NetApp Console documentação de implantação local

NetApp Console local deployment

NetApp
August 10, 2026

Índice

NetApp Console implantação local

Notas de lançamento

Novidades na implantação local do NetApp Console

Saiba mais sobre os novos recursos e melhorias da versão mais recente da implantação local do NetApp Console.

Apresentando a implantação local do NetApp Console

"Saiba como implantar localmente o NetApp Console".

Limitações conhecidas na implantação local do NetApp Console

As limitações conhecidas identificam plataformas, dispositivos ou funções que não são compatíveis com esta versão do produto ou que não interoperam corretamente com ela. Analise estas limitações cuidadosamente.

Essas limitações são específicas da configuração do NetApp Console e da administração: o agente, a plataforma de software como serviço (SaaS) e outros.

Limitações da VM do NetApp Console

Possível conflito com endereços IP nos intervalos 10.42.0.0/16 e 10.43.0.0/16

NetApp Console local deployment utiliza um espaço de endereçamento fixo para a comunicação entre serviços. Os intervalos de endereço IP 10.42.0.0/16 e 10.43.0.0/16 são usados para a rede interna. Antes de implantar o Console local deployment, certifique-se de que esses intervalos de endereço IP não estejam atribuídos a outras VMs, escopos DHCP, registros DNS ou pools de VIP de balanceadores de carga nas VLANs disponibilizadas para o Console local deployment.

Consulte o artigo da Knowledge Base Agent IP conflict with existing network para obter instruções sobre como alterar o endereço IP das interfaces do agente.

Hosts Linux compartilhados não são suportados

O agente não é compatível com uma máquina virtual que é compartilhada com outros aplicativos. A máquina virtual deve ser dedicada ao software do agente.

Agentes e extensões de terceiros

Agentes de terceiros ou extensões de VM não são suportados na VM do agente.

Compare a implantação local do NetApp Console e o NetApp Console

Escolha o NetApp Console se você gerencia ambientes de nuvem e locais e deseja que a NetApp cuide da infraestrutura da plataforma. Escolha a implantação local do NetApp Console se você gerencia um grande ambiente ONTAP local e precisa de total soberania de dados e gerenciamento de storage voltado a políticas.

NetApp Console

NetApp hospeda e mantém o NetApp Console como um aplicativo SaaS. Você se inscreve e começa a gerenciar o storage imediatamente. Para gerenciar sistemas de storage, você implanta agentes leves do Console em seus ambientes de nuvem ou locais. Os agentes se conectam externamente à plataforma NetApp Console, e a NetApp gerencia automaticamente a autenticação, as atualizações e a disponibilidade da plataforma.

O NetApp Console também oferece suporte ao modo restrito (instalado em sua própria nuvem pública com conectividade de saída limitada) e ao modo privado (instalado localmente ou em sua nuvem sem conectividade com a plataforma NetApp Console, incluindo ambientes isolados da internet).

"Saiba mais sobre os modos de implantação do NetApp Console".

O NetApp Console oferece suporte à mais ampla gama de sistemas de storage, incluindo storage de nuvem como Amazon FSx for ONTAP, Cloud Volumes ONTAP, Amazon S3, Google Cloud Storage, E-Series, StorageGRID e clusters ONTAP locais. Ele fornece acesso ao conjunto completo de serviços de dados da NetApp, incluindo NetApp Backup and Recovery, NetApp Disaster Recovery, NetApp Ransomware Resilience, NetApp Copy and Sync e NetApp Data Classification. O NetApp Console também oferece recursos de contrato de suporte, como Digital Advisor, Lifecycle Planning e painéis de Sustainability.

O NetApp Console é mais adequado para organizações que gerenciam ambientes de nuvem híbrida e desejam o máximo de recursos, menos trabalho para manter tudo funcionando e licenciamento flexível.

"Saiba mais sobre o NetApp Console^."

NetApp Console implantação local

A implantação local do NetApp Console permite que você execute o plano de controle do NetApp Console inteiramente dentro da sua própria infraestrutura local, sem que nenhum tráfego de gerenciamento saia do seu ambiente. Você implanta o Console como uma máquina virtual usando uma imagem de appliance virtual e o gerencia como qualquer outra máquina virtual em seu ambiente vCenter. Não são necessários agentes do Console. A máquina virtual se comunica diretamente com seus clusters ONTAP.

Embora o NetApp Console no modo privado também ofereça suporte a implantações isoladas da internet e locais, a implantação local do Console foi projetada especificamente para o gerenciamento de frotas ONTAP em escala empresarial. Ela adiciona recursos que não estão disponíveis em nenhum modo de implantação do NetApp Console:

Políticas de classe de armazenamento

Defina os padrões de armazenamento uma única vez como modelos reutilizáveis que agrupam requisitos de desempenho, capacidade e hierarquização. Todo o provisionamento utiliza classes aprovadas, e a implantação local do Console monitora continuamente as cargas de trabalho para garantir a conformidade e identificar desvios.

Gerenciamento de frotas

Organize os clusters em pastas e frotas que reflitam a estrutura da sua empresa, depois delegue a administração no âmbito da organização, da pasta ou da frota.

Analisador de carga de trabalho

Correlacione latência, taxa de transferência, operações de entrada/saída por segundo e alterações de configuração ao longo do tempo para encontrar problemas de desempenho antes que eles afetem as cargas de trabalho.

Integração de modelos de linguagem em larga escala

Conecte-se ao seu próprio modelo de linguagem abrangente para provisionar storage usando linguagem natural, investigar alertas e obter respostas contextuais sobre seu ambiente de storage.

Remediação guiada e automatizada

Quando uma carga de trabalho se desvia de sua classe de armazenamento ou um alerta é acionado, a implantação local do Console fornece recomendações de correção. Use etapas guiadas ou a correção automatizada com um clique para restaurar a conformidade sem etapas manuais.

Envio de alertas por e-mail e webhook

Configure canais de notificação por e-mail e webhook para que os alertas cheguem às equipes certas quando as condições de storage mudarem. Os webhooks se integram às suas ferramentas de monitoramento e gerenciamento de incidentes existentes.

A implantação local do console oferece suporte a clusters ONTAP locais e ao NetApp Backup and Recovery. Ela se integra ao Active Directory para autenticação federada e oferece suporte à autenticação multifator para usuários locais.

A implantação local do Console é mais adequada para organizações com grandes ambientes ONTAP locais que exigem provisionamento voltado a políticas, verificações automatizadas de conformidade e total soberania de dados.

"Saiba mais sobre a implantação local do NetApp Console^."

Comparação de recursos

Gerenciamento de storage

Recurso	NetApp Console	NetApp Console implantação local
Clusters ONTAP locais	Sim (requer o agente do Console)	Sim (comunicação direta da máquina virtual Console)
Sistemas de storage de nuvem (Amazon FSx para ONTAP, Cloud Volumes ONTAP, Amazon S3 e outros)	Sim	Não
E-Series e StorageGRID	Sim	Não
NetApp Backup e recuperação	Sim	Sim
O NetApp Disaster Recovery	Sim	Não
O NetApp Ransomware Resilience	Sim	Não
O NetApp Copy and Sync	Sim	Não
NetApp Data Classification	Sim	Não
Digital Advisor, Planejamento do Ciclo de Vida, Sustentabilidade	Sim	Não
Políticas de classe de armazenamento e monitoramento de conformidade	Não	Sim
Remediação guiada e automatizada	Não	Sim

Recurso	NetApp Console	NetApp Console implantação local
Gerenciamento de frotas (pastas e frotas)	Não	Sim
Analisador de carga de trabalho	Não	Sim
Integração de modelo de linguagem de grande escala para operações assistidas por IA	Não	Sim

Configuração e segurança do console

Recurso	NetApp Console	NetApp Console implantação local
Modelo de implantação	Software como serviço, hospedado por NetApp (diferentes modos de implantação disponíveis)	Máquina virtual autogerenciada em sua própria infraestrutura
Agente do Console necessário	Sim	Não
Atualizações de software	Automático, gerenciado por NetApp	Manual
Acesso à interface do usuário	NetApp Console aplicativo (acesso pela internet ou máquina virtual)	Máquina virtual do Console (local, sem necessidade de internet)
Soberania de dados	O tráfego de gerenciamento vai para a plataforma NetApp Console	Nenhum tráfego de dados ou de gerenciamento sai do seu ambiente
Integração com o Active Directory	Não	Sim
Federação de identidades	Sim	Não
Autenticação multifator (usuários locais)	Sim	Sim
Registro de auditoria	Sim	Sim
Licenciamento	Assinaturas do Marketplace e bring-your-own-license	Traga sua própria licença

Comece agora

Saiba mais sobre a implantação local do NetApp Console

A implantação local do NetApp Console permite que você hospede e execute o plano de controle autônomo do NetApp Console em sua própria infraestrutura.

