**. Preparação Inicial:**

Antes de iniciar a migração, faça uma análise completa de sua infraestrutura atual para entender todas as dependências e requisitos. Certifique-se de ter acesso à AWS e os privilégios necessários para configurar os serviços relevantes.

* Documente todas as configurações do servidor Cerberus, incluindo usuários, permissões, configurações de segurança e configurações de diretórios.
* Identifique os sistemas e aplicativos que dependem do SFTP Cerberus para garantir que eles funcionem sem problemas após a migração.

**2. Configuração do Serviço AWS SFTP:**

A AWS oferece um serviço gerenciado de SFTP chamado AWS Transfer for SFTP. Você deve configurá-lo primeiro.

* Acesse o Console da AWS e navegue até o AWS Transfer for SFTP.
* Crie um novo servidor SFTP e configure as opções de segurança e permissões de acordo com seus requisitos. Certifique-se de criar os usuários SFTP necessários.
* Configure grupos de usuários e políticas de permissões para corresponder à sua configuração atual do Cerberus.
* Use a AWS Identity and Access Management (IAM) para gerenciar permissões adicionais, se necessário.
* Crie diretórios raiz e defina políticas de acesso a esses diretórios de acordo com as configurações existentes do Cerberus.

**3. Preparação do Ambiente de Transferência:**

* Prepare seu servidor AWS com as configurações necessárias, incluindo segurança, grupos de segurança e permissões IAM para permitir a comunicação SFTP com o AWS Transfer for SFTP.
* Instale quaisquer dependências ou aplicativos que você precise no servidor AWS para suportar os processos de transferência de arquivos.

**4. Migração dos Dados:**

* Mova os dados do servidor Cerberus para o novo servidor AWS Transfer for SFTP. Você pode usar ferramentas como **rsync**, **scp** ou outras opções que preferir.
* Certifique-se de preservar as estruturas de diretório e permissões durante a migração.

**5. Teste e Validação:**

* Teste a funcionalidade do novo ambiente SFTP na AWS, verificando se os usuários têm acesso aos arquivos corretos e se as configurações de segurança estão funcionando conforme o esperado.
* Execute testes de integração com os sistemas e aplicativos dependentes para garantir que a migração não cause interrupções.

**6. Redirecionamento DNS/Alteração de Configurações:**

* Atualize as configurações DNS ou qualquer configuração de redirecionamento que direcione o tráfego SFTP para o servidor AWS em vez do servidor Cerberus on-premise.

**7. Monitoramento e Manutenção:**

* Implemente soluções de monitoramento e alerta para rastrear o desempenho e a integridade do seu ambiente SFTP na AWS.
* Crie planos de backup e recuperação de dados para garantir a disponibilidade contínua dos arquivos.

**8. Documentação e Treinamento:**

* Atualize a documentação interna para refletir as mudanças na infraestrutura.
* Forneça treinamento aos membros da equipe que precisarão gerenciar o ambiente SFTP na AWS.

**9. Finalização da Migração:**

* Após testar e verificar que tudo está funcionando conforme o esperado, você pode finalizar a migração, desativando o servidor Cerberus on-premise, se aplicável.

Lembre-se de que a migração pode ser complexa, e é importante realizar um planejamento detalhado, envolvendo todas as partes interessadas, para garantir uma transição suave. Além disso, faça um backup completo de todos os dados críticos antes de iniciar a migração para evitar perda de dados inesperada.

Mapear o ambiente SFTP Cerberus é uma parte fundamental do processo de migração, pois permite entender todas as configurações e dados que você precisa transferir para o ambiente AWS. Abaixo, estão detalhados os principais aspectos que você precisa mapear do seu servidor SFTP Cerberus:

**1. Usuários e Grupos:**

* Liste todos os usuários SFTP que têm acesso ao servidor Cerberus.
* Identifique a que grupos esses usuários pertencem, se aplicável.
* Registre as permissões de acesso para cada usuário ou grupo, incluindo permissões de leitura, gravação e execução em diretórios específicos.

**2. Configurações de Segurança:**

* Anote as políticas de segurança configuradas no Cerberus, como políticas de senha, requisitos de autenticação multifatorial (MFA), políticas de bloqueio de contas, etc.

