



Administrar e monitorar

ASA r2

NetApp
April 08, 2026

Índice

Administrar e monitorar	1
Atualizar e reverter o ONTAP	1
Atualizar o ONTAP em sistemas de storage ASA R2	1
Reverter ONTAP em sistemas de armazenamento ASA r2	1
Atualize o firmware em sistemas de armazenamento ASA R2	2
Gerenciar o acesso do cliente a VMs de storage em sistemas de storage ASA R2	4
Crie uma VM de storage	4
Crie IPspaces	4
Crie sub-redes	5
Criar um LIF (interface de rede)	5
Modificar um LIF (interfaces de rede)	8
Gerenciar a rede de cluster em sistemas de storage ASA R2	9
Adicione um domínio de broadcast	9
Reatribuir portas a um domínio de broadcast diferente	10
Crie uma VLAN	10
Monitorar o uso e aumentar a capacidade	11
Saiba mais sobre balanceamento de capacidade do ONTAP em um cluster ASA r2	11
Monitore o desempenho do cluster e da unidade de armazenamento em sistemas de armazenamento ASA R2	12
Monitorar a utilização de cluster e unidades de storage em sistemas de storage ASA R2	13
Aumentar a capacidade de storage em sistemas de storage ASA R2	15
Otimize a segurança e a performance do cluster com os insights do sistema de storage do ASA R2	16
Exibir eventos e trabalhos de cluster em sistemas de storage ASA R2	17
Envie notificações por e-mail para eventos de cluster e logs de auditoria	17
Gerenciar nós	18
Adicione nós do ASA R2 a um cluster do ONTAP	18
Reinicie um nó em um sistema de storage ASA R2	18
Renomeie um nó em um sistema de storage ASA R2	19
Gerenciar contas de usuários e funções em sistemas de storage ASA R2	19
Configurar o acesso do controlador de domínio do diretório ativo	19
Configurar o LDAP	20
Configurar a autenticação SAML	20
Criar funções de conta de usuário	21
Crie uma conta de administrador	21
Gerenciar certificados de segurança em sistemas de storage ASA R2	21
Gerar uma solicitação de assinatura de certificado	22
Adicione uma autoridade de certificação confiável	22
Renove ou exclua uma autoridade de certificação confiável	22
Adicione um certificado de cliente/servidor ou autoridades de certificação locais	23
Renovar ou eliminar um certificado de cliente/servidor ou autoridades de certificação locais	23
Verifique a conectividade de host no sistema de storage ASA R2	24

Administrar e monitorar

Atualizar e reverter o ONTAP

Atualizar o ONTAP em sistemas de storage ASA R2

Ao atualizar o software ONTAP no sistema ASA R2, você pode aproveitar os novos e aprimorados recursos do ONTAP que ajudam a reduzir custos, acelerar workloads críticos, melhorar a segurança e expandir o escopo de proteção de dados disponível para sua organização.

As atualizações de software ONTAP para sistemas ASA r2 seguem o mesmo processo que as atualizações para outros sistemas ONTAP. Recomenda-se que você comece por ["Preparando-se para a sua atualização com Upgrade Advisor no Active IQ Digital Advisor ou Upgrade Health Checker"](#).

Depois de se preparar para a atualização, é recomendável que você execute atualizações usando ["Atualização automatizada e sem interrupções \(ANDU\) do System Manager"](#)o . O ANDU aproveita a tecnologia de failover de alta disponibilidade (HA) da ONTAP para garantir que os clusters continuem fornecendo dados sem interrupção durante a atualização.

Saiba mais ["Atualizações de software ONTAP"](#)sobre o .

Reverter ONTAP em sistemas de armazenamento ASA r2

As reversões de software ONTAP para sistemas ASA r2 seguem o mesmo processo de reversões para outros sistemas ONTAP .

A reversão de um cluster ONTAP é disruptiva. Você deve deixar o cluster offline durante a reversão. Você não deve reverter um cluster de produção sem assistência do suporte técnico. Você pode reverter um cluster novo ou de teste sem assistência. Se a reversão de um sistema novo ou de teste falhar ou for concluída com sucesso, mas você não estiver satisfeito com o desempenho do cluster em seu ambiente de produção, entre em contato com o suporte técnico para obter assistência.

["Reverter um cluster ONTAP"](#) .

Rever requisitos para sistemas ASA r2

Certas configurações de cluster ASA r2 exigem que você execute ações específicas antes de iniciar uma reversão de software ONTAP .

Revertendo do ONTAP 9.17.1

Se você estiver revertendo do ONTAP 9.17.1 em um sistema ASA r2, execute as seguintes ações antes de iniciar a reversão:



["equilíbrio espacial dinâmico"](#)É ativado por padrão 14 dias após a atualização para o ONTAP 9.17.1 ou a inicialização de um novo cluster ONTAP 9.17.1 ASA r2. Não é possível reverter do ONTAP 9.17.1 para o ASA r2 após a ativação do balanceamento dinâmico de espaço.

Se você tem...	Antes de reverter você deve...
Grupos de consistência hierárquica em um relacionamento de sincronização ativa do SnapMirror	"Excluir o relacionamento de sincronização ativa do SnapMirror".
Relacionamentos de importação ativos	Exclua os relacionamentos de importação ativos. "Saiba mais sobre relações de importação".
Proteção anti-ransomware habilitada	"Desative a proteção contra ransomware."

Atualize o firmware em sistemas de armazenamento ASA R2

O ONTAP transfere e atualiza automaticamente ficheiros de firmware e de sistema no seu sistema ASA R2 por predefinição. Se você quiser a flexibilidade de visualizar as atualizações recomendadas antes que elas sejam baixadas e instaladas, você pode usar o Gerenciador de sistema do ONTAP para desativar atualizações automatizadas ou editar parâmetros de atualização para mostrar notificações de atualizações disponíveis antes que qualquer ação seja executada.

Ativar atualizações automáticas

As atualizações recomendadas para firmware de armazenamento, firmware SP/BMC e ficheiros de sistema são automaticamente transferidas e instaladas no sistema ASA R2 por predefinição. Se as atualizações automáticas tiverem sido desativadas, você poderá habilitá-las a restabelecer o comportamento padrão.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Em **Atualizações de software**, selecione **Ativar**.
3. Leia o CLUF.
4. Aceite os padrões para **Mostrar notificação** de atualizações recomendadas. Opcionalmente, selecione **Atualizar automaticamente** ou **Descartar automaticamente** as atualizações recomendadas.
5. Selecione para confirmar que suas modificações de atualização serão aplicadas a todas as atualizações atuais e futuras.
6. Selecione **Guardar**.