Você obtém gerenciamento de storage unificado, aplicação de políticas, automação em escala de fleet e operações assistidas por IA. Nenhum dado, metadado ou tráfego de gerenciamento sai do seu ambiente.

Implemente e opere o NetApp Console em sua própria infraestrutura

NetApp Console local é implantado em sua própria infraestrutura, então sua equipe controla a implantação, a conectividade e as operações diárias. Você implanta o agente do Console, mantém a máquina virtual do Console e gerencia os caminhos de rede necessários para o tráfego de monitoramento e gerenciamento. Isso oferece aos administradores corporativos controle total dos limites operacionais, mantendo os dados de gerenciamento dentro do ambiente.

- "Instale o NetApp Console em uma implantação local usando um OVA no vCenter".
- "Mantenha seu vCenter ou host ESXi para implantação local do NetApp Console".
- "Saiba mais sobre as portas para o agente do Console local na implantação local do NetApp Console".

Automatize as operações de storage com APIs e contas de serviço

NetApp Console local oferece suporte a integrações baseadas em API, permitindo que sua organização automatize operações de storage repetitivas. As contas de serviço permitem que os aplicativos se autentiquem e operem com funções atribuídas. Os mesmos controles de acesso baseado em funções e controles de auditoria aplicados a usuários interativos regem essas ações. Isso oferece suporte à automação empresarial, mantendo o acesso delimitado e rastreável.

- "Adicione membros à sua organização de implantação local do NetApp Console".
- "Saiba mais sobre a API do NetApp Console IAM"

Controle o acesso com RBAC e integração ao Active Directory

NetApp Console local oferece controle de acesso baseado em funções (RBAC) de confiança zero, que limita o que os usuários podem ver e fazer nas frotas e recursos que gerenciam. Você pode integrar com o Active Directory para que os usuários façam login com suas credenciais corporativas existentes, e os usuários locais podem adicionar autenticação multifator (MFA) para outra camada de verificação. A governança de acesso permanece alinhada com as práticas mais amplas de gerenciamento de identidade e acesso da sua organização.

- "Saiba mais sobre gerenciamento de identidade e acesso na implantação local do NetApp Console".
- "Saiba mais sobre o acesso seguro ao NetApp Console implantação local".

Organize frotas e delegue a administração de storage

NetApp Console local permite dimensionar a administração organizando recursos em pastas e frotas. Você pode mapear frotas para ambientes, unidades de negócios ou regiões e, em seguida, delegar a administração no âmbito da organização, da pasta ou da frota para manter a responsabilidade clara. Essa estrutura ajuda grandes equipes de storage a distribuir o trabalho sem perder a consistência das políticas ou a governança.

- "Saiba mais sobre pastas e frotas na implantação local do NetApp Console".
- "Saiba mais sobre frotas de armazenamento na implantação local do NetApp Console".

Rastrear e exportar atividades administrativas para fins de conformidade

Cada ação administrativa gera um registro de auditoria. As equipes de segurança e conformidade podem usar esses registros para investigar incidentes, demonstrar a eficácia dos controles e atender aos requisitos de auditoria. Exporte os logs de auditoria para o seu servidor syslog por meio de um webhook para monitoramento centralizado, maior retenção e análise. Como a implantação local do NetApp Console é executada em seu próprio ambiente, os dados de log nunca saem da sua infraestrutura.

- "Audite a atividade de implantação local do NetApp Console".

Provisione storage de forma consistente com as políticas de classe de storage

NetApp A implantação local do Console impõe o storage consistente por meio de classes de storage — modelos que agrupam desempenho, capacidade e políticas de tiering em definições reutilizáveis. Os administradores definem os padrões de storage uma única vez. Administradores e fluxos de trabalho automatizados usam essas classes aprovadas para toda atividade de provisionamento em seu ambiente. Isso impede a deriva de configuração, reduz o tempo que administradores menos experientes gastam em decisões de provisionamento e garante que toda carga de trabalho atenda imediatamente aos padrões da sua organização. Após o provisionamento, a implantação local do Console continua monitorando cada carga de trabalho para garantir a conformidade.

- "Saiba mais sobre como gerenciar o storage com a implantação local do NetApp Console".

Monitore a conformidade da classe de armazenamento e corrija desvios automaticamente

A implantação local do NetApp Console monitora cada carga de trabalho em relação à classe de armazenamento usada para provisioná-la. Quando uma carga de trabalho apresenta desvios, devido a uma alteração direta na configuração do cluster ou à degradação do desempenho, a implantação local do NetApp Console sinaliza a violação imediatamente. Os administradores podem seguir etapas de correção guiadas ou configurar a correção automatizada para resolver condições comuns de desvio sem intervenção manual. Essa aplicação contínua reduz o risco de auditoria e mantém seu ambiente em conformidade entre as revisões programadas.

Monitore a integridade do storage e receba alertas em todas as frotas

A implantação local do NetApp Console oferece a você um local centralizado para monitorar a integridade e o desempenho de cada cluster que você gerencia. Painéis de controle para toda a frota exibem clusters e volumes que precisam de atenção. Painéis de controle personalizados permitem que os administradores criem visualizações de monitoramento que correspondam às suas responsabilidades. O Workload Analyzer correlaciona latência, taxa de transferência, utilização de recursos e alterações de configuração ao longo do tempo para ajudar você a identificar as causas raiz antes que os problemas afetem as cargas de trabalho.

Configure canais de entrega de e-mail e webhook para que os alertas cheguem às equipes certas quando as condições mudam. Os administradores da organização configuram os destinos e os administradores de storage os aplicam nas regras de alerta para que os fluxos de resposta correspondam ao seu modelo operacional. Isso ajuda as equipes corporativas a responder mais rapidamente a eventos de capacidade, desempenho e proteção.

- "Saiba mais sobre como monitorar a integridade do storage na implantação local do NetApp Console".
- "Configure os canais de entrega de notificações na implantação local do NetApp Console".
- "Configure regras de notificação para alertas na implantação local do NetApp Console".

Provisione armazenamento e investigue alertas com linguagem natural

NetApp A implantação local do Console pode se conectar ao seu próprio large language model (LLM) para fornecer gerenciamento de storage assistido por IA. Você pode descrever uma carga de trabalho em linguagem simples para obter um plano de provisionamento, pedir ao Console para investigar um alerta ativo ou obter respostas contextuais sobre seu ambiente de storage. Cada ação de IA permanece dentro dos limites das suas classes de storage e dos controles de acesso baseado em funções que se aplicam à sua conta, e você deve confirmar operações confidenciais antes que elas prossigam. A implantação local do Console envia solicitações apenas para o endpoint LLM que seus administradores configurarem.

- "Saiba mais sobre a integração do LLM na implantação local do NetApp Console".

Faça backup e restaure o storage com o NetApp Backup and Recovery

Além do provisionamento e monitoramento, a implantação local do NetApp Console oferece acesso ao NetApp Backup and Recovery, permitindo que você proteja seus dados a partir da mesma interface. Você pode fazer backup e restaurar seus dados para atender aos seus requisitos de proteção e recuperação. Gerenciar a proteção de dados juntamente com seu storage mantém a governança consistente e reduz o número de ferramentas que suas equipes precisam para operar.

