Configurar Proteção de Dados no Hyperflex

Contents

Introdução

Este documento descreve como configurar a replicação no Hyperflex.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

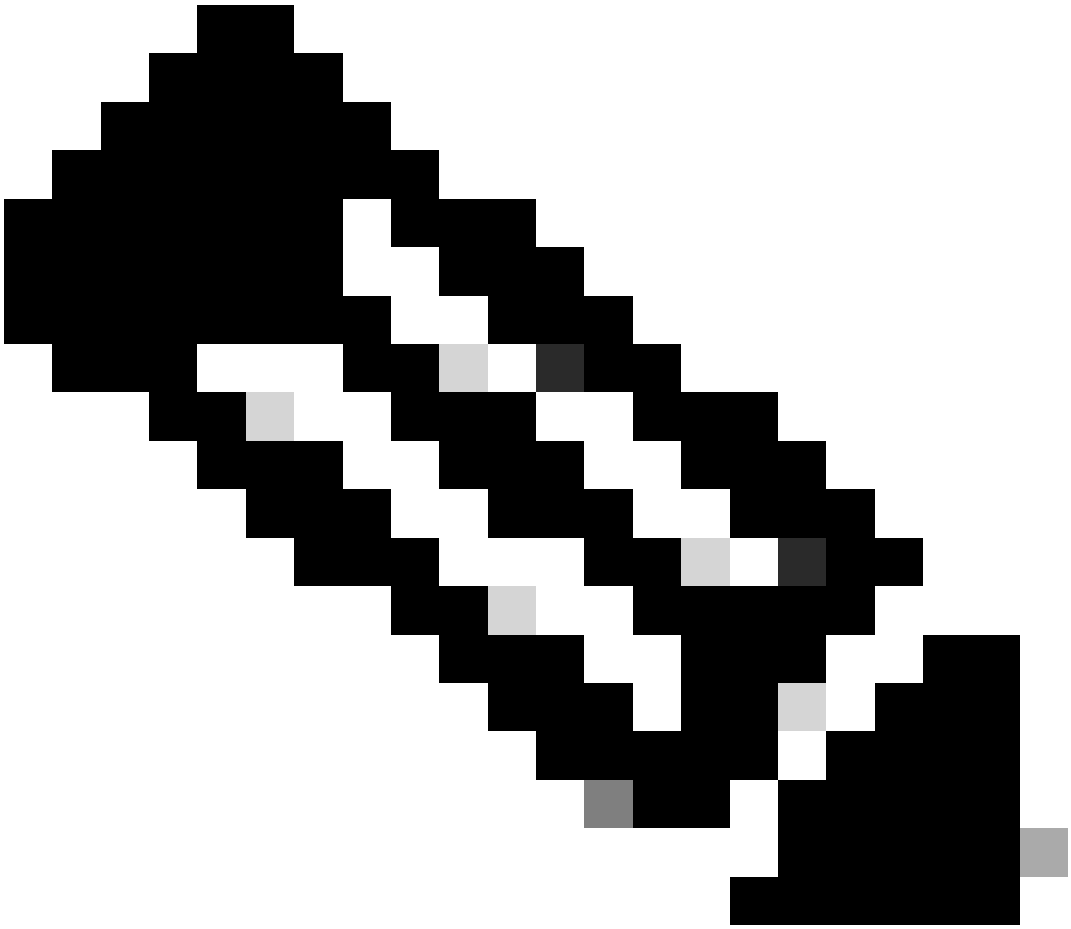
- Gerenciador do Unified Computing System (UCSM)
- HyperFlex
- vCenter
- Redes
- DNS

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- HyperFlex Connect 5.0.2d
- Cluster de Ampliação Hyperflex

- Cluster Padrão Hyperflex
- UCSM 4.2(1l)
- vCenter 7.0 U3



> Observação: para que a proteção de dados seja necessária para ter a mesma versão do Hyperflex Data Platform em ambos os clusters, o cluster pode ser diferente em tamanho e tipo.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A proteção de dados Hyperflex oferece um plano de recuperação de desastres. Ele permite que você tenha snapshots automáticos que são replicados para o cluster remoto. Os instantâneos das

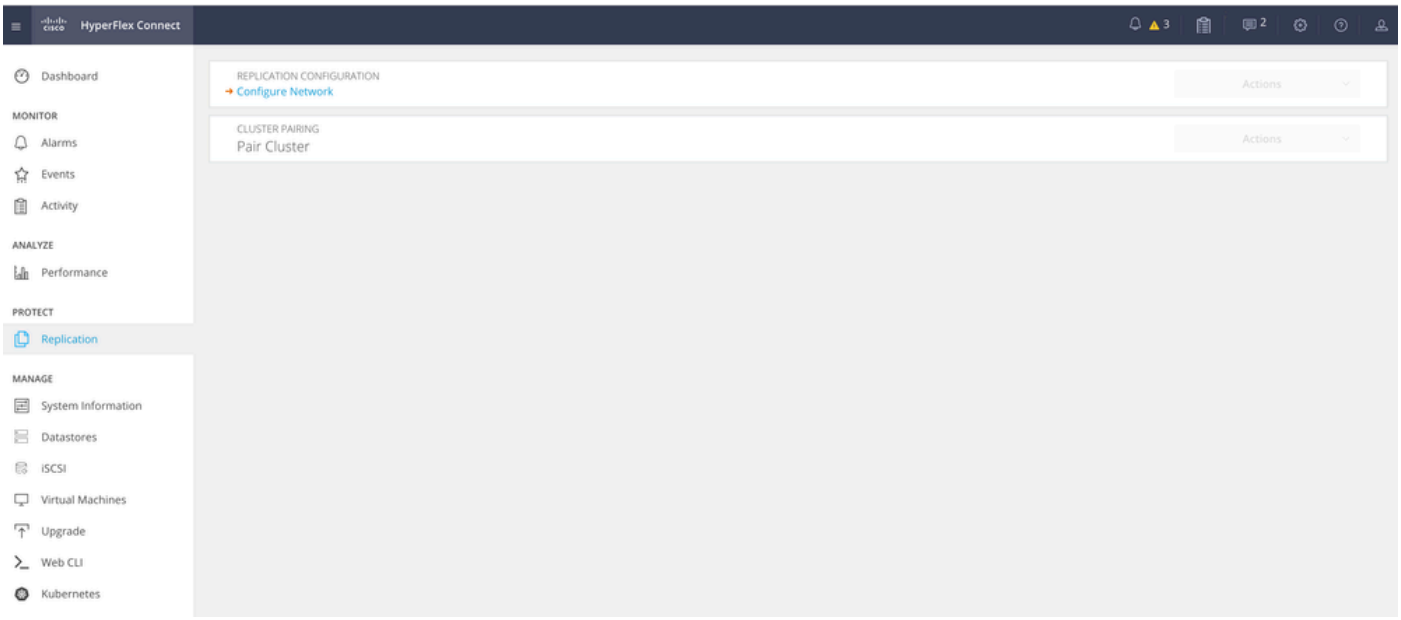
máquinas virtuais protegidas são enviados para o cluster remoto, dependendo da frequência configurada no cluster. No entanto, apenas o instantâneo obtido mais recentemente permanece no cluster de destino.

Informações adicionais de apoio

- É uma prática recomendada ao configurar o intervalo de IPs para alocar mais IPs do que os nós presentes no cluster, caso uma expansão seja planejada para o futuro.
- O MTU deve ser o mesmo em ambas as extremidades.
- A rede de replicação deve usar a mesma sub-rede IP em ambos os clusters na mesma VLAN.

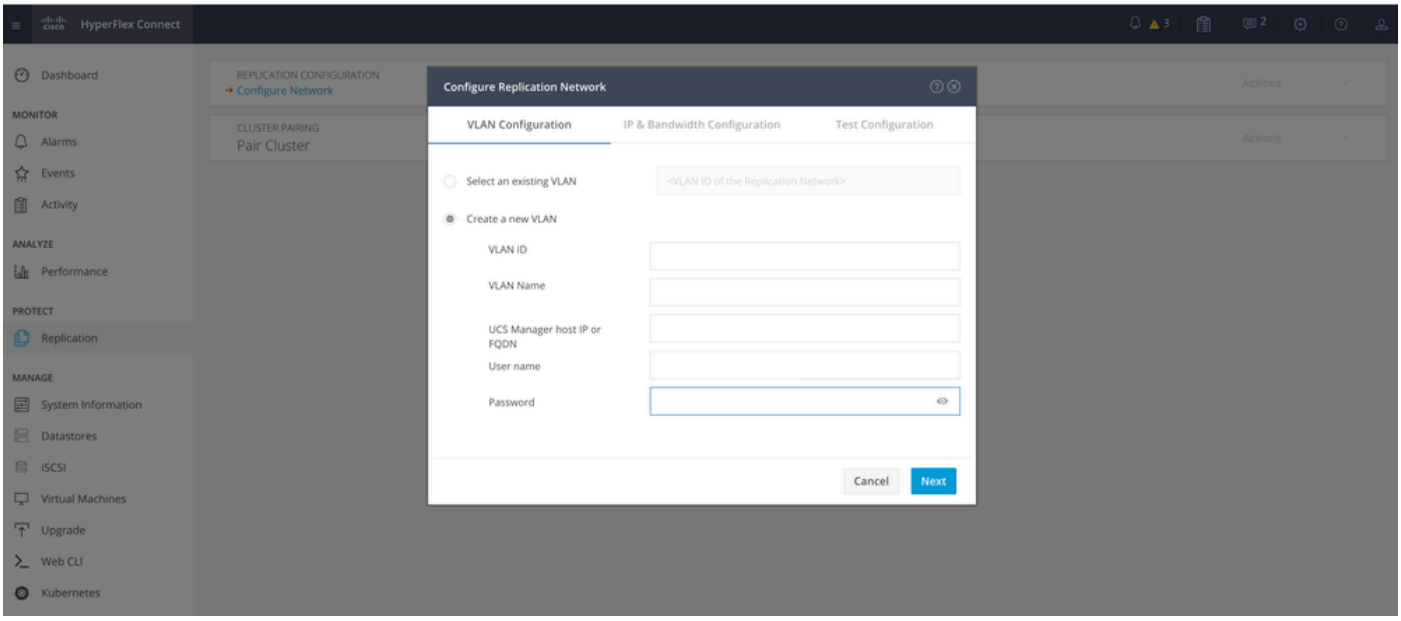
Procedimento

Etapa 1. Efetue login no sistema Hyperflex e vá para a opção Replication no painel de ação à esquerda:



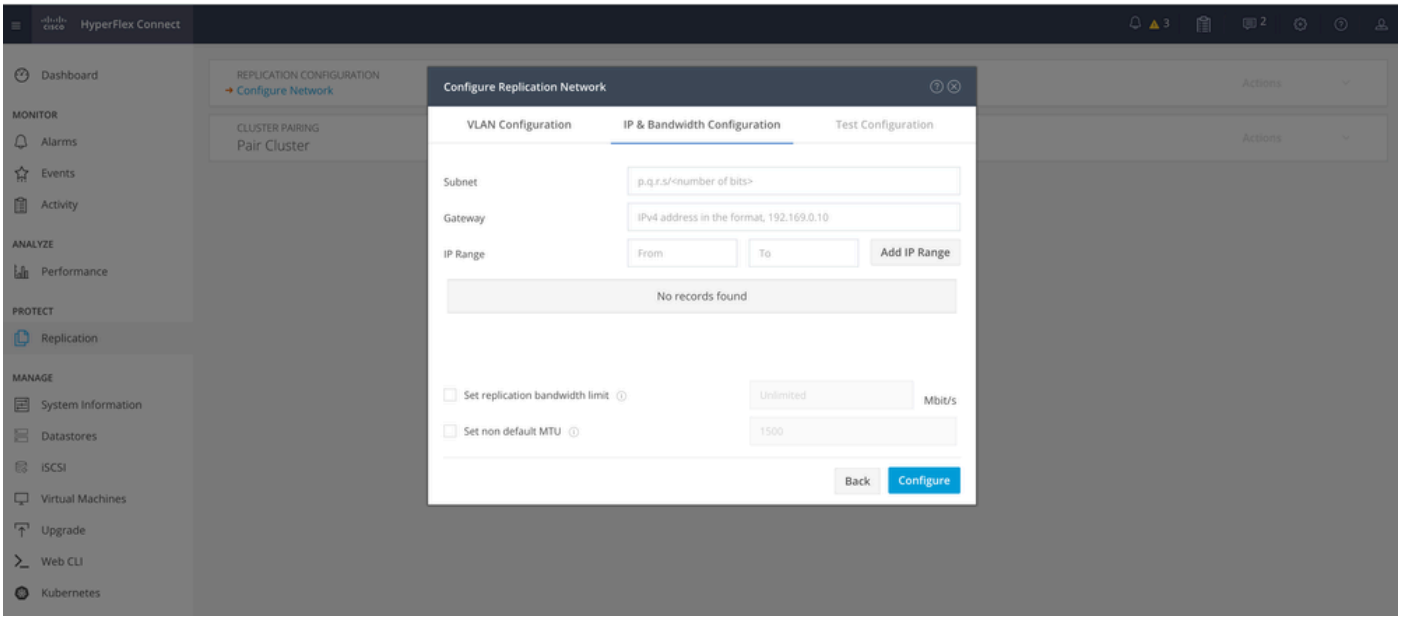
Opção de replicação

Etapa 2. Clique na opção Configure Network, preencha as informações para cada um dos campos e clique em Next:



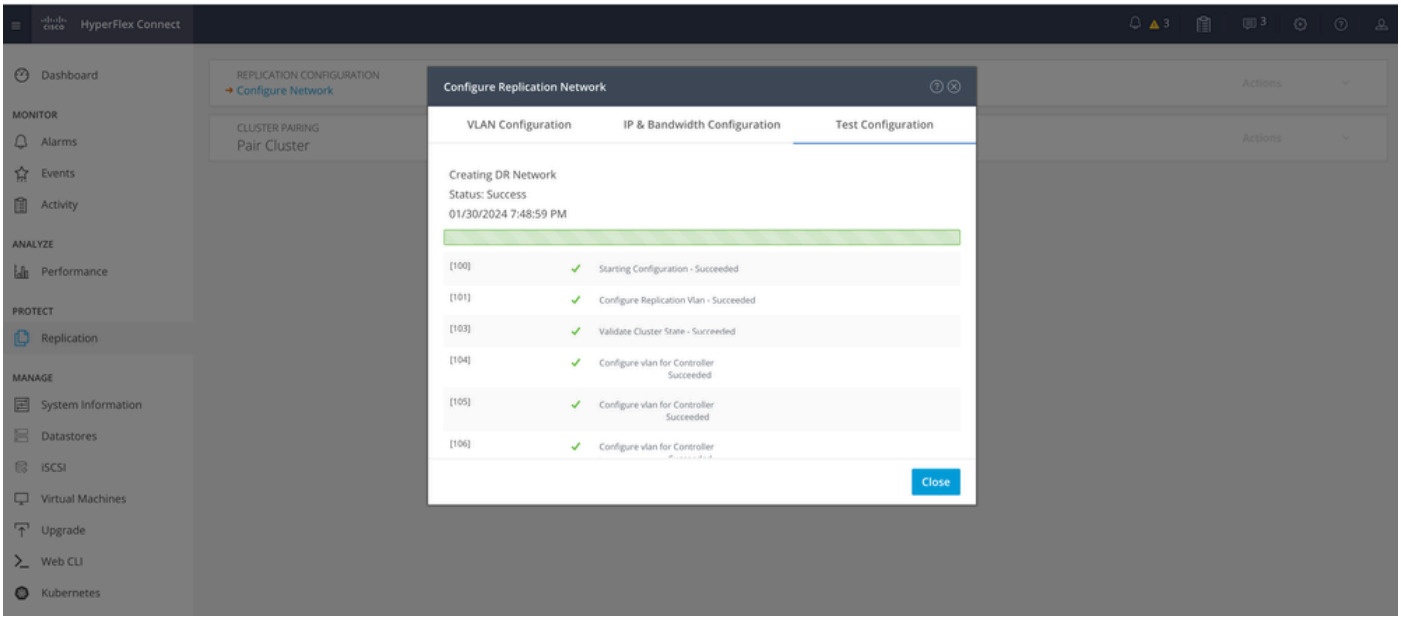
Configurar Rede de Replicação

Etapa 3. Definir as informações de IP para a rede de replicação, adicionando a sub-rede, o gateway e o intervalo de IP. Depois que o intervalo de IPs for atribuído, clique em Add IP Range e em Configure.



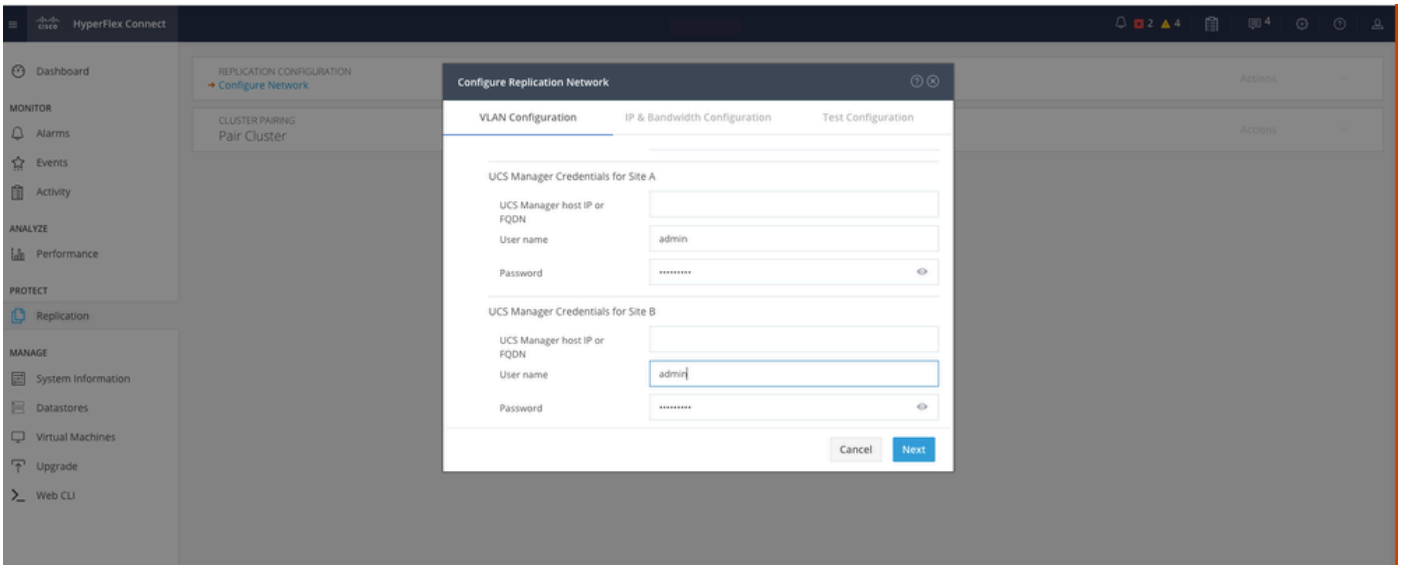
Configurar Rede de Replicação

Etapa 4. A configuração é validada e aplicada. Depois de concluída, clique em Fechar:



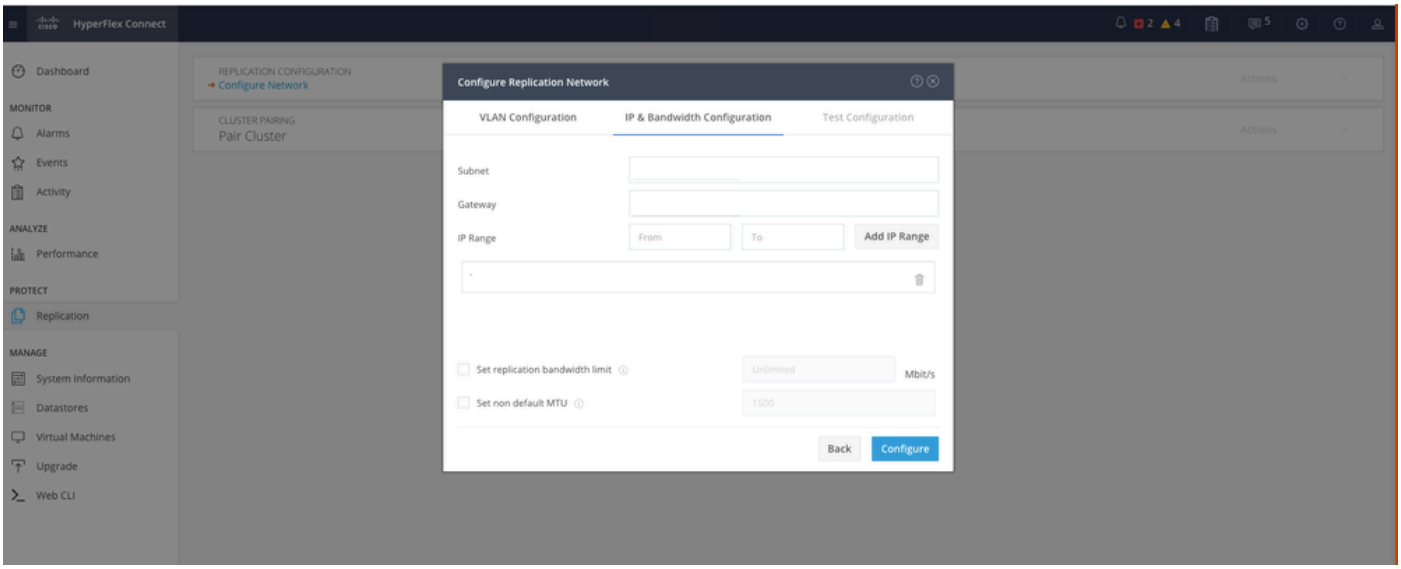
Configuração de Rede DR

Etapa 5. Configure a rede no outro cluster. Para este exemplo, o segundo cluster é ampliado, portanto, ambas as credenciais UCSM são necessárias. Preencha as informações conforme aplicável e clique em Avançar:



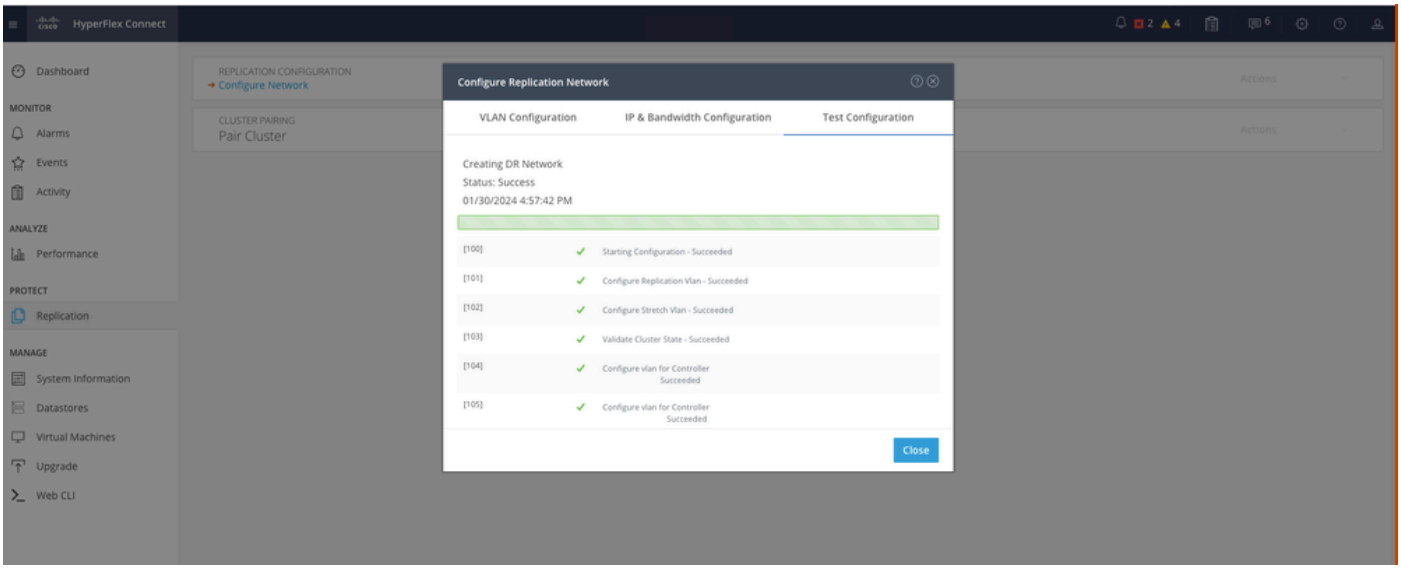
Configuração de Rede do Segundo Cluster

Etapa 6. Defina as informações de IP para a rede de replicação no segundo cluster, adicionando a mesma sub-rede, gateway e intervalo de IP. Depois que o intervalo de IPs for atribuído, clique em Add IP Range e em Configure:

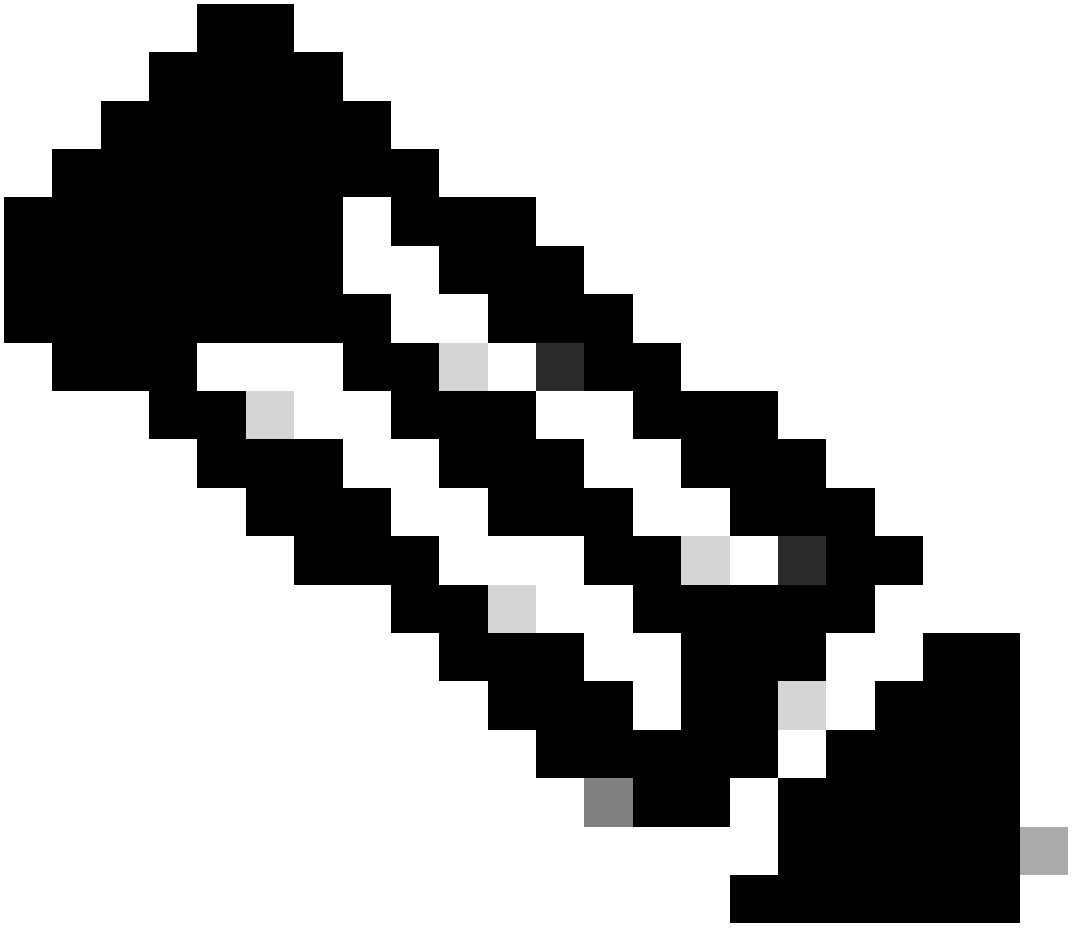


Configurando o segundo cluster da rede

Passo 7. Quando a configuração estiver concluída, um status de êxito será exibido e clique em Close:

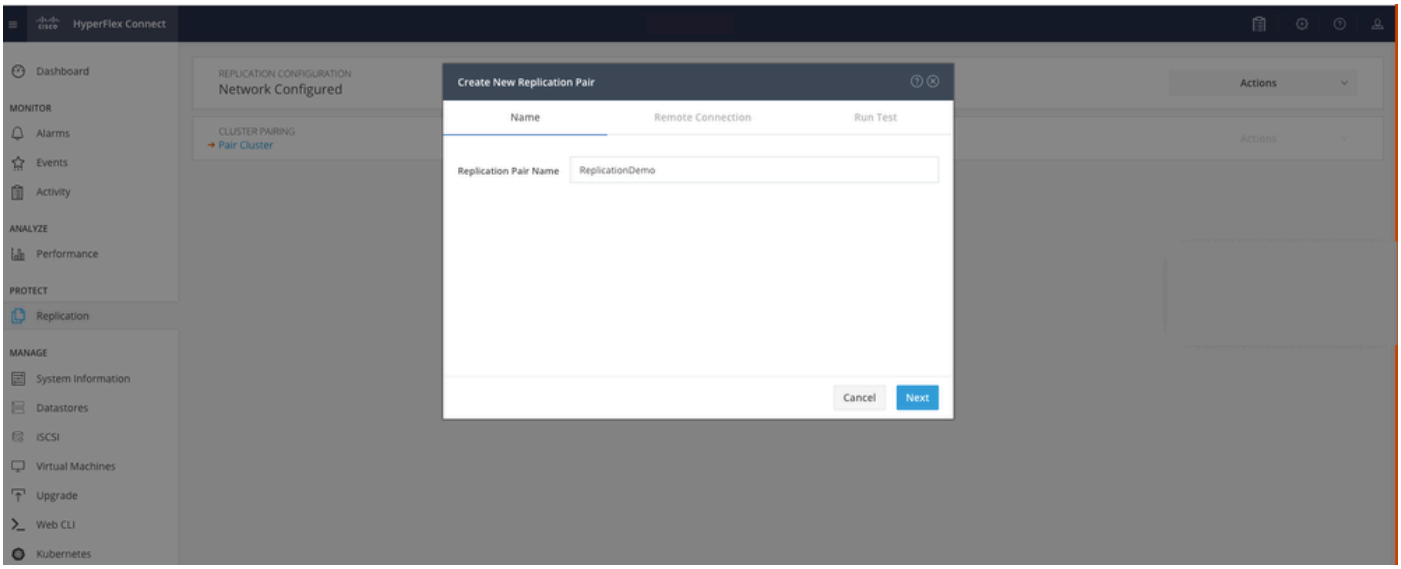


Segundo cluster de configuração de rede de DR



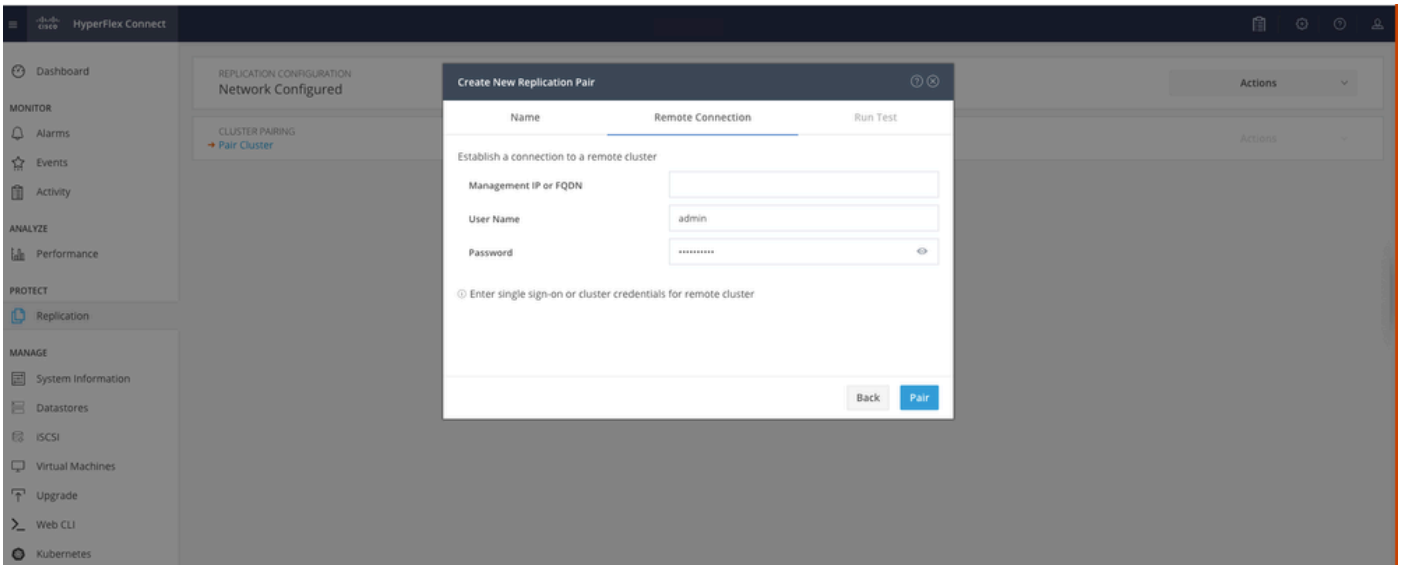
Observação: depois que a rede é configurada, é uma prática recomendada fazer um teste de rede entre os dois clusters para confirmar se eles conseguem se comunicar. Use o ping para testar a alcançabilidade de IPs entre as interfaces eth2.

Passo 7. Criando o par de replicação, clique em Replicação e clique em Par Cluster na opção Emparelhamento de Cluster. Atribua um nome para o Nome do Par de Replicação e clique em Avançar:



Par de Replicação

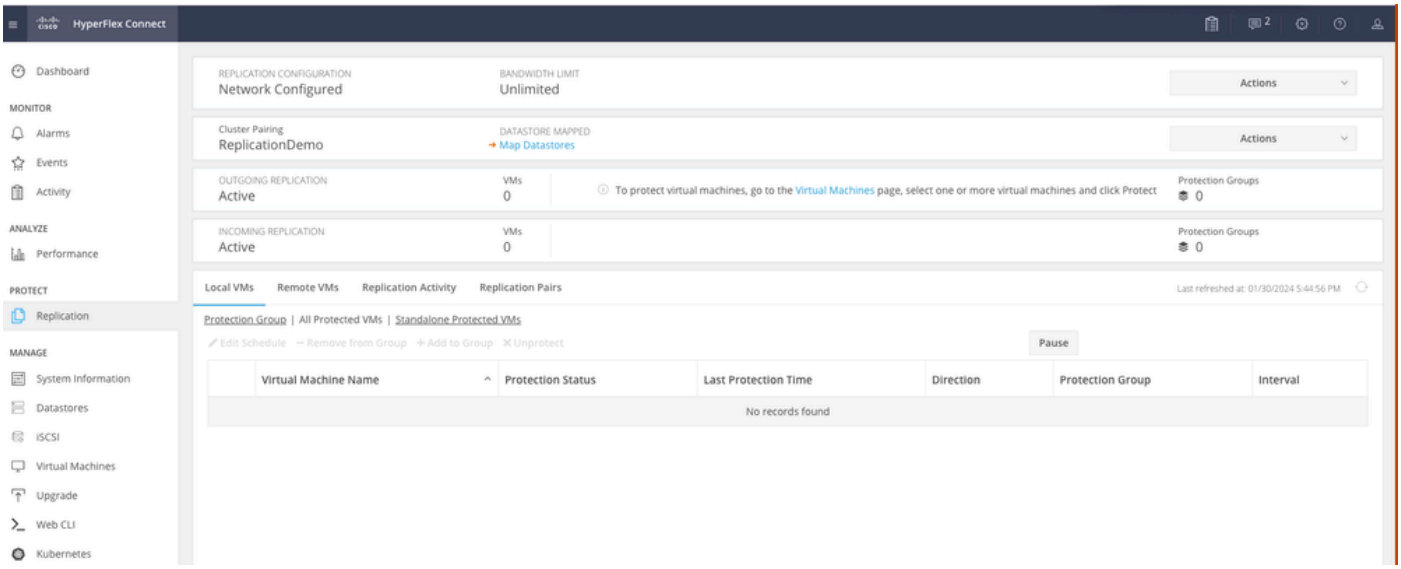
Etapa 8. Forneça o IP de Gerenciamento de cluster ou o FQDN para que o cluster seja o par de replicação e clique em Par:



Emparelhando Cluster

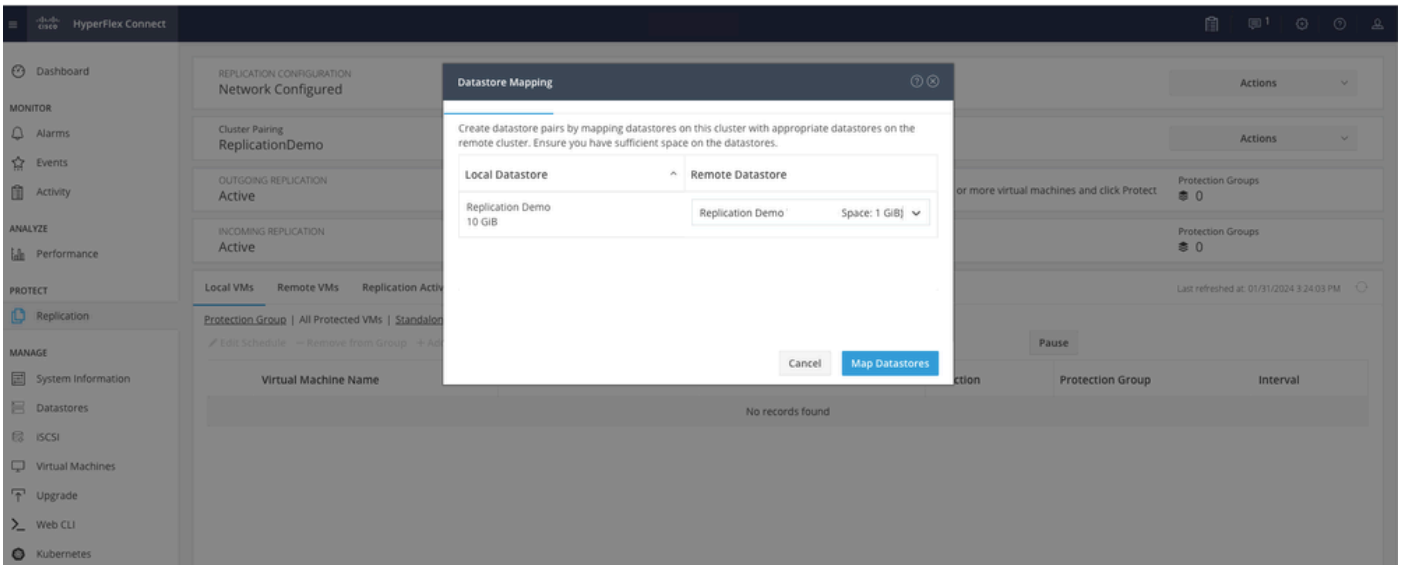
m

Etapa 8. Quando os clusters estiverem emparelhados, tudo será definido para iniciar o mapeamento do armazenamento de dados entre os dois clusters, na mesma página de replicação. A opção Map Datastore aparece, clique nela:

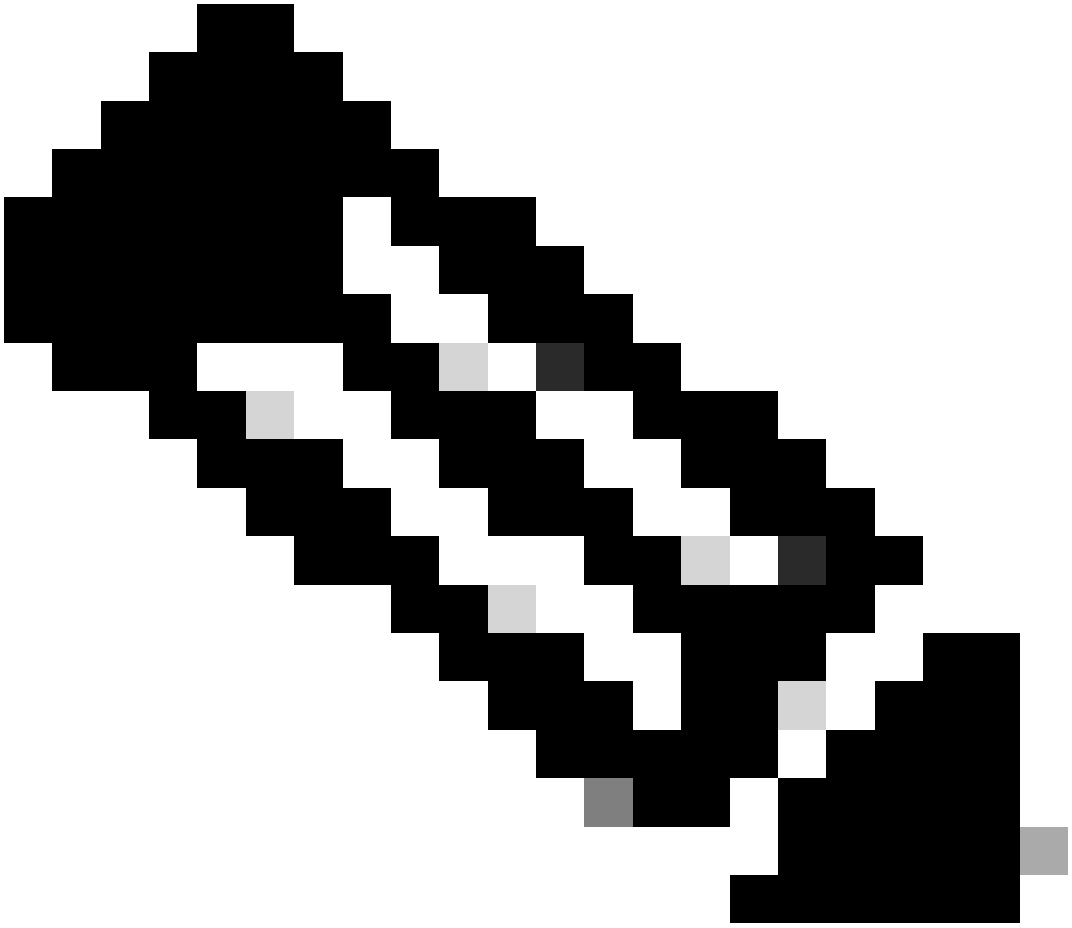


Mapeando Armazenamento de Dados

Etapa 9. Na janela pop-up, Datastore Mapping é exibido, mostrando os datastores disponíveis no cluster à esquerda e um menu suspenso com os datastores disponíveis no cluster emparelhado onde as VMs estão tentando ser protegidas:

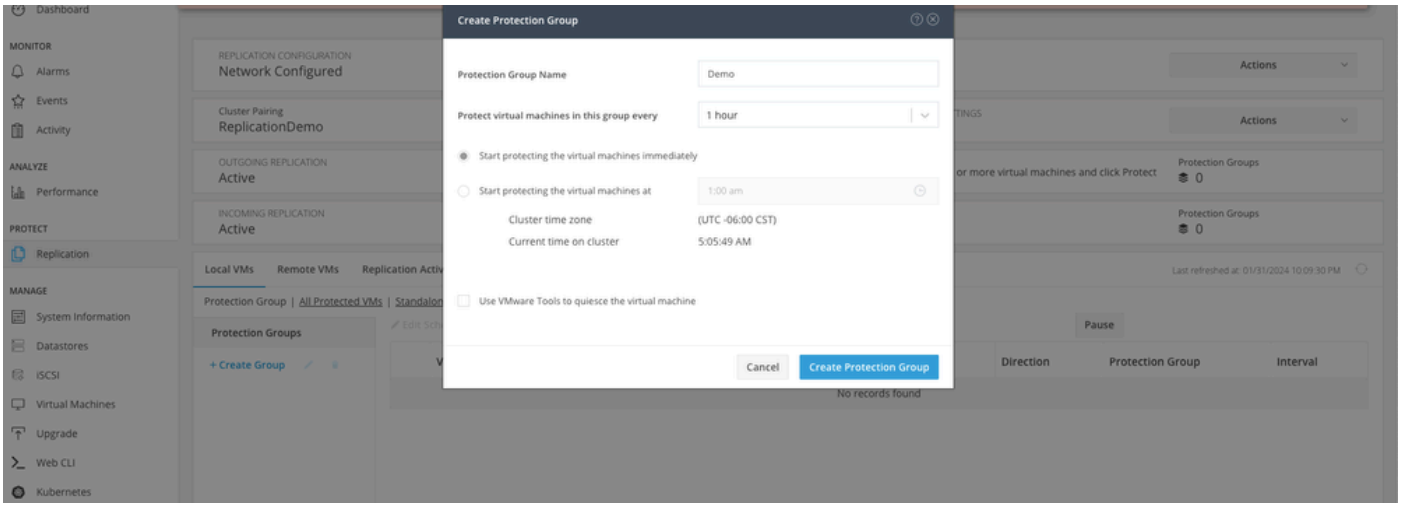


Mapeando armazenamentos de dados



Observação: o mapeamento de armazenamentos de dados pode ser feito de ambos os sites para o outro; por exemplo, Cluster1 pode Mapear armazenamentos de dados para cluster2 e Cluster2 pode mapear armazenamentos de dados para cluster1 sem qualquer configuração adicional.

Etapa 10. Depois que os armazenamentos de dados forem mapeados, defina o grupo de proteção, especifique um nome e selecione um período para proteger as máquinas virtuais a serem associadas a ele. Por fim, especifique a hora em que o grupo de proteção é iniciado e clique em Create Protection Group.

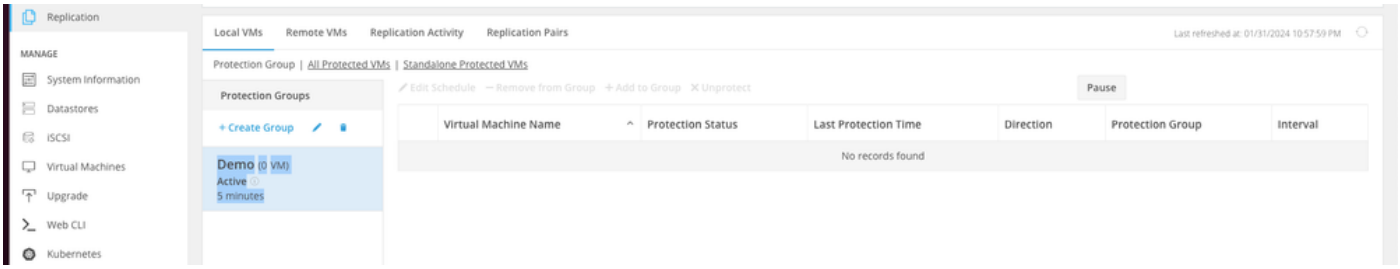


Criação de Grupo de Proteção

Considerações sobre o grupo de proteção

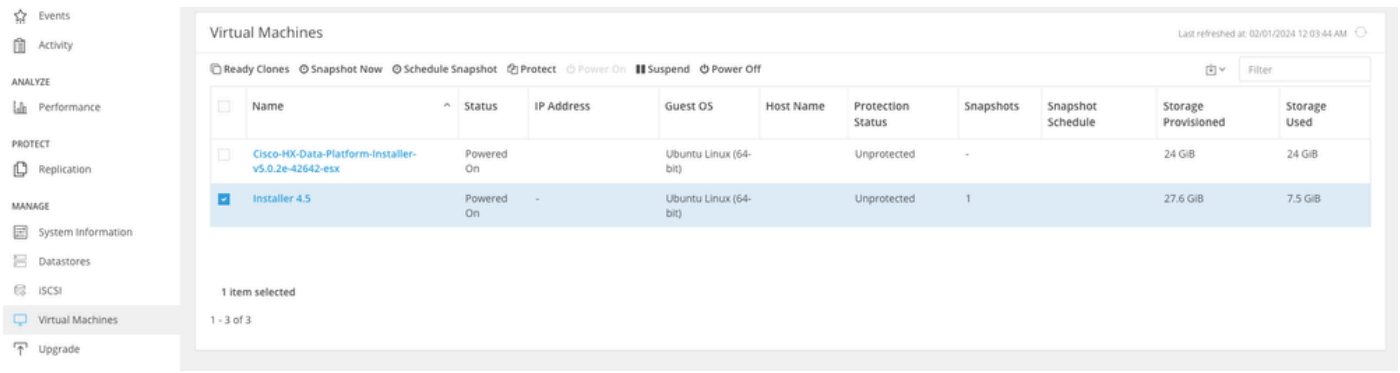
- O grupo de proteção define como a proteção de dados se comporta.
- Permite especificar a frequência para proteger a máquina virtual.
- Ele pode ir de 5 minutos a 24 horas, também o horário em que a proteção começa.
- Pode ter um horário imediato ou específico.
- As ferramentas VMware podem ser ativadas para silenciar a máquina virtual.