Resultado

As atualizações recomendadas são transferidas e instaladas automaticamente no sistema ASA R2 com base nas seleções de atualização.

Desativar as atualizações automáticas

Desative as atualizações automáticas somente se você quiser gerenciar as atualizações inteiramente por conta própria. Com as atualizações automáticas desativadas, o sistema não notificará, baixará ou instalará atualizações. Você é responsável por monitorar, baixar, agendar e instalar todas as atualizações manualmente.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Em **Atualizações de software**, selecione **Desativar**.

Resultado

As atualizações automáticas estão desativadas. Deve verificar regularmente as atualizações recomendadas e decidir se pretende efetuar uma instalação manual.

Ver atualizações automáticas

Veja uma lista de atualizações de firmware e de ficheiros de sistema que foram transferidas para o cluster e que estão agendadas para instalação automática. Veja também as atualizações que foram instaladas automaticamente anteriormente.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Ao lado de **Atualizações de software** selecione → e selecione **Exibir todas as atualizações automáticas**.

Editar atualizações automáticas

Você pode optar por ter as atualizações recomendadas para o firmware de armazenamento, o firmware SP/BMC e os arquivos de sistema baixados e instalados automaticamente no cluster, ou pode optar por ter as atualizações recomendadas descartadas automaticamente. Se você quiser controlar manualmente a instalação ou a demissão de atualizações, selecione para ser notificado quando uma atualização recomendada estiver disponível; então você pode selecionar manualmente para instalá-la ou descartá-la.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Ao lado de **Atualizações de software** selecione → e selecione **Todas as outras atualizações**.
3. Atualize as seleções para atualizações automáticas.
4. Selecione **Guardar**.

Resultado

As atualizações automáticas são modificadas com base nas suas seleções.

Atualize o firmware manualmente

Se você quiser a flexibilidade de visualizar as atualizações recomendadas antes que elas sejam baixadas e instaladas, você pode desativar as atualizações automatizadas e atualizar seu firmware manualmente.

Passos

1. Transfira o ficheiro de atualização do firmware para um servidor ou cliente local.
2. No Gerenciador do Sistema, selecione **Cluster > Visão geral** e, em seguida, selecione **Todas as outras atualizações**.
3. Em **Atualizações manuais**, selecione **Adicionar arquivos de firmware**; depois selecione **Baixar do servidor** ou **Carregar do cliente local**.
4. Instale o arquivo de atualização de firmware.

Resultado

O firmware é atualizado.

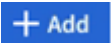
Gerenciar o acesso do cliente a VMs de storage em sistemas de storage ASA R2

As unidades de armazenamento em um sistema ASA R2 estão contidas nas máquinas virtuais de armazenamento (VMs). As VMs de storage são usadas para fornecer dados aos clientes de SAN. Use o Gerenciador do sistema ONTAP para criar um LIF (interface de rede) para que seus clientes SAN se conectem a uma VM de storage e acessem dados nas unidades de armazenamento. Opcionalmente, você pode usar sub-redes para simplificar a criação de LIF e IPspaces para fornecer às VMs de armazenamento seu próprio armazenamento seguro, administração e roteamento.

Crie uma VM de storage

Durante a configuração do cluster, sua máquina virtual de armazenamento de dados (VM) padrão é criada. Todas as novas unidades de armazenamento são criadas dentro da VM de armazenamento de dados padrão, a menos que você crie e selecione uma VM de armazenamento diferente. Você pode criar uma VM de armazenamento adicional para segregar suas unidades de armazenamento para diferentes aplicativos, departamentos ou clientes. Por exemplo, você pode querer criar uma VM de storage para seu ambiente de desenvolvimento e outra VM de storage para seu ambiente de produção ou criar uma VM de storage para seu departamento financeiro e outra VM de storage para seu departamento de marketing.

Passos

1. Selecione **Cluster > Storage VMs**.
2.  Selecione .
3. Insira um nome para a VM de armazenamento ou aceite o nome padrão.
4. Em **Configurar protocolos**, selecione os protocolos para a VM de armazenamento.

Selecione **IP** para iSCSI e NVMe/TCP. Selecione **FC** para Fibre Channel ou NVMe/FC.

5. Em **Storage VM Administration**, selecione **Manage administrator account** (gerir conta de administrador); em seguida, introduza o nome de utilizador e a palavra-passe da conta de administrador.
6. Adicione uma interface de rede para a VM de storage.
7. Selecione **Guardar**.

O que se segue?

Você criou uma VM de storage. Agora você pode usar a VM de storage para "[provisionamento de storage](#)".

Crie IPspaces

Um espaço IPspace é um espaço de endereço IP distinto no qual as VMs de armazenamento residem. Quando você cria IPspaces, você habilita as VMs de armazenamento para ter seu próprio armazenamento seguro, administração e roteamento. Você também permite que os clientes em domínios de rede separados administrativamente usem endereços IP sobrepostos do mesmo intervalo de sub-rede de endereços IP.

Você deve criar um espaço IPspace antes de criar uma sub-rede.

Passos

1. Selecione **rede > Visão geral**.

2. Em **IPspaces**, **+ Add** selecione .
3. Introduza um nome para o IPspace ou aceite o nome predefinido.

Um nome IPspace não pode ser "All" porque "All" é um nome reservado ao sistema.

4. Selecione **Guardar**.

O que se segue?

Agora que você criou um espaço IPspace, você pode usá-lo para criar uma sub-rede.

Crie sub-redes

Uma sub-rede permite alocar blocos específicos de endereços IPv4 ou IPv6 para usar quando você cria um LIF (interface de rede) . Uma sub-rede simplifica a criação de LIF, permitindo que você especifique o nome da sub-rede em vez de um endereço IP específico e uma máscara de rede para cada LIF.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- O "[domínio de transmissão](#)" e o espaço IPspace onde pretende adicionar a sub-rede já devem existir.

Passos

1. Selecione **rede > Visão geral**.
2. Selecione **sub-redes**; em seguida, **+ Add** selecione .
3. Introduza o nome da sub-rede.

Todos os nomes de sub-rede devem ser exclusivos dentro de um espaço IPspace.

4. Introduza o endereço IP da sub-rede e a máscara de sub-rede.
5. Especifique o intervalo de endereços IP para a sub-rede.

Quando especificar o intervalo de endereços IP para a sub-rede, não sobreponha endereços IP com outras sub-redes. Problemas de rede podem ocorrer quando os endereços IP de sub-rede se sobrepõem e diferentes sub-redes ou hosts tentam usar o mesmo endereço IP.

6. Selecione o domínio de broadcast para a sub-rede.
7. Selecione **Adicionar**.

O que se segue?

Você criou uma sub-rede que agora pode usar para simplificar a criação de seus LIFs.

