**Forma

Descrição gerada automaticamente com confiança média**

**MICROINFORMÁTICA**

**Relatório de Falhas na**

**Aplicação de GPOs em Grupos do Domínio**

Autor: Darlan Henrique de Souza Oliveira

Equipe Responsável:

Engenheiro de Redes: **Ricardo Augusto L. Garcia Gonçalves**

Engenheiro de Redes: **Cleverson Alexandre Zocca**

Tech Lead II: **Tiago Henrique Pezato**

Gestor: **Gabriel Magarotti Moutinho**

Sorocaba – SP

01/06/2023

1. **EXPLICAÇÃO DO PROBLEMA**

Recentemente estão ocorrendo muitos problemas com a aplicação de GPOs nas máquinas de todos os modelos, onde ao tentar aplicar a GPO “forçadamente” com o comando **gpupdate** e/ou **gpupdate /force**,há um retorno de erro onde o ID da GPO não corresponde a nenhum ID existente na pasta, “\\grupo-sorocred.br\sysvol\grupo-sorocred.br\Policies{%ID%}\gpt.ini”, portanto impede que as políticas da máquina atualizem e que o pleno funcionamento e configuração da máquina por parte da microinformática não ocorra de forma eficiente, o que acarreta em atrasos no prazo da SLA e um enorme retrabalho ao tentar resolver superficialmente um possível problema de raiz.

1. **ANÁLISE DO CASO**

Contextualizado no item um, a seguir haverá figuras que exemplificam os problemas ocorridos, na figura 1 e 2 é mostrado o maior problema da não aplicação das GPOs, onde impede que façamos as devidas configurações na máquina.

Figura 1 – tentativa de login com os computadores que não aplicam a política.

Interface gráfica do usuário

Descrição gerada automaticamente

Fonte: própria autoria (VNCViewer, 2023).

Figura 2 – Erro ao tentar utilizar um usuário da rede com mais permissões (com o user local “sete” funciona).

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

Fonte: própria autoria (VNCViewer, 2023).

Após essa limitação, o mais lógico seria prosseguir para tentar atualizar a política de grupo manualmente, o que acarreta ao erro exemplificado pelas figuras 3 e 4, que são duas máquinas diferentes, porém apresentam o mesmo erro - com IDs de GPO diferentes -, a terceira está com o CMD sem elevar e a quarta está com o CMD elevado para que se prove que a falha se repete em computadores em grupos diferentes e que o privilégio não altera o problema.

Figura 3 – política de computador não foi aplicada.

Texto

Descrição gerada automaticamente

Fonte: própria autoria (VNCViewer, 2023).

Figura 4 - Testando com o CMD elevado (user sete) ocorre o mesmo erro.

Texto

Descrição gerada automaticamente

Fonte: própria autoria (VNCViewer, 2023).

O ID da política de grupo que o comando “gpupdate” tenta achar, não existe no endereço, o que ocasiona essas falhas, mais a frente irá ser apresentado teorias do possível problema que ocasiona a isso.

Figura 5 – Buscando a referência de ID da figura 3 no endereço de pesquisa, porém sem sucesso pois é inexistente.

Tabela

Descrição gerada automaticamente

Fonte: própria autoria (VNCViewer, 2023).

1. **POSSÍVEIS CAUSAS**

Uma possível causa seria uma GPO desatualizada nos grupos do domínio **grupo-sorocred.br**\Site\_XV\Departamentos\.

Neste caso, os grupos a serem verificados primeiro seriam o “%domínio%\TI\Seguranca” e “%domínio%\Renegociacao”, pois foram os reportados neste relatório.

Verificar se existe ou já existiu, e o que a GPO do ID da figura 3 **“{7BC52E3E-3438-464C-B5B7-158A0A5AFDAD}**” faz, usando o AD Admin, e ver se o arquivo GPT.ini está funcionando corretamente ou se apagando a GPO em um grupo teste o erro deixará de ocorrer.

Verificar se existe ou já existiu, e o que a GPO do ID da figura 4 **“{E5CDFCD4-DC20-418A-BCDC-4E621E52E265}**” faz, usando o AD Admin, e ver se o arquivo GPT.ini está funcionando corretamente ou se apagando a GPO em um grupo teste o erro deixará de ocorrer.

Outra possível causa do problema, é que quando a máquina entra no domínio pega as GPOs “gerais”, e nessas antes de movimentar podem estar essas desatualizadas, e quando a máquina é movimentada ela ainda tenta puxar uma GPO que não mais existe em seu grupo, impedindo que as outras sejam aplicadas pois há um conflito.

A última coisa que foi teorizada é verificar se o arquivo gpt.ini tem as permissões corretas para que o sistema possa lê-lo. Talvez a conta do usuário ou grupo não tenha permissões de leitura para o arquivo.

Nota

**Desde já agradeço pelos ensinamentos e suporte do Engenheiro Cleverson Alexandre Zocca, que despertou a curiosidade e vontade de me aprofundar na área de infraestrutura.**