Uma mensagem de êxito é exibida indicando que o grupo de proteção foi criado e aparece listado na área do grupo de proteção:

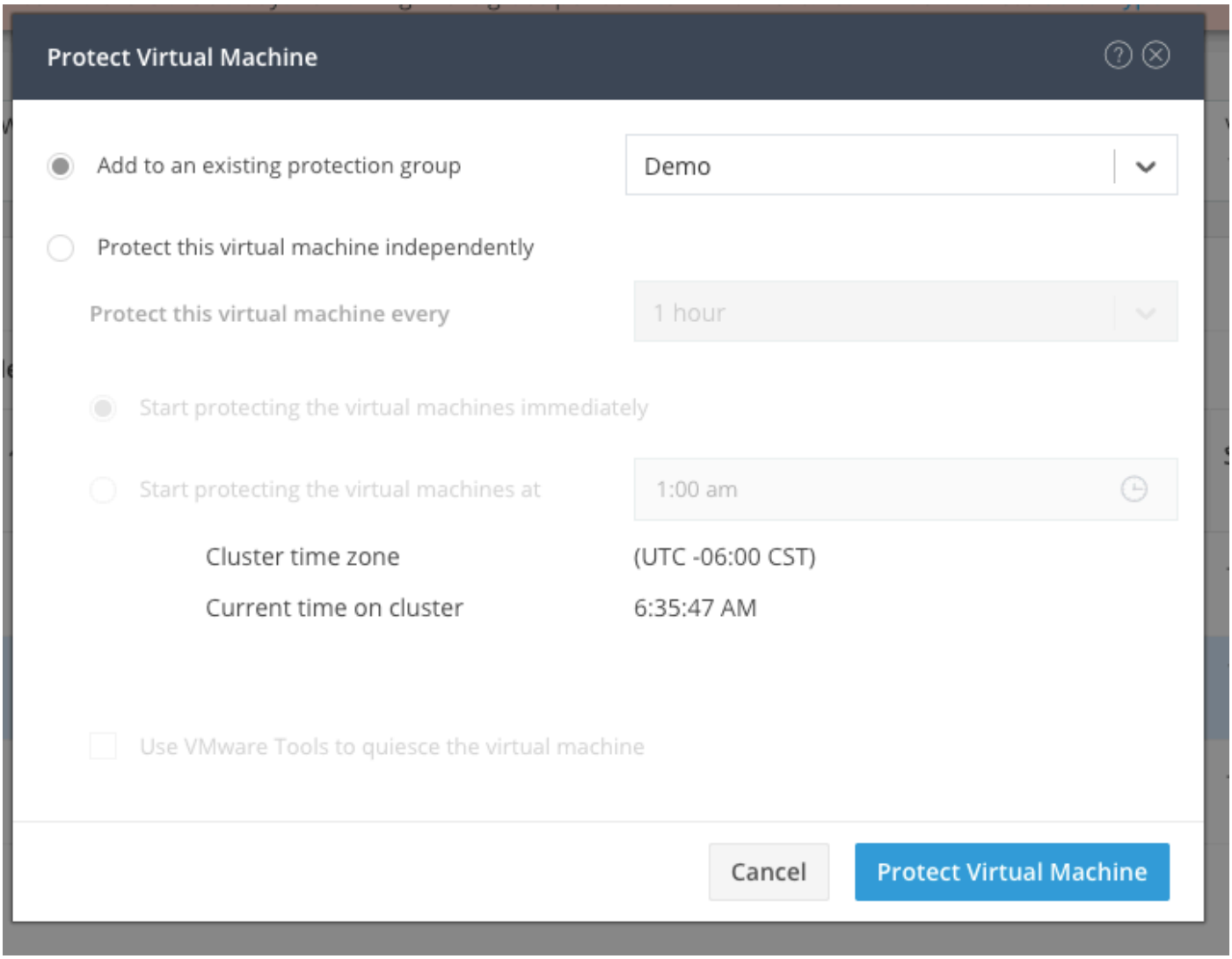


Grupo de Proteção Criado

Etapa 11. Com o grupo de proteção criado, a etapa final é atribuí-lo às máquinas virtuais que devem ser protegidas. Navegue até a guia Máquinas virtuais, selecione a máquina virtual a ser protegida e clique em Proteger:

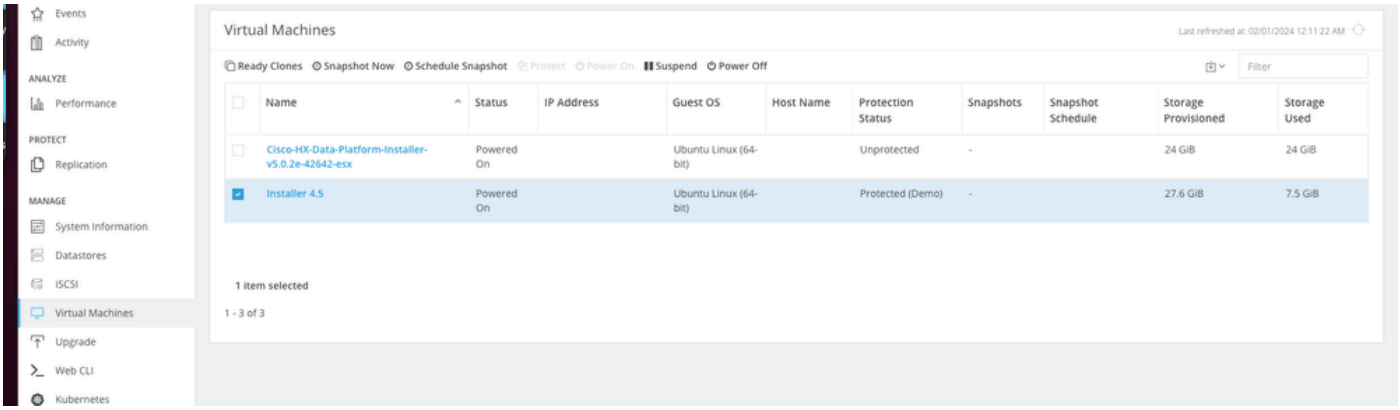


Uma janela pop-up será exibida para anexar o grupo de proteção criado, selecioná-lo e clicar em Proteger máquina virtual:

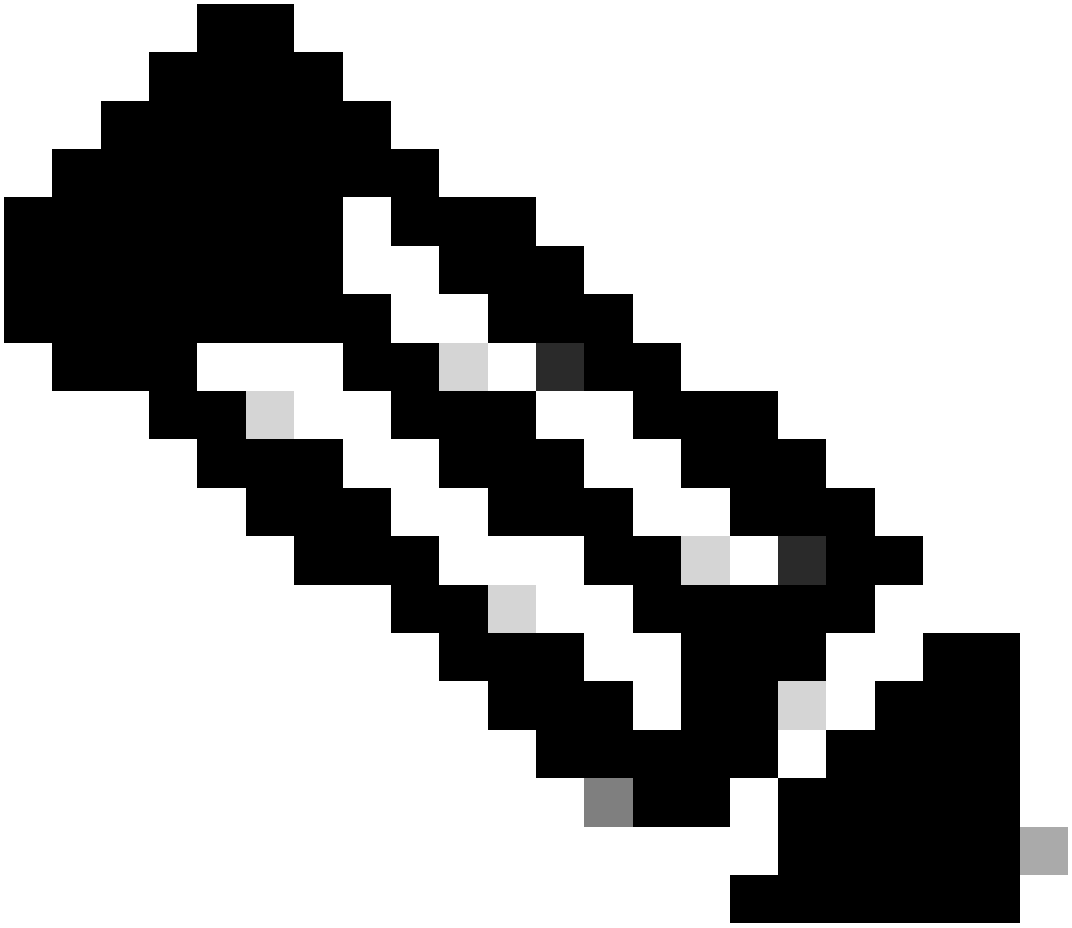


Selecionando o grupo de proteção

Depois de protegida, a VM é exibida como protegida para o Grupo de proteção.