Criar um LIF (interface de rede)

Um LIF (interface de rede) é um endereço IP associado a uma porta física ou lógica. Crie LIFs nas portas que você deseja usar para acessar dados. As VMs de storage fornecem dados aos clientes por meio de uma ou mais LIFs. Se houver uma falha de componente, um LIF pode falhar ou ser migrado para uma porta física diferente, de modo que a comunicação de rede não seja interrompida.

Em um sistema ASA R2, você pode criar LIFs IP, FC e NVMe/FC. Um LIF de dados IP pode atender o tráfego iSCSI e NVMe/TCP por padrão. É necessário criar LIFs de dados separados para o tráfego FC e NVMe/FC.

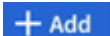
Se pretender ativar o failover de LIF iSCSI automático, tem de criar um LIF IP para tráfego apenas iSCSI.

Quando o failover automático de LIF iSCSI é ativado, se ocorrer um failover de armazenamento, o IP iSCSI LIF é migrado automaticamente de seu nó ou porta inicial para seu nó ou porta parceiro de HA e, em seguida, volta assim que o failover for concluído. Ou, se a porta para um IP iSCSI LIF não for saudável, o LIF é migrado automaticamente para uma porta saudável em seu nó inicial atual e, em seguida, de volta para sua porta original quando a porta estiver funcionando novamente.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- A porta de rede física ou lógica subjacente deve ter sido configurada para o status administrativo `up`.
- Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, a sub-rede já deve existir.
- Um tráfego entre nós que lida com LIF não deve estar na mesma sub-rede que um tráfego de gerenciamento de manipulação de LIF ou um tráfego de dados de manipulação de LIF.

Passos

1. Selecione **rede > Visão geral**.
2. Selecione **interfaces de rede**; em seguida,  selecione .
3. Selecione o tipo de interface e o protocolo e, em seguida, selecione a VM de armazenamento.
4. Introduza um nome para o LIF ou aceite o nome predefinido.
5. Selecione o nó inicial para a interface de rede e, em seguida, introduza o endereço IP e a máscara de sub-rede.
6. Selecione **Guardar**.

Resultado

Você criou um LIF para acesso aos dados.

O que se segue?

Você pode usar a interface de linha de comando (CLI) do ONTAP para criar um LIF somente iSCSI com failover automático.

Crie uma política de serviço LIF personalizada somente iSCSI

Se você quiser criar LIFs somente iSCSI com failover automático de LIF, primeiro crie uma política de serviço LIF somente iSCSI personalizada.

Você deve usar a interface de linha de comando (CLI) do ONTAP para criar a política de serviço personalizada.

Passo

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Crie uma política de serviço LIF personalizada somente para iSCSI:

```
network interface service-policy create -vserver <storage_VM_name>
-policy <service_policy_name> -services data-core,data-iscsi
```

3. Verifique se a política de serviço foi criada:

```
network interface service-policy show -policy <service_policy_name>
```

4. Retorne o nível de privilégio para admin:

```
set -privilege admin
```

Crie LIFs somente iSCSI com failover automático de LIF

Se existirem LIFs iSCSI na VM de armazenamento que não estejam habilitadas para failover automático de LIF, as LIFs recém-criadas também não serão habilitadas para failover automático de LIF. Se o failover automático de LIF não estiver habilitado e ocorrer um evento de failover, suas LIFs iSCSI não serão migradas.

Antes de começar

Você deve ter criado uma política de serviço LIF personalizada somente iSCSI.

Passos

1. Crie LIFs somente iSCSI com failover automático de LIF:

```
network interface create -vserver <storage_VM_name> -lif
<iscsi_lif_name> -service-policy <service_policy_name> -home-node
<home_node> -home-port <port_name> -address <ip_address> -netmask
<netmask> -failover-policy sfo-partner-only -status-admin up
```

- Recomenda-se criar dois iSCSI LIFs em cada nó, um para a malha A e outro para a malha B. Isso proporciona redundância e balanceamento de carga para o tráfego iSCSI. No exemplo a seguir, são criados um total de quatro iSCSI LIFs, dois em cada nó e um para cada malha.

```
network interface create -vserver svml -lif iscsi-lif-01a -service
-policy custom-data-iscsi -home-node node1 -home-port e2b -address
<node01-iscsi-a-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up
```

```
network interface create -vserver svml -lif iscsi-lif-01b -service
-policy custom-data-iscsi -home-node node1 -home-port e4b -address
<node01-iscsi-b-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up
```

```
network interface create -vserver svml -lif iscsi-lif-02a -service
-policy custom-data-iscsi -home-node node2 -home-port e2b -address
<node02-iscsi-a-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up
```

```
network interface create -vserver svml -lif iscsi-lif-02b -service
-policy custom-data-iscsi -home-node node2 -home-port e4b -address
<node02-iscsi-b-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up
```

- Se você estiver usando VLANs, ajuste o `home-port` parâmetro para incluir as informações da porta VLAN para a respectiva estrutura iSCSI, por exemplo, `-home-port e2b-<iSCSI-A-VLAN>` para tecido iSCSI A e `-home-port e4b-<iSCSI-B-VLAN>`.
- Se você estiver usando grupos de interface (ifgroups) com VLANs, ajuste o `home-port` parâmetro para incluir a porta VLAN apropriada, por exemplo, `-home-port a0a-<iSCSI-A-VLAN>` para tecido iSCSI A e `-home-port a0a-<iSCSI-B-VLAN>` para tecido iSCSI B onde `a0a` é o ifgroup e `a0a-<iSCSI-A-VLAN>` e `a0a-<iSCSI-B-VLAN>` são as respectivas portas VLAN para a estrutura iSCSI A e a estrutura iSCSI B.

2. Verifique se os LIFs iSCSI foram criados:

```
network interface show -lif iscsi*
```

Modificar um LIF (interfaces de rede)


Os LIFs podem ser desativados ou renomeados conforme necessário. Você também pode alterar o endereço IP de LIF e a máscara de sub-rede.

Sobre esta tarefa

O ONTAP utiliza o Network Time Protocol (NTP) para sincronizar o tempo no cluster. Após alterar os endereços IP do LIF, talvez seja necessário atualizar a configuração do NTP para evitar falhas de sincronização. Para obter mais informações, consulte o artigo da Base de Conhecimento "[A sincronização NTP falha após a alteração do IP do LIF](#)".

Passos

1. Selecione **rede > Visão geral**; em seguida, selecione **interfaces de rede**.

2. Passe o Mouse sobre a interface de rede que você deseja editar; em seguida,  selecione .
3. Selecione **Editar**.
4. Pode desativar a interface de rede, mudar o nome da interface de rede, alterar o endereço IP ou alterar a máscara de sub-rede.
5. Selecione **Guardar**.

