ATIVAÇÃO DO TESTE DE CONTINGÊNCIA

1) TROCA DO IP NAS CONFIGURAÇÕES DA PLACA DE REDE.

Mudar a configuração da placa de rede para o IP do servidor de produção –> 1.0.1.1 .

2) INICIALIZAÇÃO DO DOMINO.

Executar os comandos abaixo para carregar o serviço do Domino:

cd /local/notesdata <ENTER>
/opt/ibm/domino/bin/server <ENTER >

Comando para baixar o serviço do Domino: quit <enter>

3) PARA INICIAR OU PARAR O SERVIÇO DO DOMINO UTILIZE UM DOS COMANDOS ABAIXO:

service domino start
service domino stop

4) RESTAURAÇÃO.

Restaure uma cópia de segurança do diretório notesdata no caminho /local do novo servidor. Após a cópia do diretório, execute os comandos listados abaixo para adicionar as permissões de acesso nos diretórios para que SiGDEM 2.0 funcione corretamente.

1. Abra o terminal;
2. Digite o comando cd /local/notesdata <Enter>;
3. Digite o comando chmod -R 755 * <Enter>; e
4. Digite o comando chown -R notes:notes * <Enter>;

5- ALTERNAR AS TELAS ENTRE O MODO GRÁFICO, TERMINAL E O CONSOLE DO DOMINO:

DOMINO - CTRL + ALT + F12
MODO GRÁFICO – ALT + F1
TERMINAL - CTRL + ALT + F1

6- ATENTAR PARA DESABILITAR O SELinux.

Security-Enhanced Linux (SELinux) é uma arquitetura de segurança para sistemas Linux® que permite aos administradores mais controle sobre quem pode acessar o sistema. Ele foi originalmente desenvolvido pela Agência de Segurança Nacional (NSA) dos Estados Unidos como uma série de patches para o kernel do Linux usando módulos de segurança do Linux (LSM).

A desativação do SELinux usando a opção `SELINUX=disabled` no `/etc/selinux/config` resulta em um processo no qual o kernel inicia com o SELinux ativado e muda para o modo

desativado mais tarde no processo de inicialização. Como podem ocorrer vazamentos de memória e condições de corrida causando pânico no kernel, prefira desativar o SELinux adicionando o parâmetro `selinux=0` à linha de comando do kernel.

Procedimento

1. Abra o arquivo `/etc/selinux/config` em um editor de texto de sua escolha, por exemplo:

   ```
   # vi /etc/selinux/config
   ```

2. Configure a opção `SELINUX=disabled`:

   ```
   # This file controls the state of SELinux on the system.
   # SELINUX= can take one of these three values:
   #       enforcing - SELinux security policy is enforced.
   #       permissive - SELinux prints warnings instead of enforcing.
   #       disabled - No SELinux policy is loaded.
   SELINUX=disabled
   # SELINUXTYPE= can take one of these two values:
   #       targeted - Targeted processes are protected,
   #       mls - Multi Level Security protection.
   SELINUXTYPE=targeted
   ```

3. Salve a mudança, e reinicie seu sistema:

   ```
   # reboot
   ```

Etapas de verificação

1. Após reiniciar, confirme que o comando `getenforce` retorna `Disabled`:

   ```
   $ getenforce
   Disabled
   ```

7- TEMPO DE DURAÇÃO DA FAINA.
Aproximadamente 3hs ou mais.