VM protegida

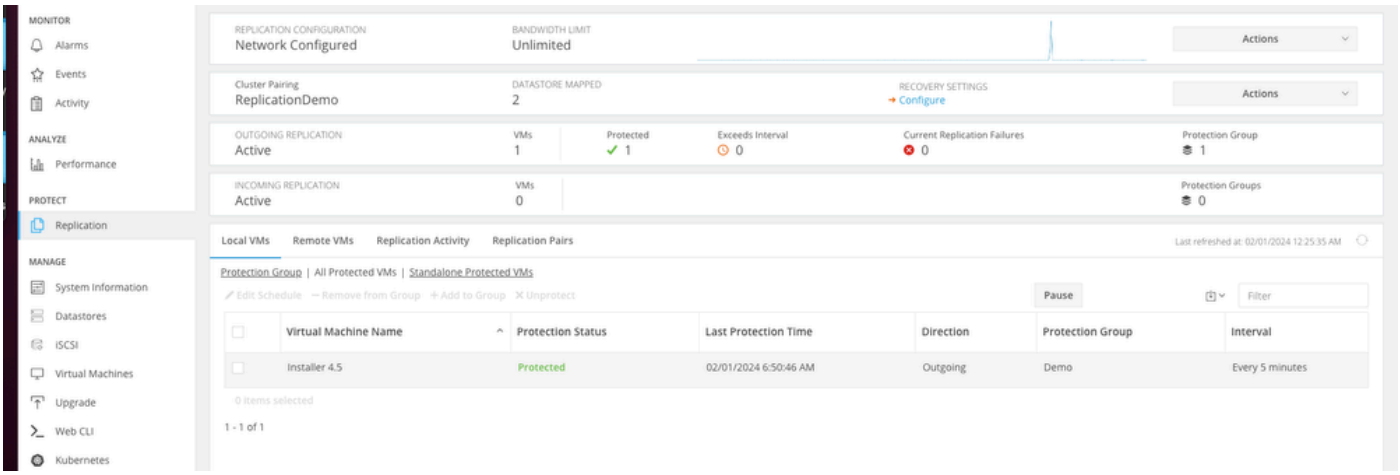


Observação: verifique se a VM protegida pertence a um armazenamento de dados que está sendo mapeado, caso contrário, a proteção falhará.

Troubleshooting

Verificar a Configuração de Proteção da VM

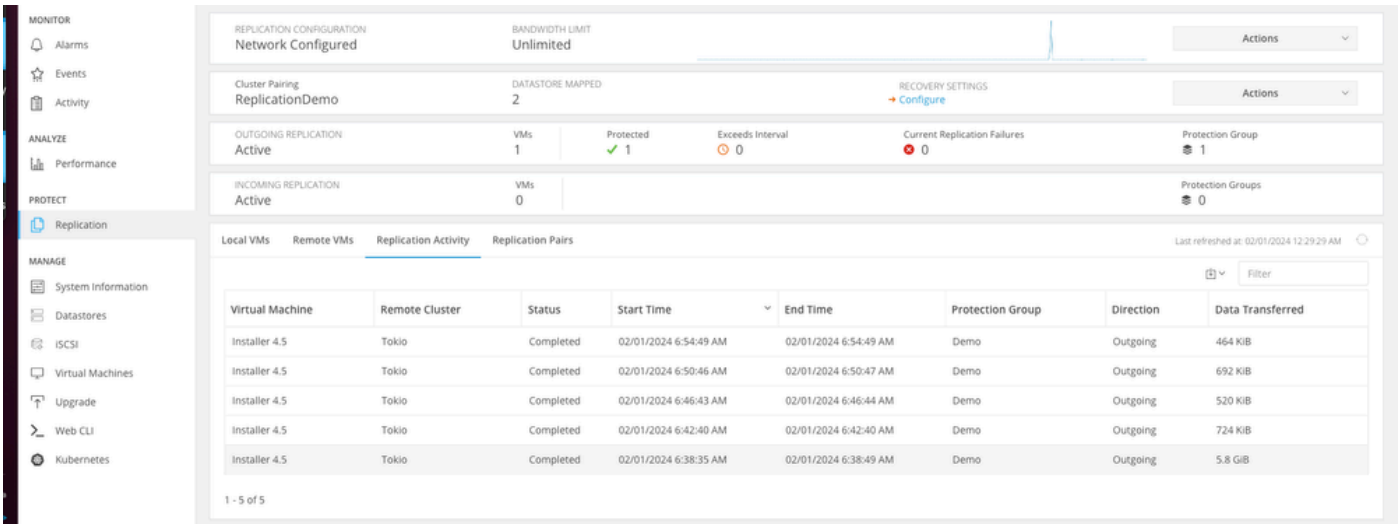
É uma prática recomendada monitorar a proteção da VM na guia Replication:



Monitorando VMs Protegidas

Monitorar Atividades de Replicação

As atividades de replicação podem ser monitoradas clicando na guia Atividade de Replicação:

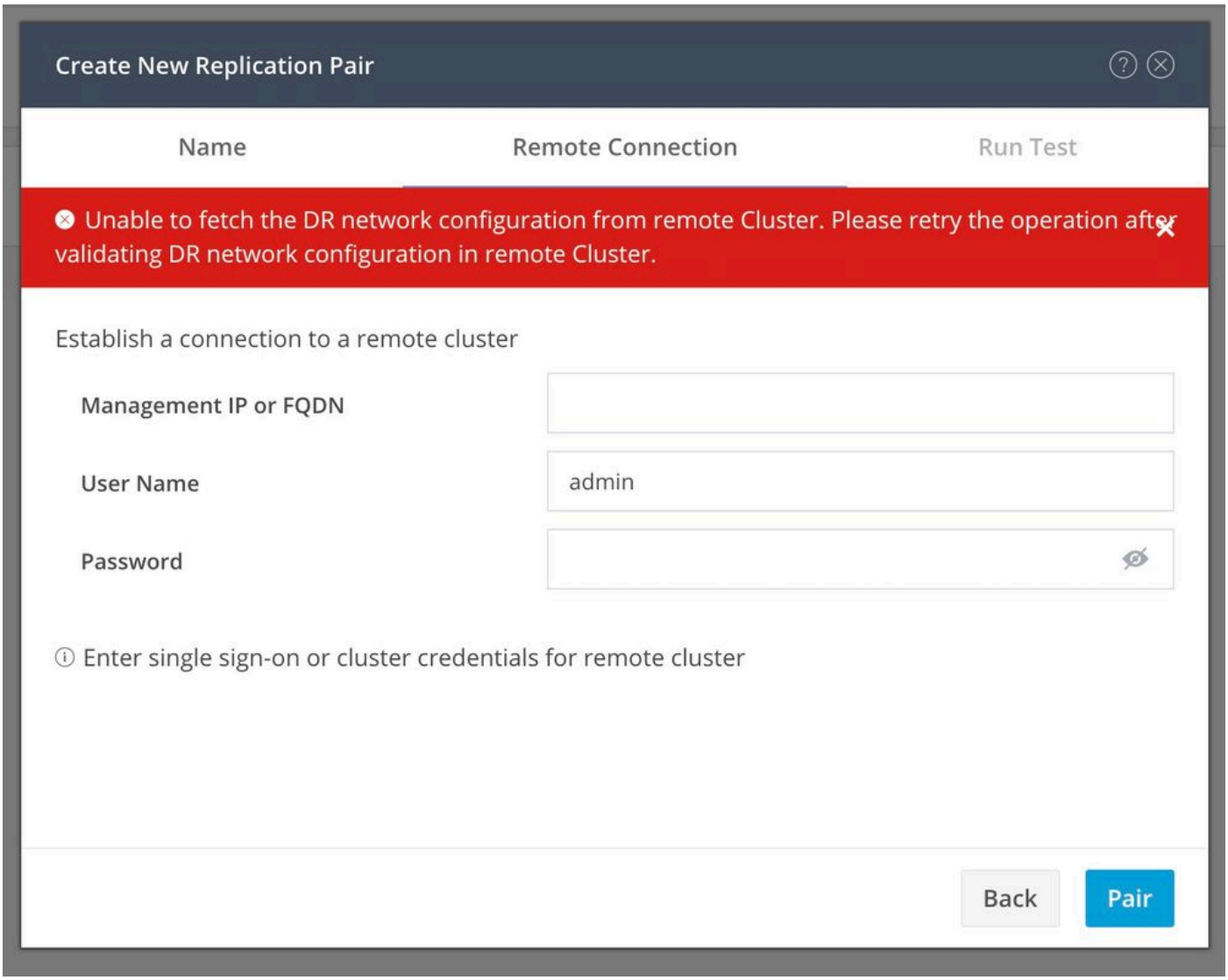


Atividades de Replicação

Problemas comuns

Problemas de pares

Problemas de emparelhamento podem aparecer:

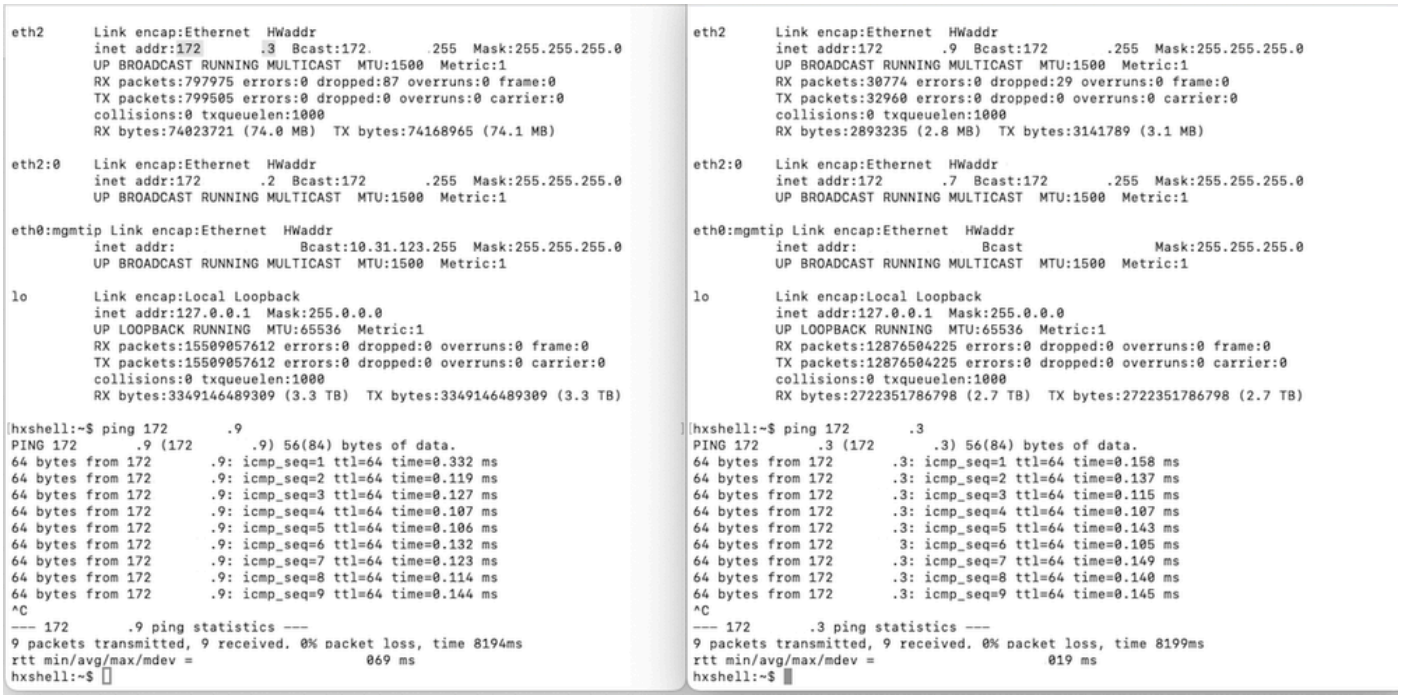


Problemas de emparelhamento

- Verifique se a rede de replicação está configurada em ambos os clusters.
- Certifique-se de que os clusters estejam acessíveis um do outro.

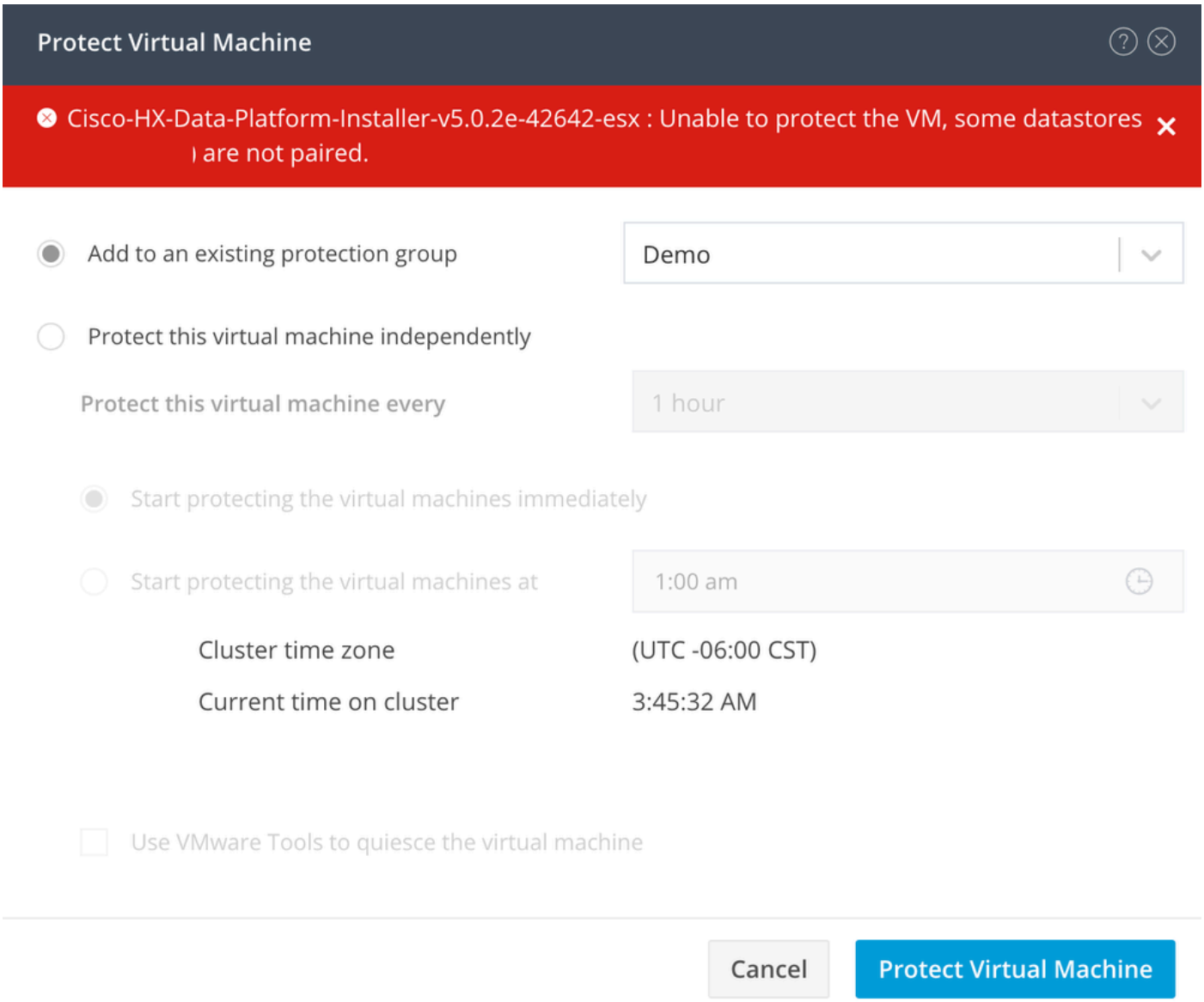
Problemas de conectividade

- Verifique se eth2 está presente. Use o comando ifconfig em cada uma das Máquinas Virtuais do Controlador de Armazenamento para confirmar se a eth2 está configurada corretamente.
- Use o ping para testar a conectividade entre as interfaces eth2.
- Verifique se a VLAN de Replicação em ambos os clusters corresponde.
- Verifique se a VLAN de replicação está configurada corretamente em todos os caminhos entre os clusters.



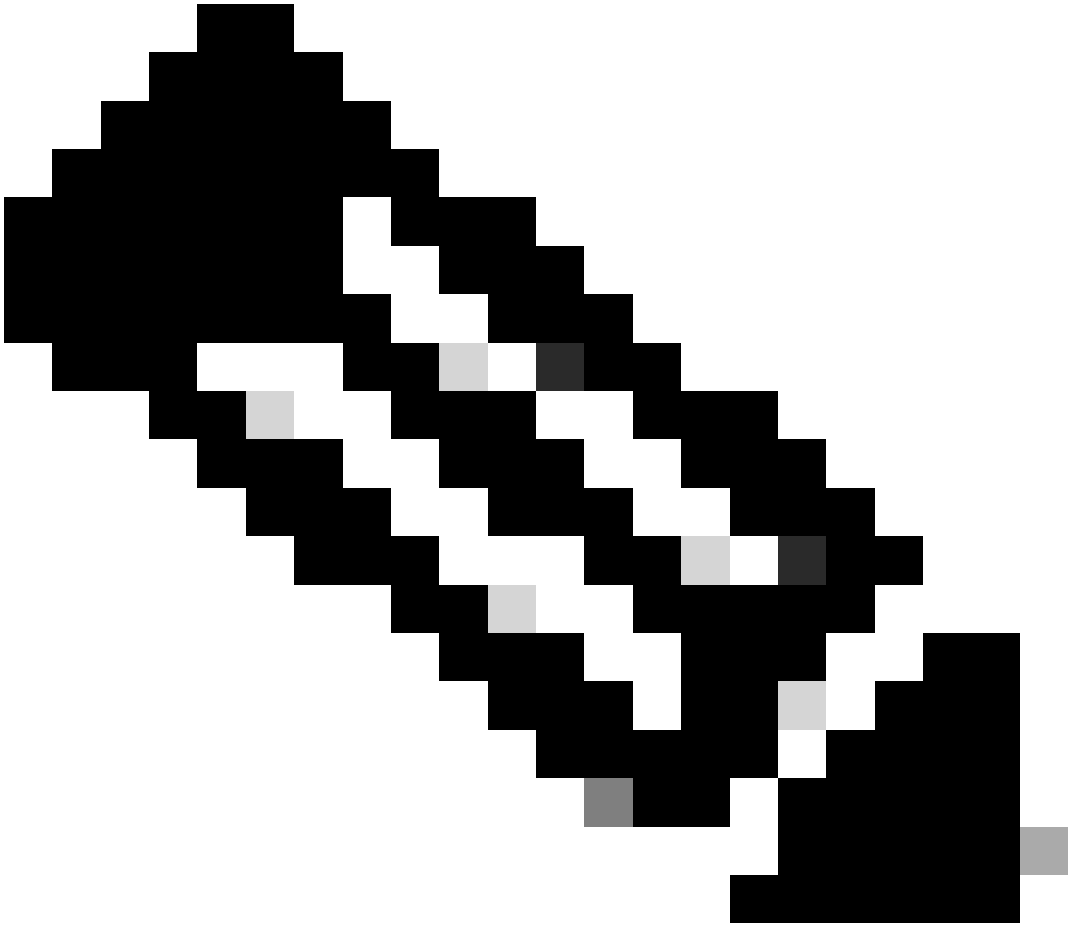
Teste de ping

Problemas de proteção



Problemas de proteção

- Verifique se a VM a ser protegida pertence a um armazenamento de dados mapeado.
- Verifique se os armazenamentos de dados estão mapeados corretamente.



Observação: algumas correções exigem a intervenção do Technical Assistance Center (TAC). Abra um caso no TAC, se necessário.

Informações Relacionadas

- Guia de Administração da Cisco HyperFlex Data Platform, Versão 5.0
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.