Resultado

Seu LIF foi modificado.

Gerenciar a rede de cluster em sistemas de storage ASA R2

Você pode usar o Gerenciador de sistema do ONTAP para executar a administração básica da rede de storage no sistema ASA R2. Por exemplo, você pode adicionar um domínio de broadcast ou reatribuir portas a um domínio de broadcast diferente.

Adicione um domínio de broadcast

Use domínios de broadcast para simplificar o gerenciamento da rede de cluster agrupando portas de rede que pertencem à mesma rede de camada 2. As máquinas virtuais de armazenamento (VMs) podem então usar as portas do grupo para tráfego de dados ou gerenciamento.

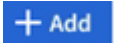
O domínio de broadcast "padrão" e o domínio de broadcast "Cluster" são criados durante a configuração do cluster. O domínio de broadcast "padrão" contém portas que estão no IPspace "padrão". Essas portas são usadas principalmente para fornecer dados. As portas de gerenciamento de clusters e de nós também estão neste domínio de transmissão. O domínio de broadcast "Cluster" contém portas que estão no espaço IPspace "Cluster". Essas portas são usadas para comunicação de cluster e incluem todas as portas de cluster de todos os nós no cluster.

Você pode criar domínios de broadcast adicionais após o cluster ter sido inicializado. Quando você cria um domínio de broadcast, um grupo de failover que contém as mesmas portas é criado automaticamente.

Sobre esta tarefa

A unidade máxima de transmissão (MTU) das portas adicionadas a um domínio de broadcast são atualizadas para o valor MTU definido no domínio de broadcast.

Passos

1. No System Manager, selecione **rede > Visão geral**.
2. Em domínios **Broadcast**,  selecione .
3. Introduza um nome para o domínio de difusão ou aceite o nome predefinido.

Todos os nomes de domínio de broadcast devem ser exclusivos dentro de um espaço IPspace.

4. Selecione o espaço IPspace para o domínio de broadcast.

Se você não especificar um nome de IPspace, o domínio de broadcast será criado no IPspace "padrão".

5. Introduza a unidade de transmissão máxima (MTU).

MTU é o maior pacote de dados que pode ser aceito no seu domínio de broadcast.

6. Selecione as portas desejadas; em seguida, selecione **Salvar**.


Resultado

Você adicionou um novo domínio de broadcast.

Reatribuir portas a um domínio de broadcast diferente

As portas podem pertencer a apenas um domínio de broadcast. Se você quiser alterar o domínio de broadcast ao qual uma porta pertence, você precisa reatribuir a porta de seu domínio de broadcast existente a um novo domínio de broadcast.

Passos

1. No System Manager, selecione **rede > Visão geral**.
2. Em **Broadcast Domains**,  selecione ao lado do nome de domínio; em seguida, selecione **Edit**.
3. Desmarque as portas Ethernet que você deseja reatribuir a outro domínio.
4. Selecione o domínio de broadcast ao qual deseja reatribuir a porta; em seguida, selecione **Reatribuir**.
5. Selecione **Guardar**.

Resultado

Você reatribuiu portas a um domínio de broadcast diferente.

Crie uma VLAN

Uma VLAN consiste em portas de switch agrupadas em um domínio de broadcast. As VLANs permitem aumentar a segurança, isolar problemas e limitar os caminhos disponíveis na infraestrutura de rede IP.


Antes de começar

Os switches implantados na rede devem estar em conformidade com os padrões IEEE 802,1Q.1X ou ter uma implementação de VLANs específica do fornecedor.

Sobre esta tarefa

- Uma VLAN não pode ser criada em uma porta de grupo de interfaces que não contém portas membro.
- Quando você configura uma VLAN por uma porta pela primeira vez, a porta pode cair, resultando em uma desconexão temporária da rede. As adições subsequentes de VLAN à mesma porta não afetam o estado da porta.
- Você não deve criar uma VLAN em uma interface de rede com o mesmo identificador que a VLAN nativa do switch. Por exemplo, se a interface de rede e0b estiver na VLAN 10 nativa, você não deverá criar uma VLAN e0b-10 nessa interface.

Passos

1. No System Manager, selecione **rede > portas Ethernet** e, em seguida,  **VLAN** selecione .
2. Selecione o nó e o domínio de broadcast para a VLAN.
3. Selecione a porta para a VLAN.

A VLAN não pode ser conetada a uma porta que hospeda um cluster LIF ou a portas atribuídas ao cluster IPspace.

4. Insira um ID de VLAN.

5. Selecione **Guardar**.

Resultado

Você criou uma VLAN para aumentar a segurança, isolar problemas e limitar os caminhos disponíveis na sua infraestrutura de rede IP.

Monitorar o uso e aumentar a capacidade

Saiba mais sobre balanceamento de capacidade do ONTAP em um cluster ASA r2.

Para sistemas ASA r2, o ONTAP utiliza o *posicionamento balanceado* para alocar automaticamente as unidades de armazenamento recém-criadas na melhor zona de disponibilidade de armazenamento, visando o desempenho ideal e a utilização equilibrada do espaço de armazenamento. Se você estiver executando o ONTAP 9.17.1 ou posterior, o espaço consumido pelas unidades de armazenamento existentes será balanceado usando o *balanceamento dinâmico de espaço*. Se você estiver executando o ONTAP 9.16.1, o espaço consumido pelas unidades de armazenamento existentes será balanceado usando o *rebalanceamento de carga de trabalho baseado em cópia*.

Recurso	Apoiado em...
Posicionamento equilibrado	ONTAP 9.16.1 e posterior
Equilíbrio espacial dinâmico	ONTAP 9.17.1 e posterior
Rebalanceamento de carga de trabalho baseado em cópias	Somente ONTAP 9.16.1

Posicionamento equilibrado

Com o recurso de *posicionamento balanceado*, as unidades de armazenamento recém-criadas são automaticamente posicionadas na zona de melhor disponibilidade de armazenamento para otimizar o desempenho e o uso equilibrado do espaço. O posicionamento balanceado está ativado por padrão no ONTAP 9.16.1 e versões posteriores.

Equilíbrio espacial dinâmico

Com o *balanceamento dinâmico de espaço*, o ONTAP monitora ativamente a quantidade de espaço livre no cluster e move automaticamente as unidades de armazenamento dentro das zonas de disponibilidade de armazenamento para manter a utilização equilibrada do espaço. Um aviso do EMS é emitido automaticamente se a utilização da capacidade em todo o cluster atingir 80% e um alerta do EMS é emitido automaticamente se atingir 90%.

