – Configuração do Veeam.

Vinicius Ocker Fagundes – Configuração do Windows Server.

Rômulo Costa Pereira da Silva – Testes de integridade.

1.2 Cronograma do Projeto

Planejamento – 1 Semana.

Configuração do Servidor BKP – 1 dias.

Configuração do Servidor Zabbix – 3 Semanas.

Testes e Ajustes – 3 Semanas.

Entrega Final – 1 Semana

2. Problema Escolhido e Descrição

2.1Contextualização:

Em um cenário empresarial cada vez mais dependente de dados, a perda de informações críticas pode causar impactos devastadores - desde interrupções operacionais e prejuízos financeiros significativos até danos irreparáveis à reputação da organização. Diante de riscos como ransomware, falhas de hardware e erros humanos, empresas de todos os portes e segmentos precisam de soluções robustas para garantir não apenas a execução regular de backups, mas principalmente a integridade e a disponibilidade desses dados quando mais se necessita. Um sistema de monitoramento contínuo se torna, portanto, componente essencial da estratégia de continuidade de negócios, transformando o backup de um mero procedimento técnico em um ativo estratégico que protege o valor da informação corporativa.

2.2 Descrição do Problema:

O verdadeiro desafio na gestão de backups não está na criação das cópias, mas na invisibilidade sobre sua integridade. Muitas empresas descobrem que seus sistemas de backup falharam apenas no momento crítico de recuperação, quando já é tarde demais. Essa falta de visibilidade transforma o que deveria ser uma rede de segurança em uma falsa sensação de proteção, deixando organizações vulneráveis mesmo quando acreditam estar resguardadas.

2.3 Impacto:

A perda de dados vai além da interrupção operacional - ela compromete relações com clientes, mancha reputações construídas ao longo de anos e paralisa a capacidade de decisão estratégica. Transformando cada minuto de indisponibilidade em perdas concretas e danos que podem se tornar irreversíveis para o negócio.

2.4 Justificativa:

Monitorar a integridade de backups é como verificar regularmente os extintores de incêndio - a maioria nunca será usado, mas quando for necessário, precisam funcionar perfeitamente. Essa vigilância constante transforma dados em ativos confiáveis. Não se trata apenas de evitar falhas, mas de garantir que toda a organização possa seguir em frente sem o fantasma da perda repentina de informações essenciais.

3. Necessidades do Cliente/Usuário e Validação

3.1 Perfil do Cliente/Usuário:

Empresas que necessitam de monitoramento proativo de backups em ambientes Windows, com:

Infraestrutura local ou virtualizada
Requisitos de conformidade e auditoria
Necessidade de reduzir tempo de recuperação de dados.

3.2 Necessidades identificadas:

Necessidade 1: Garantia de integridade

Dashboard Zabbix com índice de integridade (0-100%) e alertas em tempo real.

Validação – Testes de recuperação simulada com arquivos corrompidos/intactos.

Necessidade 2: Redução de riscos

Monitoramento contínuo de jobs do Windows Server Backup e HD externo

Validação – Monitoramento contínuo de jobs do Windows Server Backup e HD externo.

Necessidade 3: Conformidade

Relatórios automatizados para auditoria.
Validação – Check-list baseado em ISO 27001 e LGPD

Necessidade 4: Recuperação rápida

Métricas de tempo de backup/restore no Zabbix
Validação – Simulações de disaster recovery

Necessidade 5: Visibilidade centralizada

Dashboard unificado com métricas críticas
Validação – Avaliação por usuários finais (equipe de TI)

3.3 Método de validação:

Falhas simuladas em backups (arquivos excluídos/corrompidos).

Verificação de alertas no Zabbix e tempo de detecção.

3.4 Conclusões obtidas:

A invisibilidade na integridade dos backups representa um risco crítico, exigindo monitoramento contínuo e métricas bem definidas. Para ser eficaz, a solução precisa incorporar critérios de verificação (como checksum e disponibilidade do HD externo), aliados a relatórios de conformidade e mecanismos de alerta proativos no Zabbix, garantindo não apenas a execução, mas a confiabilidade dos backups quando mais importa.