- "Saiba mais sobre os serviços de dados na implantação local do NetApp Console".

Saiba mais sobre o gerenciamento de identidade e acesso na implantação local do NetApp Console

O gerenciamento de identidade e acesso (IAM) na implantação local do NetApp Console controla quem pode fazer login, como as identidades são verificadas, a quais recursos os usuários podem acessar e quais ações eles podem executar. Na implantação local do NetApp Console, o IAM inclui controle de acesso baseado em funções (RBAC), autenticação multifator (MFA) e autenticação com suporte de diretório, além da hierarquia e do modelo de auditoria que dão suporte à administração delegada.

Use esta página para entender o modelo IAM de implantação local do NetApp Console em alto nível. Para exemplos detalhados de planejamento de hierarquia, "Saiba mais sobre pastas e frotas na implantação local do NetApp Console".

Você precisa ter as funções de *Super admin*, *Organization admin* ou *Folder or fleet admin* para gerenciar o IAM no NetApp Console.

O que significa IAM na implantação local do NetApp Console

NetApp Console implantação local do IAM combina verificação de identidade, controle de acesso, delegação e auditabilidade:

- A *autenticação* determina como os usuários fazem login, seja com credenciais locais ou por meio da configuração do seu diretório.
- A *autorização* determina o que os membros podem fazer depois de iniciarem sessão, com base em funções predefinidas e no escopo onde você os atribui.
- A hierarquia e o escopo determinam a quais pastas, frotas e recursos um membro pode acessar.
- O gerenciamento de membros e credenciais determina como você adiciona usuários, contas de serviço e como gerencia a MFA e os segredos das contas de serviço.
- O recurso *Auditoria e rastreamento de conformidade* registra a atividade relacionada ao IAM para que você possa revisar quem alterou o acesso e quando.

Como a autenticação funciona

NetApp Console local oferece suporte tanto a identidades locais quanto à integração de identidades externas.

Você pode integrar a implantação local do NetApp Console com o Active Directory para que os usuários façam login com suas credenciais corporativas existentes. Isso elimina a necessidade de senhas separadas na

implantação local do Console e permite que os administradores pesquisem usuários do diretório ao atribuir acesso.

Para usuários locais, a MFA adiciona mais uma etapa de verificação para reduzir o risco de acesso não autorizado caso as credenciais sejam comprometidas.

Para saber mais sobre autenticação e opções de login seguro, "Saiba mais sobre acesso seguro na implantação local do NetApp Console".

Como funciona a autorização

Após o usuário efetuar login, a implantação local do NetApp Console utiliza o RBAC para determinar o que esse usuário pode ver e fazer.

A integração com o Active Directory ou LDAP lida com autenticação. NetApp Console a autorização de implantação local permanece separada: os administradores atribuem funções predefinidas no nível da organização, pasta ou frota para controlar o que cada membro pode acessar.

A mesma função concede diferentes níveis de acesso efetivo dependendo do escopo em que você a atribui. Esse modelo permite que você conceda amplo acesso a administradores centrais, enquanto limita administradores regionais ou de equipe às frotas que eles gerenciam.

As funções que você atribui no nível de organização ou de pasta são herdadas pelos escopos filhos. Esse modelo de herança é uma parte fundamental de como o NetApp Console delega o acesso entre pastas e frotas.

NetApp projeta as funções de implantação local do NetApp Console com princípios de privilégio mínimo, para que cada função inclua apenas as permissões necessárias para suas tarefas.

"Saiba mais sobre controle de acesso baseado em funções e herança de funções na implantação local do NetApp Console".

Como funciona a hierarquia do IAM

NetApp Console local deployment usa uma hierarquia para agrupar recursos e definir o escopo de acesso. A organização está no topo, depois pastas, depois frotas e, por fim, os recursos (incluindo possíveis subpastas) associados a essas frotas.

Essa hierarquia é o que torna a delegação possível. Por exemplo, um administrador da organização pode gerenciar o acesso em toda a organização, enquanto um administrador de pasta ou de frota pode gerenciar apenas os recursos e membros dentro da parte da hierarquia que lhe pertence.

NetApp Console IAM é construído com base em três tipos de componentes: componentes organizacionais que definem a hierarquia, recursos que são atribuídos dentro dessa hierarquia e membros e funções que controlam quem pode acessar o quê.

Como as funções são herdadas nessa hierarquia, o design de suas pastas e frotas afeta diretamente a abrangência com que cada atribuição de acesso se aplica.

"Aprenda como adicionar frotas à sua organização.".

Segurança e credenciais de membro

O IAM na implantação local do NetApp Console também inclui controles operacionais para proteger o acesso dos membros após a existência das contas.

Para usuários locais, os administradores podem ajudar os usuários a recuperar o acesso, orientando a redefinição de senha, removendo ou desativando temporariamente a autenticação multifator (MFA) e revisando o comportamento da MFA do usuário local. Para contas de serviço, os administradores podem recriar as credenciais quando os segredos forem perdidos ou rotacionados.

Esses controles fazem parte do IAM porque determinam como as identidades permanecem seguras ao longo do tempo, não apenas como o acesso é atribuído inicialmente.

"Aprenda como gerenciar a segurança dos membros".

Auditar atividade de IAM

O IAM na implantação local do NetApp Console inclui a capacidade de revisar e exportar atividades relacionadas ao acesso.

Na página de Auditoria, você pode revisar ações relacionadas ao gerenciamento da sua organização, como adicionar membros, criar frotas e associar recursos. Você também pode filtrar os registros de auditoria pelo serviço Tenancy para focar em alterações relacionadas ao IAM ou exportar os logs de auditoria para um sistema externo.

A auditabilidade é um princípio importante do IAM porque permite verificar quem alterou o acesso, quando a alteração ocorreu e se a alteração foi bem-sucedida.

"Saiba como auditar a atividade de implantação local do NetApp Console".

Próximos passos com o IAM no NetApp Console

- "Comece a usar identidade e acesso no NetApp Console"
- "Saiba mais sobre acesso seguro na implantação local do NetApp Console"
- "Saiba mais sobre RBAC na implantação local do NetApp Console"
- "Monitore ou audite a atividade de implantação local do NetApp Console"
- "Saiba mais sobre a API do NetApp Console IAM"

Saiba mais sobre gerenciamento de frotas na implantação local do NetApp Console

O gerenciamento de frota no NetApp Console em implantação local é a prática de organizar sistemas de storage em grupos lógicos para que você possa aplicar políticas consistentes, controlar o acesso e monitorar a integridade em clusters relacionados. Em vez de gerenciar cada cluster de forma independente, o gerenciamento de frota permite que você trate sua frota como um pool comum de recursos para apoiar seus objetivos de storage.

À medida que seu ambiente de storage cresce, gerenciar clusters individuais torna-se impraticável. O gerenciamento de frota resolve esse problema, oferecendo uma maneira estruturada de agrupar sistemas relacionados, delegar responsabilidades e garantir que todos os clusters operem sob os mesmos padrões.

Por que o gerenciamento de fleet é importante

O gerenciamento de frotas aborda três desafios principais:

- **Simplificação por meio da abstração** - O gerenciamento de frota abstrai a complexidade do gerenciamento de infraestrutura de storage. Em vez de lidar com a configuração cluster por cluster, você gerencia seu ambiente de storage como um todo unificado, reduzindo a sobrecarga operacional e a fadiga de tomada de decisões.
- **Consistência e escalabilidade** - Sem uma organização clara, diferentes equipes tomam decisões diferentes para cargas de trabalho semelhantes, o que leva a configurações fragmentadas. O gerenciamento de frotas permite que você aplique padrões em dezenas de sistemas ao mesmo tempo, garantindo que novas cargas de trabalho partam da mesma base em todas as equipes e frotas.
- **Governança e controle** - À medida que as equipes crescem, você precisa de limites claros para quem pode gerenciar o quê. O gerenciamento de frotas fornece esses limites por meio de estrutura organizacional e controle de acesso, garantindo que as decisões de storage permaneçam governadas e auditáveis.