O balanceamento dinâmico de espaço é ativado por padrão 14 dias após a atualização ou instalação do ONTAP 9.17.1 ou posterior. Caso precise modificar o período de ativação padrão de 14 dias, entre em contato com o Suporte da NetApp. Não é possível reverter da ONTAP 9.17.1 após a ativação do balanceamento dinâmico de espaço.

O balanceamento dinâmico de espaço opera no *modo normal* ou no *modo de pouco espaço*, com base na média geral de espaço livre em todos os nós do cluster (média global).

- **Modo normal**

No modo normal, o ONTAP verifica a cada três minutos se é necessário balanceamento dinâmico de

espaço. O balanceamento dinâmico de espaço opera no modo normal quando as seguintes condições são verdadeiras:

- A média global de espaço livre é de 10% ou mais.
- Pelo menos um nó no cluster possui mais espaço livre do que a média global.
- Pelo menos um nó no cluster tem 20% menos espaço livre do que a média global.

• **Modo de baixo consumo de espaço**

No modo de baixo espaço, o ONTAP verifica a cada minuto se é necessário balanceamento dinâmico de espaço. O balanceamento dinâmico de espaço opera no modo de espaço reduzido quando as seguintes condições são verdadeiras:

- A média global de espaço livre é inferior a 10%.
- Pelo menos um nó no cluster possui mais espaço livre do que a média global.
- Pelo menos um nó no cluster tem menos espaço livre do que a média global.

Rebalanceamento de carga de trabalho baseado em cópias

Com o *rebalanceamento de carga de trabalho baseado em cópia*, se ocorrer um desequilíbrio na utilização do armazenamento dentro das zonas de disponibilidade de armazenamento, o ONTAP copia automaticamente a unidade de armazenamento que está causando o desequilíbrio para uma zona de disponibilidade de armazenamento com mais espaço livre. Se não houver espaço livre suficiente na zona de disponibilidade de armazenamento de destino, o ONTAP não executará nenhuma ação de balanceamento. O rebalanceamento de carga de trabalho baseado em cópias aplica-se apenas ao sistema ASA r2 que executa o ONTAP 9.16.1 e está ativado por padrão nesses sistemas. No ONTAP 9.17.1 e versões posteriores, ele foi substituído pelo balanceamento dinâmico de espaço.

Caso precise modificar as configurações padrão para o rebalanceamento de cargas de trabalho baseado em cópias, entre em contato com o Suporte da NetApp .

Monitore o desempenho do cluster e da unidade de armazenamento em sistemas de armazenamento ASA R2


Use o Gerenciador de sistema do ONTAP para monitorar o desempenho geral do cluster e o desempenho de unidades de storage específicas para determinar como a latência, o IOPS e a taxa de transferência estão impactando suas aplicações essenciais aos negócios. O desempenho pode ser monitorado em vários períodos de tempo, variando de uma hora a um ano.

Por exemplo, suponha que um aplicativo crítico esteja com alta latência e baixa taxa de transferência. Quando você visualiza o desempenho do cluster nos últimos cinco dias úteis, observa uma diminuição na performance ao mesmo tempo todos os dias. Use essas informações para determinar se o aplicativo crítico está competindo por recursos de cluster quando um processo não crítico começa a ser executado em segundo plano. Você poderá modificar sua política de QoS para limitar o impacto do workload não crítico nos recursos do sistema e garantir que seu workload crítico atenda aos destinos mínimos de taxa de transferência.

Monitorar o desempenho do cluster

Use métricas de performance do cluster para determinar se você precisa mudar os workloads para minimizar a latência e maximizar o IOPS e a taxa de transferência para suas aplicações essenciais.

Passos

1. No System Manager, selecione **Dashboard**.
2. Em **desempenho**, visualize a latência, IOPS e taxa de transferência do cluster por hora, dia, semana, mês ou ano.
3.  Selecione para transferir os dados de desempenho.


O que se segue?

Use as métricas de performance do cluster para analisar se você precisa modificar suas políticas de QoS ou fazer outros ajustes nos workloads da aplicação para maximizar o desempenho geral do cluster.

Monitore o desempenho da unidade de armazenamento

Use as métricas de desempenho da unidade de storage para determinar o impacto de aplicações específicas na latência, IOPS e taxa de transferência.

Passos

1. No System Manager, selecione **Storage**.
2. Selecione a unidade de armazenamento que pretende monitorizar e, em seguida, selecione **Visão geral**.
3. Em **desempenho**, visualize a latência, IOPS e taxa de transferência da unidade de armazenamento por hora, dia, semana, mês ou ano.
4.  Selecione para transferir os dados de desempenho.

O que se segue?

Use as métricas de performance da unidade de storage para analisar se você precisa modificar as políticas de QoS atribuídas às unidades de storage a fim de diminuir a latência e maximizar o IOPS e a taxa de transferência.

Monitorar a utilização de cluster e unidades de storage em sistemas de storage ASA R2

Use o Gerenciador do sistema do ONTAP para monitorar a utilização do storage e garantir que você tenha a capacidade de storage necessária para atender a workloads atuais e futuros.

Monitorar a utilização do cluster

Monitore regularmente a quantidade de storage consumida pelo cluster para garantir que, se necessário, esteja preparado para expandir a capacidade do cluster antes de ficar sem espaço.

Passos

1. No System Manager, selecione **Dashboard**.
2. Em **Capacity**, visualize a quantidade de espaço físico usado e a quantidade de espaço disponível no cluster.

A taxa de redução de dados representa a quantidade de espaço economizado com a eficiência de storage.

O que se segue?

Se o cluster estiver com pouco espaço ou se não tiver capacidade para atender a uma demanda futura, você deve Planejar "[adicionar novas unidades](#)" seu sistema ASA R2 para aumentar a capacidade de storage.

Monitorar a utilização de zona de disponibilidade de storage

Cada par de HA em um sistema ASA R2 usa um pool comum de armazenamento chamado *zona de disponibilidade de armazenamento*. A zona de disponibilidade de storage tem acesso a todos os discos disponíveis no sistema de storage e é visível para ambos os nós do par de HA.

Se você tiver 4 ou mais nós no cluster, poderá visualizar a quantidade de espaço usada pela zona de disponibilidade de storage para cada par de HA. Essa métrica não está disponível para clusters de 2 nós.

Passos

1. No System Manager, selecione **Cluster**; em seguida, selecione **Overview**.

Um resumo da utilização da zona de disponibilidade de storage é exibido para cada par de HA no cluster.

2. Se você quiser métricas mais detalhadas, selecione uma disponibilidade de armazenamento específica.

Em **Visão geral**, a capacidade da zona de disponibilidade de armazenamento, a quantidade de espaço usado e a taxa de redução de dados são exibidos.