4. Tecnologias Escolhidas e Justificativa

4.1 Zabbix (Monitoramento)

Monitoramento em tempo real do status do backup (sucesso/falha), espaço em disco e saúde do HD externo.

Funciona bem com Windows sem deixar o servidor lento.

Dashboard fácil de usar que mostra:

Histórico de backups (índice de integridade 0-100%)

Tempo de execução dos backups

Espaço disponível no HD

4.2 Veeam Backup (Backup Avançado)

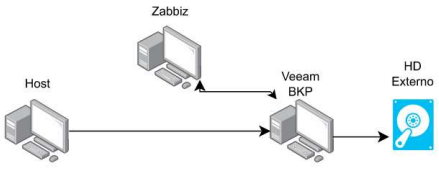
Verifica automaticamente se o backup está bom (testa restaurar arquivos).

Criptografa os backups (protege contra roubo de dados).

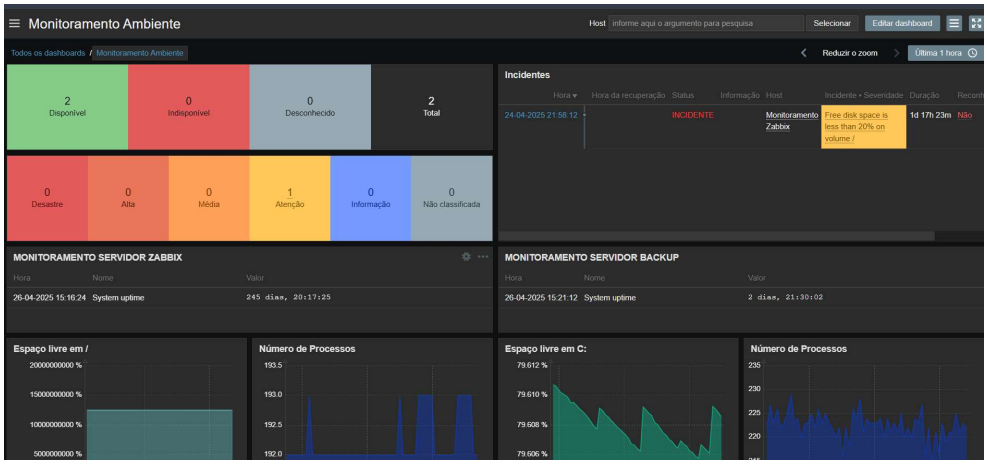
Pode substituir o Windows Server Backup se precisar de mais recursos.

5. Diagrama e Descrição da Solução Proposta

Diagrama do projeto:



Proposta do dashboard:



5.1 Descrição do fluxo:

Zabbix (em seu host dedicado):

monitora todos os hosts da rede, incluindo o Host AD e o Host Veeam.

Veeam Backup (em seu host próprio):

Executa backups do Host AD (Active Directory) e do Host Zabbix.

Armazena os backups em um HD Externo conectado fisicamente a este host.

Interdependências:

O Zabbix verifica o status do serviço Veeam e a disponibilidade do HD Externo.

O Veeam protege até mesmo o host onde o Zabbix está instalado, garantindo redundância.

Observações:

O HD Externo é acessível apenas pelo host do Veeam (conexão física/direta).

Setas indicam direção do monitoramento (Zabbix) e do fluxo de backup (Veeam).

6. Conclusão e Próximos Passos

6.1 Conclusão

A solução proposta, baseada em Zabbix + Veeam, oferece um sistema completo para:

Garantir a integridade dos backups através de monitoramento contínuo.

Reduzir riscos com alertas proativos e relatórios mensais automatizados.

A combinação dessas tecnologias proporciona segurança, visibilidade e controle sobre os dados corporativos, transformando o backup de uma tarefa operacional em um processo estratégico.

6.2 Próximos Passos

Instalar e configurar o Zabbix Server para monitoramento.

Configurar o Windows Server Backup para backups semanais no HD externo.