Como as frotas organizam seus recursos

A hierarquia de recursos da sua organização consiste em pastas e frotas:

Para uma visão geral detalhada da hierarquia e do modelo de acesso, consulte "Saiba mais sobre pastas e frotas na implantação local do NetApp Console".

- **Organização** - o nível mais alto que representa sua empresa.
- **Pastas** - Ajudam você a organizar frotas relacionadas. Por exemplo, você pode criar uma pasta para cada região ou unidade de negócios, depois criar frotas dentro de cada pasta. As pastas podem conter outras pastas ou frotas. Quando você atribui uma função no nível da pasta, os membros herdam essa função para todas as frotas dentro da pasta.
- **Frotas** - Agrupe os sistemas de storage que você gerencia. Você associa sistemas de storage a frotas e atribui membros às frotas para conceder acesso a eles.

> As pastas são uma ferramenta organizacional e não são visíveis para membros que não possuem permissões do IAM, como as funções de administrador da organização, administrador de pastas ou administrador de frota. Os membros acessam frotas, não pastas.

Padrões comuns de organização de frotas

A forma como você organiza suas frotas depende do seu modelo operacional:

- **Por ambiente** - Crie frotas separadas para cargas de trabalho de produção, desenvolvimento e teste. Isso mantém o storage de produção sob políticas mais rigorosas, ao mesmo tempo que permite maior flexibilidade em ambientes de menor criticidade.
- **Por unidade de negócio** - Agrupe clusters que atendem a um departamento específico, como finanças, engenharia ou RH, em uma frota dedicada. Você pode então atribuir responsabilidades de gerenciamento de storage a membros da equipe dentro dessa unidade de negócio, sem expor outras frotas a eles.
- **Por localização ou data center** - Quando os clusters estão distribuídos em vários locais, a organização por localização permite monitorar a integridade em nível de site, aplicar políticas específicas da região e acompanhar o consumo de capacidade por site.
- **Por camada de aplicativos** - Agrupe clusters que hospedam uma classe específica de carga de trabalho, como bancos de dados, compartilhamentos de arquivos ou máquinas virtuais, para que você possa aplicar padrões consistentes ajustados a esse tipo de carga de trabalho em toda a frota.

Utilize pastas para adicionar mais um nível de organização. Por exemplo, crie uma pasta para cada região e depois crie frotas baseadas em ambiente dentro de cada pasta regional.

Como o gerenciamento de fleet possibilita o controle de acesso

Frotas e pastas servem como limites para o acesso do usuário e a responsabilidade administrativa:

- **Acesso em nível de pasta** - Ao atribuir uma função em nível de pasta, o membro herda essa função para todas as frotas e recursos dentro da pasta. Isso permite delegar responsabilidades administrativas sem conceder acesso a toda a organização.
- **Acesso em nível de frota** - Ao atribuir uma função em nível de frota, o membro terá acesso apenas aos sistemas de storage dentro dessa frota. Isso permite delegar o gerenciamento de storage a membros da equipe ou proprietários de aplicativos sem expor partes não relacionadas da sua infraestrutura.

A implantação local do NetApp Console fornece monitoramento de integridade e desempenho em nível de frota, permitindo que você veja o status de todos os clusters em uma frota a partir de uma única visualização, identifique problemas precocemente e aja antes que eles afetem as cargas de trabalho.

Como o gerenciamento de storage funciona

O gerenciamento de storage é a prática de definir padrões de storage, aplicá-los de forma consistente e operar as cargas de trabalho para que permaneçam alinhadas ao longo do tempo. Na implantação local do NetApp Console, esses padrões são expressos como políticas de classe de storage e classes de storage, com escopo definido para frotas e aplicados por meio de fluxos de trabalho de provisionamento regidos por RBAC e registro de auditoria.

O deployment local do Console conecta quatro conceitos em um único fluxo de trabalho:

- **Frotas** definem o escopo em que você gerencia o storage. Uma frota agrupa sistemas para que você possa controlar o acesso, aplicar padrões de forma consistente e gerenciar recursos como uma unidade.
- **As políticas de classe de armazenamento** definem padrões como blocos de construção reutilizáveis (desempenho, capacidade, segurança, proteção de dados).
- **Classes de armazenamento** expressam a intenção da carga de trabalho. Uma classe de armazenamento é um modelo nomeado montado a partir de uma ou mais políticas.
- **Fluxos de trabalho de provisionamento** criam armazenamento dentro de limites definidos. Diferentes fluxos de trabalho tomam decisões de configuração de maneiras distintas, mas todos podem impor classes de armazenamento e permanecer regidos por RBAC e registro de auditoria.

Abordagens de provisionamento

A implantação local do NetApp Console oferece suporte a três abordagens de provisionamento, todas regidas por RBAC, registro de auditoria e padrões de classe de armazenamento:

- **Provisionamento manual** - Você seleciona o sistema de destino e especifica os detalhes de configuração diretamente. Use esta opção quando você precisar de controle explícito sobre a seleção e configuração do sistema.
- **Provisionamento automatizado** - Você fornece as informações da carga de trabalho e, opcionalmente, seleciona uma classe de armazenamento. A implantação local no Console recomenda o posicionamento mais adequado e aplica configurações baseadas em classe para reduzir decisões manuais.
- **Provisionamento assistido por IA (agente)** - você descreve o que precisa em linguagem natural. A implantação local no NetApp Console propõe um plano limitado por RBAC e classes de armazenamento,

e só faz o provisionamento depois que você revisa e aprova.

Para onde ir a seguir

- Para entender os padrões de storage, consulte "Saiba mais sobre classes e políticas de armazenamento na implantação local do NetApp Console".
- Para criar e gerenciar frotas, consulte "Gerencie pastas e frotas".
- "Provisionar storage manualmente"
- "Provisionar storage automaticamente"
- "Provisione storage com assistência de IA"

Saiba mais sobre classes e políticas de armazenamento na implantação local do NetApp Console

Uma classe de armazenamento é um modelo reutilizável que define como o armazenamento deve se comportar. Ao provisionar armazenamento usando uma classe de armazenamento, a implantação local do NetApp Console aplica automaticamente os padrões codificados nessa classe, sem exigir que os administradores tomem decisões de configuração individuais para cada carga de trabalho.

As classes de armazenamento são construídas a partir de políticas de classe de armazenamento, que definem dimensões individuais do comportamento do armazenamento. Juntas, elas permitem que você capture os padrões de armazenamento da sua organização uma única vez e os aplique de forma consistente em toda a sua frota.

O que são as políticas de classe de armazenamento

Uma política de classe de armazenamento define uma dimensão do comportamento do armazenamento. As políticas são blocos de construção reutilizáveis que você combina para criar classes de armazenamento.

Os tipos de políticas mais comuns incluem:

- **Políticas de desempenho** - Defina metas de latência, IOPS ou requisitos de taxa de transferência.
- **Políticas de capacidade** - Defina o modo de provisionamento, alertas de limite ou limites de crescimento.
- **Políticas de segurança** - Defina os requisitos de criptografia, conformidade ou controle de acesso.
- **Políticas de proteção de dados** - Defina cronogramas de snapshots, destinos de replicação ou períodos de retenção.

Você define as políticas de forma independente e, em seguida, as combina ao criar uma classe de storage. Isso permite reutilizar a mesma política de desempenho em várias classes ou atualizar uma política de capacidade em um único local e aplicar essa alteração a todas as classes que a utilizam.

O que são classes de armazenamento

Uma classe de armazenamento é um modelo nomeado, composto por uma ou mais políticas. Ela representa os padrões de storage da sua organização para um tipo específico de carga de trabalho.