**3. Diretórios e Estrutura de Arquivos:**

* Mapeie a estrutura de diretórios do servidor Cerberus, incluindo diretórios raiz e subdiretórios.
* Registre as permissões de acesso para cada diretório.
* Liste todos os arquivos importantes que estão armazenados no servidor Cerberus.

**4. Regras e Automação:**

* Identifique quaisquer regras de automação ou scripts que estão em execução no Cerberus para processamento de arquivos.
* Liste os gatilhos que acionam esses scripts (por exemplo, novos arquivos são detectados em um diretório específico).

**5. Configurações de Rede:**

* Anote as configurações de rede, como portas de serviço usadas pelo Cerberus, endereços IP permitidos para acesso, configurações de firewall e regras de NAT (Network Address Translation).

**6. Logs e Auditoria:**

* Registre as configurações de logging e auditoria do Cerberus. Isso inclui onde os logs são armazenados e quais eventos são registrados.

**7. Configurações de Integração:**

* Identifique quaisquer integrações ou conexões de banco de dados que o Cerberus usa para processamento de arquivos.
* Liste quaisquer configurações de notificação ou alerta.

**8. Certificados e Chaves:**

* Anote informações sobre certificados SSL/TLS usados para proteger as conexões SFTP.
* Certifique-se de que você tem acesso às chaves privadas associadas a esses certificados.

**9. Scripts de Migração:**

* Se você planeja usar scripts para automatizar a migração de dados, crie ou obtenha scripts que ajudem a exportar os dados do Cerberus e importá-los para o ambiente AWS.

**10. Dependências de Aplicativos:**

* Identifique quais aplicativos ou sistemas dependem dos dados no servidor Cerberus, para garantir que as integrações sejam atualizadas ou reconfiguradas após a migração.

**11. Políticas de Retenção de Dados:**

* Registre as políticas de retenção de dados que estão em vigor no Cerberus, especificando quanto tempo os arquivos são mantidos e como eles são descartados quando não mais necessários.

Certificar-se de que você tenha um mapeamento completo de todos esses elementos é essencial para garantir uma migração bem-sucedida e a transição suave para o ambiente SFTP na AWS. Esse mapeamento servirá como guia durante o processo de configuração do serviço AWS Transfer for SFTP e a migração de dados.

**1. Avaliação Inicial:**

* Faça uma análise detalhada do ambiente Cerberus existente, documentando configurações, usuários, diretórios e políticas de segurança.

**2. Configuração AWS Transfer for SFTP:**

* Acesse o Console da AWS e configure um novo servidor SFTP usando o serviço AWS Transfer for SFTP.
* Crie grupos de usuários e configure políticas de permissão para corresponder à configuração do Cerberus.

**3. Migração de Dados:**

* Mova os dados do Cerberus para o AWS Transfer for SFTP, preservando estruturas de diretórios e permissões. Você pode usar o próprio serviço AWS Transfer for SFTP para fazer isso.

**4. Teste e Validação:**

* Teste o novo ambiente SFTP na AWS para garantir que os usuários tenham acesso adequado aos arquivos e que a segurança esteja configurada corretamente.

**5. Redirecionamento DNS/Configuração:**

* Atualize as configurações DNS ou redirecione o tráfego SFTP para o novo servidor AWS Transfer for SFTP.

**6. Monitoramento e Manutenção:**

* Implemente monitoramento e alertas para o ambiente SFTP da AWS e configure planos de backup e recuperação, conforme necessário.

**7. Documentação e Treinamento:**

* Atualize a documentação interna e forneça treinamento à equipe sobre como usar o AWS Transfer for SFTP.

**8. Finalização da Migração:**

* Após testar e validar, finalize a migração e desative o servidor Cerberus on-premise, se aplicável.

Lembre-se de que o AWS Transfer for SFTP é um serviço gerenciado que cuida de grande parte da configuração e manutenção, tornando a migração mais simples em comparação com a implantação de um servidor SFTP em uma instância EC2. Certifique-se de configurar corretamente as políticas de permissão no AWS Transfer for SFTP para corresponder às configurações do Cerberus e teste exaustivamente antes de desativar o ambiente on-premise para garantir uma transição suave.

Parte superior do formulário