Em **unidades de armazenamento** é apresentada uma lista de todas as unidades de armazenamento na zona de disponibilidade de armazenamento.

O que se segue?

Se sua zona de disponibilidade de storage estiver com pouco espaço, você deverá Planejar "[mova as unidades de armazenamento](#)" outra zona de disponibilidade de storage para equilibrar a utilização de storage no cluster.

Monitorar a utilização da unidade de storage

Monitore a quantidade de storage consumida por uma unidade de storage para que você possa aumentar proativamente o tamanho da unidade de storage de acordo com as necessidades da sua empresa.

Passos

1. No System Manager, selecione **Storage**.
2. Selecione a unidade de armazenamento que pretende monitorizar e, em seguida, selecione **Visão geral**.
3. Em **armazenamento**, veja o seguinte:

- Tamanho da sua unidade de armazenamento
- Quantidade de espaço usado
- Relação de redução de dados

A taxa de redução de dados representa a quantidade de espaço economizado com a eficiência de storage

- Instantâneo utilizado

O snapshot usado representa a quantidade de storage usada pelos snapshots.

O que se segue?

Se a sua unidade de armazenamento estiver próxima da capacidade, você deve "[modifique a unidade de armazenamento](#)" aumentar seu tamanho.

Aumentar a capacidade de storage em sistemas de storage ASA R2

Adicione unidades a um nó ou gaveta para aumentar a capacidade de storage do sistema ASA R2.

Use o NetApp Hardware Universe para se preparar para a instalação de uma nova unidade

Antes de instalar uma nova unidade em um nó ou chassi, use o NetApp Hardware Universe para confirmar se a unidade que você deseja adicionar é compatível com o seu sistema ASA r2 e para identificar o slot correto para a nova unidade. Os slots corretos para adicionar unidades variam dependendo do modelo do sistema e da versão do ONTAP . Em alguns casos, é necessário adicionar unidades a slots específicos em sequência.

Passos

1. Vá para "[NetApp Hardware Universe](#)".
2. Em **Produtos**, selecione suas configurações de hardware.
3. Selecione o seu sistema ASA r2.
4. Selecione sua versão do ONTAP; em seguida, selecione **Mostrar resultados**.
5. Abaixo do gráfico, selecione **clique aqui para ver vistas alternativas**; em seguida, escolha a vista que corresponde à sua configuração.
6. Use a exibição de sua configuração para confirmar se sua nova unidade é suportada e o slot correto para instalação.

Resultado

Você confirmou que sua nova unidade é suportada e você sabe o slot apropriado para instalação.

Instale uma nova unidade no ASA R2

O número mínimo de unidades que você deve adicionar em um único procedimento é seis. Adicionar uma única unidade pode reduzir o desempenho.

Sobre esta tarefa

Você deve repetir as etapas deste procedimento para cada unidade.

Passos

1. Aterre-se corretamente.
2. Remova cuidadosamente a moldura da parte frontal do sistema.
3. Insira a nova unidade no slot correto.
 - a. Com o manípulo do excêntrico na posição aberta, utilize as duas mãos para introduzir a nova transmissão.
 - b. Prima até a unidade parar.
 - c. Feche a pega do came de forma a que a unidade fique totalmente assente no plano intermédio e a pega encaixe no devido lugar.

Certifique-se de que fecha lentamente a pega do excêntrico de forma a que fique corretamente alinhada com a face da unidade.

4. Verifique se o LED de atividade da unidade (verde) está aceso.

- SE o LED estiver sólido, a unidade tem energia.
- Se o LED estiver piscando, a unidade tem energia e e/S está em andamento. O LED também piscará se o firmware da unidade estiver sendo atualizado.

O firmware da unidade é atualizado automaticamente (sem interrupções) em novas unidades que não tenham versões de firmware atuais.

5. Se o nó estiver configurado para atribuição automática de unidade, você poderá esperar que o ONTAP atribua automaticamente as novas unidades a um nó. Se o nó não estiver configurado para atribuição automática de unidade ou se preferir, você poderá atribuir as unidades manualmente.

As novas unidades não são reconhecidas até que sejam atribuídas a um nó.

O que vem a seguir?

Depois que as novas unidades tiverem sido reconhecidas, verifique se foram adicionadas e se sua propriedade está especificada corretamente.

Otimize a segurança e a performance do cluster com os insights do sistema de storage do ASA R2

Veja *Insights* no Gerenciador de sistemas do ONTAP para identificar as práticas recomendadas e modificações de configuração que você pode implementar em seu sistema ASA R2 para otimizar a segurança e o desempenho do cluster.

Por exemplo, suponha que você tenha servidores NTP (Network Time Protocol) configurados para o cluster. No entanto, você não sabe que você tem menos do que o número recomendado de servidores NTP necessários para o gerenciamento ideal do tempo de cluster. Para ajudá-lo a evitar problemas que podem ocorrer quando a hora do cluster é imprecisa, o Insights irá notificá-lo de que você tem poucos servidores NTP configurados e lhe dará opções para saber mais sobre esse problema, corrigi-lo ou descartá-lo.

The screenshot shows the 'Insights' dashboard with the following alerts:

- Login banner isn't configured:** You haven't configured one or more login banner messages. You can create a custom login banner for the cluster or storage VM to inform visitors about terms and conditions, acceptable use, and site permissions. [Learn more about best practices for security.](#)
- Too few NTP servers are configured:** Problems can occur when the cluster time is inaccurate. Configure Network Time Protocol (NTP) servers to synchronize the cluster time with external NTP servers. For redundancy and accuracy, you should associate at least three NTP servers with the cluster. [Learn more about best practices for security.](#)
- Cluster isn't configured for automatic updates:** You aren't receiving automatic updates for this cluster. Enable automatic updates to always get the latest disk qualification package, disk firmware, shelf firmware, and SP/BMC firmware files when available.
- Global FIPS 140-2 compliance is disabled:** Global FIPS 140-2 compliance is disabled on this cluster. For security reasons, you should ensure ONTAP communicates with external clients or server components outside of ONTAP by using SSL communication that uses FIPS 140-2 compliant cryptography. [Learn more about best practices for security.](#)
- Cluster isn't configured for notifications:** You aren't receiving notifications from ONTAP about potential problems on the cluster. You can configure ONTAP to send notifications using email, a webhook, or an SNMP trapshot.

Passos

1. No System Manager, selecione **Insights**.

2. Reveja as recomendações.

O que vem a seguir

Execute todas as ações necessárias para implementar as práticas recomendadas e otimizar a segurança e o desempenho do cluster.

Exibir eventos e trabalhos de cluster em sistemas de storage ASA R2

Use o Gerenciador de sistema do ONTAP para exibir uma lista de erros ou alertas que ocorreram em seu sistema, juntamente com as ações corretivas recomendadas. Também pode visualizar registros de auditoria do sistema e uma lista de trabalhos ativos, concluídos ou com falha.