Por exemplo, você pode criar uma classe de storage **Production Database** que combine alto desempenho, alta disponibilidade e políticas rigorosas de proteção de dados, ou uma classe de storage **Development File Share** que combine desempenho moderado, capacidade flexível e políticas básicas de proteção de dados.

Os administradores de armazenamento definem classes de armazenamento para codificar requisitos empresariais. Todas as atividades de provisionamento, sejam elas manuais, por meio de fluxos de trabalho guiados ou automatizadas, utilizam a biblioteca de classes aprovadas por esses administradores.

Como as classes de armazenamento impõem padrões

Ao provisionar storage, você seleciona uma classe de storage em vez de configurar definições individuais. A implantação local do NetApp Console usa as políticas dessa classe para identificar quais clusters em sua frota têm a capacidade e o desempenho necessários para suportar a carga de trabalho, recomendar a melhor opção de posicionamento e aplicar automaticamente as configurações baseadas na classe durante o provisionamento.

Após o provisionamento, a implantação local do Console avalia continuamente cada carga de trabalho em relação aos padrões de sua classe de storage.

Desvio e conformidade da storage class

Quando uma carga de trabalho deixa de corresponder à sua intenção de classe de armazenamento, a implementação local do Console a sinaliza para investigação e correção.

Os problemas se dividem em duas categorias:

- **Desvio de configuração**: As configurações de storage regidas pela política de classe de storage deixam de corresponder à configuração pretendida. Isso pode ocorrer quando as alterações são feitas diretamente no cluster ONTAP ou fora dos fluxos de trabalho de provisionamento padrão.
- **Não conformidade de desempenho**: o comportamento de tempo de execução da carga de trabalho não atende mais à intenção de desempenho da classe de armazenamento (por exemplo, pressão sustentada próxima a um limite de QoS ou latência de cauda elevada).

Uma visualização de análise explica o que mudou e por quê. Ações de remediação guiadas (por exemplo, **Corrigir**) podem estar disponíveis para ajudar você a restaurar a conformidade. Algumas remediações podem ser aplicadas no local, enquanto outras podem exigir alinhar a carga de trabalho a uma classe de storage diferente para restaurar o comportamento pretendido.

Onde investigar

Normalmente, você pode investigar desvios e não conformidades a partir de um destes locais (a disponibilidade depende da sua implementação e permissões):

- **Classes de armazenamento:** Deriva / Conformidade
- **Alertas:** analisar

Para obter instruções passo a passo, consulte Corrigir a deriva da storage class.

Fluxo de trabalho de ponta a ponta

Os passos a seguir descrevem o processo de utilização de classes de storage para padronizar e governar o storage em seu ambiente:

1. **Criar políticas de classe de armazenamento** - As políticas definem as dimensões individuais do comportamento do storage (metas de desempenho, configurações de capacidade, requisitos de segurança, cronogramas de proteção de dados). Crie políticas antes de criar uma classe de armazenamento.
2. **Criar uma classe de armazenamento** - Monte uma classe de armazenamento combinando uma política

de cada categoria aplicável. Você pode usar uma classe de armazenamento predefinida ou criar uma personalizada de acordo com os padrões da sua organização.

3. **Associe a classe de armazenamento a uma frota** - Depois de criar uma classe de armazenamento, associe-a à frota onde ela será usada para provisionamento e monitoramento de conformidade.
4. **Provisionar storage usando a classe de storage** - Ao provisionar um volume ou LUN, selecione uma classe de storage em vez de configurar definições individuais. A implementação local do NetApp Console usa a classe para recomendar o posicionamento de cluster mais adequado e, em seguida, provisiona com as configurações definidas na classe.
5. **Monitore cargas de trabalho para detecção de desvios** - A implantação local do NetApp Console avalia continuamente cada carga de trabalho em relação aos padrões codificados em sua classe de storage. Se ocorrer desvio de configuração ou não conformidade de desempenho, o sistema sinaliza o problema e pode gerar um alerta.
6. **Corrigir desvios para restaurar a conformidade** - Quando desvios ou não conformidades de desempenho são detectados, você pode seguir etapas guiadas para corrigir o problema manualmente, deixar que a implantação local do Console resolva automaticamente as condições comuns de desvio ou desassociar uma carga de trabalho de sua classe de armazenamento caso precise alterar suas configurações.

Como as classes de armazenamento funcionam com frotas

As classes de armazenamento são associadas a frotas. Quando você associa uma classe de armazenamento a uma frota, essa classe fica disponível para todo o provisionamento dentro da frota. Isso garante que todas as cargas de trabalho provisionadas na frota sigam os mesmos padrões, tornando as frotas a principal maneira de impor storage consistente em clusters relacionados.

Para obter detalhes sobre como organizar frotas, consulte "Saiba mais sobre gerenciamento de frotas na implantação local do NetApp Console".

Para onde ir a seguir

- Para entender a organização da frota, consulte "Saiba mais sobre gerenciamento de frotas na implantação local do NetApp Console".
- Para criar políticas e classes de armazenamento, consulte "Gerenciar classes de storage e políticas".
- "Provisionar storage manualmente"
- "Provisionar storage automaticamente"
- "Provisione storage com assistência de IA"
- Para analisar e remediar a deriva, consulte "Corrigir a deriva da storage class"

Saiba mais sobre a integração do LLM na implantação local do NetApp Console

NetApp Console implantação local se conecta a um large language model (LLM) para gerenciamento de storage com assistência de IA. Após a configuração, você pode usar linguagem natural para provisionar storage, investigar alertas e obter orientações sobre storage.

Esta documentação sobre como conectar um LLM ao assistente do Console para habilitar recursos de IA é fornecida como uma prévia da tecnologia. Com esta oferta de prévia, NetApp reserva-se o direito de modificar os detalhes, o conteúdo e o cronograma da oferta antes da Disponibilidade Geral.

O gerenciamento assistido por IA permite que os usuários descrevam as solicitações em linguagem simples, enquanto a implantação local do NetApp Console aplica suas políticas de storage.

A implantação local no NetApp Console envia solicitações LLM somente para o endpoint que você configurar.

O que você pode fazer com gerenciamento de storage assistido por IA

Ao ativar a integração com o LLM, a implantação local do Console oferece três funcionalidades por meio do assistente do Console:

- **Provisionamento de storage** Descreva os requisitos da carga de trabalho em linguagem simples. A implantação local no NetApp Console recomenda e executa um plano de provisionamento com base nas suas classes de storage.
- **Resposta ao alerta** Peça para a implantação local do NetApp Console investigar um alerta ativo. Ela analisa o problema e sugere ou executa uma ação com base nas permissões atribuídas.
- **Pesquisa e orientação** Faça perguntas sobre seu ambiente de storage ou administração do ONTAP. A implantação local do NetApp Console retorna respostas contextuais da documentação e do estado atual da frota.

Escolha acesso somente leitura ou leitura/gravação para o assistente do NetApp Console

Os usuários escolhem um modo de acesso ao assistente com base no resultado que desejam:

- Modo **somente leitura** para orientação e investigação sem fazer alterações na infraestrutura.
- Modo **leitura/gravação** para execução guiada. A implantação local no console exibe a ação proposta, solicita confirmação e, em seguida, executa a alteração.

Entenda o que controla as ações do assistente do NetApp Console

A implantação local do Console controla as ações do assistente do Console por meio do mesmo modelo de governança usado em toda a plataforma:

- Os controles de acesso baseados em funções limitam o que cada usuário pode ver e fazer.
- As políticas de storage restringem o provisionamento e as ações relacionadas.
- O assistente do NetApp Console requer confirmação antes de executar ações que alteram o storage.

Escolha um caminho de provedor de LLM

NetApp Console a implantação local oferece suporte a estes tipos de provedores LLM:

- **OpenAI** para acesso direto ao modelo OpenAI.
- **Compatível com OpenAI** para um endpoint compatível, como um gateway corporativo ou serviço de proxy.
- Anthropic para os modelos Claude da Anthropic.

A disponibilidade do modelo depende do endpoint que você configurar. Selecione um modelo na lista em implantação local do NetApp Console.

Para obter detalhes sobre os modelos compatíveis, consulte "Saiba mais sobre os provedores e modelos de LLM compatíveis na implantação local do NetApp Console".

Entenda para onde vão os pedidos de LLM

O fluxo de dados depende do caminho do endpoint que você escolher:

- Se você configurar um endpoint da OpenAI, a implantação local do NetApp Console enviará prompts e contexto para o endpoint da OpenAI.
- Se você configurar um endpoint compatível com OpenAI, a implantação local do Console enviará prompts e contexto para o endpoint compatível que sua organização configurar.

Proteja as credenciais do LLM e controle o acesso administrativo

Proteja a integração com estes controles:

- Trate a chave da API como uma credencial privilegiada e faça a rotação dela de acordo com a política da sua organização.
- Analise o uso e os alertas do lado do provedor para detectar atividades inesperadas.

Conecte seu LLM

Após tomar essas decisões, continue com "Conecte seu LLM e ative o assistente do NetApp Console".

Se a conexão ou as verificações de tempo de execução falharem, consulte "Solução de problemas de integração do LLM".

Saiba mais sobre o NetApp Backup and Recovery na implantação local do NetApp Console

O NetApp Backup and Recovery é um serviço de dados que fornece proteção de dados eficiente, segura e econômica para todas as suas cargas de trabalho do ONTAP, incluindo volumes, bancos de dados, máquinas virtuais e cargas de trabalho do Kubernetes.

Uma carga de trabalho é um agrupamento lógico de recursos dentro de um sistema, gerenciado como uma única unidade para proteção, governança, detecção e recuperação. Em Backup e Recovery, uma carga de trabalho é a unidade que você protege. Seu significado depende da fonte de dados: para Kubernetes uma carga de trabalho é um aplicativo, para ambientes de máquina virtual é uma máquina virtual, e para ambientes de banco de dados é um banco de dados.

O suporte para backup e recuperação já está integrado a todos os sistemas ONTAP, portanto não há necessidade de hardware adicional ou gateways de mídia. Isso torna as operações de backup simples e econômicas. O NetApp Console simplifica a implementação de qualquer estratégia de backup, incluindo toda a gama de variantes de backup 3-2-1, sem a necessidade de múltiplos gerentes de recursos ou pessoal especializado.

NetApp Backup and Recovery está em modo de pré-visualização para implantação local no NetApp Console. O serviço ainda não está disponível para o público em geral e os recursos e funcionalidades estão sujeitos a alterações.

"Saiba mais sobre o NetApp Backup and Recovery.".

Instale e configure

Guia rápido para configurar o NetApp Console na implantação local

Após instalar o NetApp Console localmente, configure sua organização para que as equipes certas possam gerenciar com segurança os recursos de storage certos. Use esta lista de verificação para planejar sua estrutura, organizar recursos, adicionar membros, configurar integrações e habilitar serviços de dados.

Funções de acesso necessárias

Superadministrador ou administrador da organização. "Saiba mais sobre funções de acesso".

Instalar o NetApp Console implantação local

- Analise o fluxo de trabalho de instalação para compreender o processo de implantação. "Saiba mais sobre o fluxo de trabalho de instalação para implantação local do NetApp Console".
- Instale a implantação local do NetApp Console no seu vCenter. "Instale a implantação local do NetApp Console".

Planeje sua organização

- Aprenda como pastas e frotas organizam seus recursos. "Saiba mais sobre pastas e frotas".
- Entenda como o controle de acesso baseado em funções (RBAC) concede aos membros o acesso de que precisam. "Saiba mais sobre o controle de acesso baseado em funções na implantação local do NetApp Console".
- Analise o fluxo de trabalho de gerenciamento de identidade e acesso. "Comece a usar o IAM para gerenciamento de recursos e de frotas".

Configure sua organização

- Adicione seus sistemas de armazenamento ao NetApp Console implantação local. "Adicionar sistemas de armazenamento".
- Crie a hierarquia de pastas e frota que corresponda à estrutura da sua empresa. "Crie pastas e frotas".
- Associe os recursos às pastas e frotas corretas. "Associe recursos a pastas e frotas".
- Adicione membros e atribua suas funções iniciais. "Adicione membros e atribua funções".

Configure integrações e serviços

- Integre com o Active Directory para que os usuários do diretório possam acessar a implantação local do Console "Integrar com o Active Directory".
- Conecte seu modelo de linguagem amplo (LLM) para habilitar o assistente do NetApp Console e o gerenciamento assistido por IA. "Conecte seu LLM".
- Configure como a implantação local do NetApp Console entrega notificações. "Configurar o envio de notificações".

5 Configurar o NetApp Backup and Recovery

- "Obtenha uma licença para o NetApp Backup and Recovery". Você pode pular esta etapa se não desejar ter acesso aos serviços avançados de backup e recuperação.
- Adicione a licença do NetApp Backup and Recovery à implantação local do NetApp Console. "Adicione a licença ao NetApp Console implantação local".
- "Conceda aos usuários acesso ao NetApp Backup and Recovery".

Instalar NetApp Console

Instale o NetApp Console em uma implantação local usando um OVA no vCenter

Você usa um arquivo OVA para instalar uma implantação local do NetApp Console no seu vCenter. O download ou a URL do OVA estão disponíveis no site de suporte da NetApp.

Prepare-se para instalar o NetApp Console na implantação local

Antes da instalação, certifique-se de que seu host de máquina virtual atenda aos requisitos e que a implantação local do NetApp Console possa acessar a internet e as redes de destino. Para usar os serviços de dados do NetApp, como o NetApp Backup and Recovery, crie credenciais do provedor de nuvem para que a implantação local do NetApp Console execute ações em seu nome.

Analise os requisitos do host de implantação local do NetApp Console

Certifique-se de que sua máquina host atenda aos requisitos de instalação antes de instalar a implantação local do NetApp Console.

- CPU: 16 núcleos ou 16 vCPUs
- RAM: 64 GB
- Espaço em disco: 596 GB (provisionamento espesso recomendado)
- vSphere 7.0u3 ou superior, com versão de hardware virtual 19 ou superior

Instale o NetApp Console em uma implantação local em um ambiente vCenter, em vez de diretamente em um host ESXi.

Configure o acesso à rede para a implantação local do NetApp Console

NetApp Console local deployment utiliza um espaço de endereçamento fixo para a comunicação entre serviços. Os intervalos de endereço IP 10.42.0.0/16 e 10.43.0.0/16 são usados para a rede interna. Antes de implantar o Console local deployment, certifique-se de que esses intervalos de endereço IP não estejam atribuídos a outras VMs, escopos DHCP, registros DNS ou pools de VIP de balanceadores de carga nas VLANs disponibilizadas para o Console local deployment.

Consulte o artigo da Knowledge Base Agent IP conflict with existing network para obter instruções sobre como alterar o endereço IP das interfaces do agente.

Instale o NetApp Console implantação local em seu ambiente vCenter

NetApp oferece suporte à instalação do NetApp Console para implantação local em seu ambiente vCenter. O

arquivo OVA inclui uma imagem de máquina virtual pré-configurada que você pode implantar em seu ambiente VMware.

Baixe o OVA ou copie o URL

Baixe o OVA.

1. Faça o download do software de implantação local do Console no NetApp Support Site.

Implante o NetApp Console local no seu vCenter

Faça login no seu ambiente vCenter para implantar a implantação local do Console.

Passos

1. Faça o upload do certificado autoassinado para seus certificados confiáveis, caso seu ambiente exija. Você pode substituir este certificado após a instalação.
2. Implante o OVA a partir da biblioteca de conteúdo ou do sistema local.