Passos



1. No System Manager, selecione **Eventos e trabalhos**.
2. Exibir eventos e trabalhos do cluster.

Para ver isto...	Faça isso...
Eventos de cluster	Selecione Eventos ; em seguida, selecione log de eventos .
Sugestões de Active IQ	Selecione Eventos ; em seguida, selecione sugestões Active IQ .
Alertas do sistema	<ol style="list-style-type: none">a. Selecione alertas do sistema.b. Selecione o alerta do sistema para o qual pretende agir.c. Confirme ou suprima o alerta.
Trabalhos de cluster	Selecione trabalhos .
Logs de auditoria	Selecione Registro de auditoria .

Envie notificações por e-mail para eventos de cluster e logs de auditoria

Configure o sistema para enviar uma notificação para endereços de e-mail específicos quando houver um evento de cluster ou entrada de log de auditoria.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Ao lado de **Gerenciamento de notificações**,  selecione .
3. Para configurar um destino de evento, selecione **Ver destinos de eventos**; em seguida, selecione **destinos de eventos**. Para configurar um destino de log de auditoria, selecione **Exibir destinos de auditoria**; em seguida, selecione **destinos de log de auditoria**.
4.  Selecione .
5. Introduza as informações de destino e, em seguida, selecione **Add**.

Resultado

O endereço de e-mail que você adicionou receberá agora as notificações de e-mail especificadas para eventos de cluster e logs de auditoria.

Gerenciar nós

Adicione nós do ASA R2 a um cluster do ONTAP


A partir do ONTAP 9.16.1, os sistemas de armazenamento ASA r2 suportam até 12 nós por cluster. Depois que os novos nós de um par HA forem cabeados e ligados, você precisará conectá-los ao cluster.

Antes de começar

Reúna as seguintes informações:

- O endereço IP do nó
- O endereço IP da interface de rede entre clusters
- A máscara de sub-rede entre clusters
- O gateway de rede entre clusters
- Se você quiser configurar o gerenciador de chaves integrado (OKM), você precisará da senha OKM.

Passos

1. No System Manager, selecione **Cluster > Overview**.
2. Selecione  ao lado do nó que deseja ingressar no cluster; em seguida, selecione **Adicionar nó**
3. Introduza o endereço IP de cada nó.
4. Introduza o endereço IP da interface de rede entre clusters, a máscara de sub-rede e o gateway.
5. Se você quiser configurar o gerenciador de chaves integrado (OKM), insira a senha OKM.

Configurar o gerenciador de chaves integrado para criptografia é selecionado por padrão.

6. Selecione **Adicionar**.

Resultado

O novo par de HA é Unido ao cluster.


O que se segue?

Depois de adicionar o novo par de HA ao cluster, você pode "[Habilite o acesso a dados de seus hosts SAN](#)" nos novos nós.

Reinicie um nó em um sistema de storage ASA R2

Talvez seja necessário reinicializar um nó para manutenção, solução de problemas, atualizações de software ou outros motivos administrativos. Quando um nó é reinicializado, o parceiro de HA executa automaticamente um takeover. Em seguida, o nó do parceiro executa um giveback automático após o nó reinicializado voltar online.

Passos

1. No System Manager, selecione **Cluster > Overview**.
2. Selecione  ao lado do nó que deseja reinicializar; em seguida, selecione **Reboot**.
3. Digite o motivo pelo qual você está reiniciando o nó; em seguida, selecione **Reboot**.

O motivo que introduzir para a reinicialização é registrado no registro de auditoria do sistema.


O que se segue?

Enquanto o nó está sendo reinicializado, seu parceiro de HA realiza um takeover para que não haja interrupção no serviço de dados. Quando a reinicialização estiver concluída, o parceiro de HA executa um giveback.

Renomeie um nó em um sistema de storage ASA R2

Você pode usar o Gerenciador de sistema do ONTAP para renomear um nó no sistema ASA R2. Talvez seja necessário renomear um nó para alinhar com as convenções de nomenclatura da sua organização ou por outros motivos administrativos.

Passos

1. No System Manager, selecione **Cluster > Overview**.
2. Selecione  ao lado do nó que deseja renomear; em seguida, selecione **Renomear**.
3. Insira o novo nome para o nó e selecione **Renomear**.

Resultado

O novo nome é aplicado ao nó.

Gerenciar contas de usuários e funções em sistemas de storage ASA R2

Use o System Manager para configurar o acesso do controlador de domínio do diretório ativo, a autenticação LDAP e SAML para suas contas de usuário. Crie funções de conta de usuário para definir funções específicas que os usuários atribuídos às funções podem executar no cluster.

Configurar o acesso do controlador de domínio do diretório ativo

Configure o acesso do controlador de domínio do ative Directory (AD) ao cluster ou à VM de armazenamento para que você possa habilitar o acesso à conta do AD.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Na seção **Segurança**, em **ative Directory**, selecione **Configurar**.

O que se segue?

Agora você pode ativar o acesso à conta AD no seu sistema ASA R2.


Configurar o LDAP

Configure um servidor LDAP (Lightweight Directory Access Protocol) para manter centralmente as informações do usuário para autenticação.

Antes de começar

Você deve ter gerado uma solicitação de assinatura de certificado e adicionado um certificado digital de servidor assinado pela CA.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Na seção **Segurança**, ao lado de **LDAP**,  selecione .
3. Introduza o servidor LDAP necessário e as informações de encadernação; em seguida, selecione **Guardar**.

O que se segue?

Agora você pode usar o LDAP para informações e autenticação do usuário.

Configurar a autenticação SAML

A autenticação SAML (Security Assertion Markup Language) permite que os usuários sejam autenticados por um provedor de identidade seguro (IDP) em vez dos provedores de serviços diretos, como ative Directory e LDAP.


Antes de começar

- O IDP que pretende utilizar para autenticação remota tem de ser configurado.

Consulte a documentação do IDP para obter a configuração.

- Você deve ter o URI do IDP.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Em **Segurança**, ao lado de **autenticação SAML**,  selecione .
3. Selecione **Ativar autenticação SAML**.
4. Insira o URL do IDP e o endereço IP do sistema host; em seguida, selecione **Salvar**.

Uma janela de confirmação exibe as informações de metadados, que foram copiadas automaticamente para a área de transferência.

5. Vá para o sistema IDP que você especificou; em seguida, copie os metadados da área de transferência para atualizar os metadados do sistema.
6. Retorne à janela de confirmação no System Manager; em seguida, selecione **Eu configurei o IDP com o URI do host ou metadados**.
7. Selecione **Logout** para ativar a autenticação baseada em SAML.

O sistema IDP exibirá uma tela de autenticação.

O que se segue?

Agora você pode usar a autenticação SAML para suas contas de usuário.

Criar funções de conta de usuário

As funções para administradores de cluster e administradores de VM de storage são criadas automaticamente quando o cluster é inicializado. Crie funções de conta de usuário adicionais para definir funções específicas que os usuários atribuídos às funções podem executar no cluster.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Na seção **Segurança**, ao lado de **usuários e funções**, →selecione .
3. Em **funções**, **+ Add** selecione .
4. Selecione os atributos da função.

Para adicionar vários atributos, **+ Add** selecione .

5. Selecione **Guardar**.

Resultado

Uma nova conta de usuário é criada e está disponível para uso no sistema ASA R2.

Crie uma conta de administrador

Crie uma conta de usuário administrador para permitir que o usuário da conta execute ações específicas no cluster com base na função atribuída à conta. Para melhorar a segurança da conta, configure a autenticação multifator (MFA) quando você criar a conta.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Na seção **Segurança**, ao lado de **usuários e funções**, →selecione .
3. Em **Users**, **+ Add** selecione .
4. Introduza um nome de utilizador e, em seguida, selecione uma função a atribuir ao utilizador.
5. Selecione o método de login do usuário e o método de autenticação.
6. Para ativar o MFA, **+ Add** selecione ; em seguida, selecione um método de login secundário e um método de autenticação
7. Introduza uma palavra-passe para o utilizador.
8. Selecione **Guardar**.

Resultado

Uma nova conta de administrador é criada e está disponível para uso no cluster do ASA R2.

Gerenciar certificados de segurança em sistemas de storage ASA R2

Use certificados de segurança digitais para verificar a identidade de servidores remotos.

O OCSP (Online Certificate Status Protocol) valida o status de solicitações de certificados digitais de serviços ONTAP usando conexões SSL e TLS (Transport Layer Security).

Gerar uma solicitação de assinatura de certificado

Gerar uma solicitação de assinatura de certificado (CSR) para criar uma chave privada que pode ser usada para gerar um certificado público.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Em **Segurança**, ao lado de **certificados**, → selecione ; em seguida, selecione **+ Generate CSR**.
3. Introduza o nome comum do assunto e, em seguida, selecione o país.
4. Se pretender alterar as predefinições do GSR, selecione a utilização de chave alargada ou adicione nomes alternativos de assunto, ↗ **More options** selecione ; em seguida, efetue as atualizações pretendidas.
5. Selecione **Generate**.

Resultado

Você gerou um CSR para o qual pode ser usado para gerar um certificado público.

Adicione uma autoridade de certificação confiável

O ONTAP fornece um conjunto padrão de certificados raiz confiáveis para aplicativos que usam a Segurança da camada de Transporte (TLS). Você pode adicionar autoridades de certificação confiáveis adicionais, conforme necessário.

Passos

1. Selecione **Cluster > Settings**.
2. Em **Segurança**, ao lado de **certificados**, → selecione .
3. Selecione **autoridades de certificação fidedignas**.
4. Introduza ou importe os detalhes do certificado; em seguida, **+ Add** selecione .

Resultado



Você adicionou uma nova autoridade de certificação confiável ao seu sistema ASA R2.

Renove ou exclua uma autoridade de certificação confiável

As autoridades de certificação confiáveis devem ser renovadas anualmente. Se você não quiser renovar um certificado expirado, você deve excluí-lo.

Passos

1. Selecione **Cluster > Settings**.
2. Em **Segurança**, ao lado de **certificados**, → selecione .
3. Selecione **autoridades de certificação fidedignas**.
4. Selecione a autoridade de certificação de confiança que pretende renovar ou eliminar.
5. Renovar ou eliminar a autoridade de certificação.

Para renovar a autoridade de certificação, faça isso...	Para excluir a autoridade de certificação, faça isso...
a.  Selecione ; em seguida, selecione Renew . b. Introduza ou importe as informações do certificado; em seguida, selecione Renew .	a.  Selecione ; em seguida, selecione Delete . b. Confirme que deseja excluir; em seguida, selecione Excluir .



Resultado

Renovou ou eliminou uma autoridade de certificação fidedigna existente no seu sistema ASA R2.

Adicione um certificado de cliente/servidor ou autoridades de certificação locais

Adicione um certificado de cliente/servidor ou autoridades de certificação locais para ativar serviços Web seguros.

Passos

1. No System Manager, selecione **Cluster > Settings**.
2. Em **Segurança**, ao lado de **certificados**,  selecione .
3. Selecione **certificados de cliente/servidor** ou **autoridades de certificação locais**.
4. Adicione as informações do certificado e  selecione .


Resultado



Adicionou um novo certificado de cliente/servidor ou autoridades locais ao seu sistema ASA R2.

Renovar ou eliminar um certificado de cliente/servidor ou autoridades de certificação locais

Os certificados de cliente/servidor e as autoridades de certificação locais devem ser renovados anualmente. Se você não quiser renovar um certificado expirado ou autoridades de certificado locais, você deve excluí-los.

Passos

1. Selecione **Cluster > Settings**.
2. Em **Segurança**, ao lado de certificados,  selecione .
3. Selecione **certificados de cliente/servidor** ou **autoridades de certificação locais**.
4. Selecione o certificado que pretende renovar ou eliminar.
5. Renovar ou eliminar a autoridade de certificação.

Para renovar a autoridade de certificação, faça isso...	Para excluir a autoridade de certificação, faça isso...
a.  Selecione ; em seguida, selecione Renew . b. Introduza ou importe as informações do certificado; em seguida, selecione Renew .	 Selecione ; em seguida, selecione Delete .

Resultado

Renovou ou eliminou um certificado cliente/servidor existente ou uma autoridade de certificação local no

seu sistema ASA R2.

Verifique a conectividade de host no sistema de storage ASA R2

Se houver um problema com as operações de dados do host, use o Gerenciador de sistema do ONTAP para verificar se a conexão do host ao sistema de storage do ASA R2 está ativa.

Passos

1. No System Manager, selecione **Host**.

O status de conectividade do host é indicado ao lado do nome do grupo de hosts da seguinte forma:

- **OK**: Indica que todos os iniciadores estão conectados a ambos os nós.
- **Parcialmente conectado**: Indica que alguns dos iniciadores não estão conectados a ambos os nós.
- **Nenhum conectado**: Indica que nenhum iniciador está conectado.

O que se segue?

Faça atualizações no seu host para corrigir problemas de conectividade. O ONTAP irá verificar novamente o estado da ligação a cada quinze minutos.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.