Do sistema local	Da biblioteca de conteúdo
a. Clique com o botão direito do mouse e selecione **Implantar modelo OVF…**. b. Escolha o arquivo OVA na URL ou navegue até o local onde ele está armazenado, depois selecione **Avançar**.	a. Acesse sua biblioteca de conteúdo e selecione o OVA do Console. b. Selecione **Ações** > **Nova VM a partir deste modelo**

3. Conclua o assistente de implantação do modelo OVF para implantar o Console.
4. Selecione um nome e uma pasta para a máquina virtual e, em seguida, selecione **Avançar**.
5. Selecione um recurso de computação e, em seguida, selecione **Avançar**.
6. Analise os detalhes do modelo e selecione **Avançar**.
7. Aceite o contrato de licença e selecione **Avançar**.
8. Escolha o tipo de configuração de proxy que você deseja usar: proxy explícito, proxy transparente ou nenhum proxy.
9. Selecione o datastore onde você deseja implantar a VM e, em seguida, selecione **Avançar**. Certifique-se de que ele atenda aos requisitos do host.
10. Selecione a rede à qual você deseja conectar a VM e, em seguida, selecione **Avançar**. Certifique-se de que a rede seja IPv4 e tenha acesso à internet de saída para os endpoints necessários.
11. Na janela **Personalizar modelo**, preencha os seguintes campos:
    - **Informações de proxy**
      - Se você selecionou proxy explícito, insira o nome do host ou endereço IP do servidor proxy e o número da porta, bem como o nome de usuário e a senha.
      - Se você selecionou o proxy transparente, faça o upload do respectivo certificado.
    - **Configuração de Máquina Virtual**
      - **Ignorar verificação de configuração**: Esta caixa de seleção está desmarcada por padrão, o que significa que o NetApp Console implantação local executa uma verificação de configuração para validar o acesso à rede.
        - NetApp recomenda deixar esta caixa desmarcada para que a instalação inclua uma verificação de configuração da implantação local do NetApp Console. A verificação de configuração valida

se a implantação local do NetApp Console tem acesso à rede aos endpoints necessários. Se a implantação falhar devido a problemas de conectividade, você pode acessar o relatório de validação e os logs no host da implantação local do NetApp Console. Em alguns casos, se você tiver certeza de que a implantação local do NetApp Console tem acesso à rede, pode optar por ignorar a verificação.

- **Senha de manutenção**: Defina a senha para o usuário `maint` que permite o acesso ao console de manutenção da implantação local do NetApp Console.
- **Servidores NTP**: especifique um ou mais servidores NTP para sincronização de tempo.
- **Nome do host**: Defina o nome do host para esta VM. Ele não deve incluir o nome de domínio de pesquisa. Por exemplo, um FQDN como console10.searchdomain.company.com deve ser inserido como console10.
- **DNS primário**: Especifique o servidor DNS primário a ser usado para resolução de nomes.
- **Secondary DNS**: Especifique o servidor DNS secundário a ser usado para a resolução de nomes.
- Domínios de pesquisa: especifique o nome de domínio a ser usado ao resolver o nome do host. Por exemplo, se o FQDN for console10.searchdomain.company.com, insira searchdomain.company.com.
- **Endereço IPv4**: O endereço IP que está associado ao nome do host.
- **Máscara de sub-rede IPv4**: A máscara de sub-rede para o endereço IPv4.
- **Endereço de gateway IPv4**: O endereço de gateway para o endereço IPv4.

12. Selecione **Next**.
13. Confira os detalhes na janela **Pronto para concluir** e selecione **Concluir**.

    A barra de tarefas do vSphere mostra o progresso enquanto a implantação local do NetApp Console está sendo realizada.

14. Ligue a máquina virtual.

Planeje a organização do seu NetApp Console

Comece a usar identidade e acesso na implantação local do NetApp Console

Na implantação local do NetApp Console, configure sua hierarquia de pastas e frotas, adicione membros e permissões iniciais e adicione e coloque recursos nas frotas corretas para que as equipes certas possam acessá-los e gerenciá-los.

Funções de acesso necessárias

Superadministrador, administrador da organização ou administrador de pasta ou frota. "Saiba mais sobre funções de acesso".

Você precisa da função de **Organization admin** ou **Super admin** para concluir a configuração inicial. Após a configuração, gerencie recursos, acesso dos membros e acesso à frota conforme sua organização mudar.

Adicionar ou descobrir recursos

Adicione sistemas à implantação local do Console. Durante a configuração inicial, os sistemas geralmente são adicionados enquanto a frota padrão está selecionada.

Aprenda como criar ou descobrir recursos:

- "Clusters ONTAP locais"

2 Crie sua pasta e hierarquia de frota

Crie frotas e pastas adicionais que correspondam à hierarquia da sua empresa.

"Aprenda a organizar seus recursos com pastas e frotas".

3 Associe os recursos às frotas corretas

Adicionar ou descobrir um sistema na implantação local do Console associa automaticamente o recurso à frota selecionada no momento. Para disponibilizar um sistema às equipes certas, associe-o às frotas apropriadas em sua hierarquia.

- "Aprenda a gerenciar recursos em pastas e frotas".

4 Adicione membros e atribua permissões iniciais

Adicione membros e atribua funções a eles no nível da organização, da pasta ou da frota, com base no que eles gerenciam.

"Aprenda a gerenciar membros e suas permissões".

Após a configuração inicial

Após a configuração inicial estar concluída, gerencie o acesso e o posicionamento de recursos conforme sua organização muda:

- "Gerencie recursos em pastas e frotas"
- "Gerencie o acesso de membros em frotas e pastas (centrado no membro)"
- "Gerencie quem pode acessar uma frota ou pasta específica (centrado na frota)"
- "Exclua pastas e frotas quando não forem mais necessárias"

Informações relacionadas

- "Saiba mais sobre gerenciamento de identidade e acesso no NetApp Console"
- "Saiba mais sobre a API de identidade e acesso"

Saiba mais sobre pastas e frotas na implantação local do NetApp Console

Na implantação local do NetApp Console, use pastas e storage fleets para organizar seus recursos do NetApp e controlar o acesso de acordo com a estrutura da sua empresa, seja por local, departamento ou tipo de carga de trabalho.

Use esta página para estratégia de hierarquia e padrões de design de frota. Para um modelo IAM completo de membros, funções e escopo de recursos, "Saiba mais sobre gerenciamento de identidade e acesso na implantação local do NetApp Console".

Você organiza os recursos em uma hierarquia: a organização está no topo, seguida pelas pastas (que podem conter outras pastas ou frotas) e, por fim, as frotas, que contêm os sistemas de storage. Atribua funções de

acesso no nível da organização, da pasta ou da frota para que os usuários tenham o acesso correto aos recursos.

Você precisa ter a função de administrador da organização, da pasta ou da frota para gerenciar pastas e frotas na implantação local do NetApp Console.

Componentes organizacionais

Os componentes organizacionais — organização, pastas e frotas — formam uma hierarquia que determina como os recursos são agrupados e como o acesso é delegado.

Organização

Uma organização é o nível mais alto da hierarquia de implantação local do NetApp Console e normalmente representa sua empresa. Sua organização consiste em pastas, frotas, membros, funções e recursos. Os recursos são associados às frotas e os membros recebem funções no nível da organização, da pasta ou da frota.

Pastas

As pastas agrupam frotas relacionadas para organizá-las por local, site ou unidade de negócios. Você não pode associar sistemas de storage diretamente às pastas, mas atribuir uma função a um membro no nível da pasta concede a ele acesso a todas as frotas dessa pasta.

Os administradores da organização podem adicionar um recurso a uma pasta para delegar a tarefa de associar o recurso às frotas a um administrador da pasta ou da frota "Associe recursos a pastas e frotas".

Frotas

As frotas agrupam sistemas de storage. Atribua recursos às frotas e conceda acesso aos membros no nível da frota. Os recursos podem pertencer a várias frotas. Os membros com acesso à frota podem gerenciar os recursos dessa frota.

Por exemplo, você pode associar um sistema ONTAP local a uma única frota ou a todas as frotas da sua organização, dependendo das suas necessidades.

"Aprenda como criar pastas e frotas de armazenamento".

Recursos

Um recurso é um sistema de storage que a implantação local do Console reconhece e que pode ser atribuído a uma frota. Associe um recurso a uma frota para que os usuários com acesso à frota possam gerenciar o recurso.

Por exemplo, você pode associar um ONTAP cluster a uma frota ou a todas as frotas da sua organização. A forma como você associa um recurso depende das necessidades da sua organização.

"Aprenda como associar recursos a frotas".

Membros e funções

Os membros são os usuários e as contas de serviço da sua organização. As funções definem quais ações eles podem executar e em qual nível da hierarquia: organização, pasta ou frota.

Membros

Os membros da sua organização são contas de usuário ou contas de serviço. Uma conta de serviço é normalmente usada por um aplicativo para concluir tarefas específicas sem intervenção humana.

Usuários com a função de administrador da organização podem adicionar novos membros à sua organização. Todos os usuários (incluindo contas de serviço e usuários do Active Directory) devem ser adicionados explicitamente e receber pelo menos uma função para acessar a implantação local do Console.

"Aprenda como adicionar membros à sua organização".

Funções de acesso

A implantação local do Console fornece funções de acesso que você pode atribuir aos membros da sua organização.

Ao associar um membro a uma função, você pode conceder essa função para toda a organização, uma pasta específica ou uma frota específica. A função que você selecionar concede ao membro permissão para os recursos na parte selecionada da hierarquia.

A implantação local do NetApp Console fornece funções granulares que seguem o princípio do menor privilégio, o que significa que as funções de acesso são projetadas para dar aos membros acesso apenas ao que eles precisam.

Os usuários podem desempenhar múltiplas funções à medida que suas responsabilidades se expandem.

Herança de funções

Ao atribuir uma função no nível da organização ou da pasta, as subpastas, frotas e recursos subordinados herdam essa função, então o design da sua pasta e frota determina a abrangência de cada atribuição.

"Saiba mais sobre herança de funções na implantação local do NetApp Console".

Exemplos de design organizacional

A estrutura organizacional ideal depende do tamanho da sua organização e de como suas equipes estão organizadas. Os exemplos a seguir mostram como diferentes organizações podem usar a hierarquia de pastas e de frotas para gerenciar o acesso de forma eficaz.

Estratégia para pequenas organizações

Para organizações com menos de 50 usuários e gerenciamento centralizado de storage, considere uma abordagem simplificada usando as funções de Super admin e Super viewer.

Exemplo: ABC Corporation (equipe de 5 pessoas)

- **Estrutura**: Organização única com 3 frotas (Produção, Desenvolvimento, Backup)
- **Funções**:
  - 2 membros seniores: função de super admin para acesso administrativo completo
  - 3 membros da equipe: função de supervisualizador para monitoramento sem direitos de modificação
- **Benefícios**: administração simplificada, complexidade de funções reduzida, adequado para equipes que necessitam de amplo acesso

Estratégia empresarial multirregional

Para grandes organizações com operações regionais e equipes especializadas, implemente uma abordagem hierárquica com pastas representando limites geográficos ou de unidades de negócios.

Exemplo: XYZ Corporation (empresa multinacional)

- **Estrutura**: Organização > Pastas regionais (North America, Europe, Asia-Pacific) > Frotas por região
- **Funções da plataforma**:
  - 1. Admin de organização: supervisão global e gerenciamento de políticas
  - 3 Administradores de pastas ou frotas: controle regional (um por região)
  - 1. Administrador da federação: integração do serviço de diretório corporativo
- **Funções de storage por região**:
  - Administrador de armazenamento: descubra e gerencie sistemas de armazenamento em regiões atribuídas
  - Visualizador de armazenamento: monitore recursos de storage em diferentes regiões
  - Especialista em saúde do sistema: gerencie a saúde do storage sem modificações no sistema
- **Benefícios**: Segurança reforçada por meio da segregação de funções, autonomia regional e conformidade com as regulamentações locais

Estratégia de especialização departamental

Para organizações com equipes especializadas que exigem acesso específico, utilize atribuições de funções direcionadas com base em responsabilidades funcionais.

Exemplo: TechCorp (empresa de tecnologia de médio porte)

- **Estrutura**: Organização > Pastas de departamento (TI, Segurança, Desenvolvimento) > Recursos específicos da frota
- **Funções especializadas**:
  - Equipe de segurança: funções de administrador de resiliência a ransomware e visualizador de classificação
  - Equipe de backup: superadministrador de backup e recuperação para operações de backup abrangentes
  - Equipe de desenvolvimento: administrador de storage para gerenciamento de ambiente de teste
  - Equipe de conformidade: analista de suporte operacional para monitoramento e gerenciamento de casos de suporte
- **Benefícios**: controle de acesso personalizado, maior eficiência operacional e responsabilidade clara por tarefas especializadas

Próximos passos

- "Crie pastas e frotas de storage"
- "Associe recursos a pastas e frotas"
- "Gerencie as atribuições de acesso à frota"
- "Monitore ou audite as ações de implantação local do NetApp Console"

Saiba mais sobre o controle de acesso baseado em funções na implantação local do NetApp Console

Gerencie o acesso do usuário à implantação local da NetApp Console com controle de acesso baseado em funções (RBAC), atribuindo funções predefinidas no nível da organização, pasta ou frota. Cada função concede permissões específicas que definem quais ações os usuários podem executar dentro do escopo atribuído.

NetApp projeta funções de implantação local do Console com privilégios mínimos, de forma que cada função inclua apenas as permissões necessárias para suas tarefas. Essa abordagem aumenta a segurança ao limitar o acesso ao que cada membro precisa.

Depois de organizar os recursos em pastas e frotas, atribua aos membros da organização uma função ou funções para pastas ou frotas específicas, que permitam que eles executem apenas suas responsabilidades.

Por exemplo, você pode atribuir a um membro a função de administrador de Backup e Recovery para um nível de frota específico, permitindo que ele execute operações de Backup e Recovery para recursos dentro dessa frota, sem conceder a ele acesso mais amplo a toda a organização. Esse mesmo usuário pode receber a função para várias frotas dentro da sua organização.

Você pode atribuir várias funções a membros para o mesmo escopo ou para escopos diferentes, dependendo de suas responsabilidades. Por exemplo, uma organização menor pode atribuir ao mesmo membro as funções de Storage admin e Backup and Recovery admin no nível da organização, enquanto uma organização maior pode ter membros diferentes atribuídos a cada função no nível da fleet.

Tipos de membros da organização Console

NetApp Console a implantação local oferece suporte aos seguintes tipos de membros:

- *Usuários*: Usuários individuais podem ser usuários locais que você adiciona à implantação local do NetApp Console e que usam credenciais locais, ou usuários de diretório que se autenticam por meio do seu serviço integrado de Active Directory ou LDAP. Ambos os tipos de usuários podem receber funções na implantação local do NetApp Console para acessar recursos.
- *Contas de serviço*: Contas não humanas que aplicativos ou serviços usam para interagir com a implantação local do NetApp Console por meio de APIs. Você pode adicionar contas de serviço diretamente à sua organização de implantação local do Console.

"Aprenda como adicionar membros à sua organização."

Funções predefinidas na implantação local do NetApp Console

A implantação local do NetApp Console inclui funções predefinidas que você pode atribuir a membros da organização. Cada função inclui permissões que especificam quais ações um membro pode realizar dentro de seu escopo atribuído (organização, pasta ou frota).

NetApp Console funções de implantação local usam princípios de privilégio mínimo que garantem que os membros tenham apenas as permissões necessárias para suas tarefas e categorizam as funções pelo tipo de acesso que fornecem:

- Funções da plataforma: conceder permissões de administração de implantação local do Console
- Funções de serviços de dados: conceder permissões para gerenciar serviços de dados específicos, como Resiliência a Ransomware e Backup e Recuperação
- Funções do aplicativo: fornecem permissões para gerenciar o storage, além de auditar eventos e alertas de implantação local do NetApp Console

Você pode atribuir várias funções a um membro com base em suas responsabilidades. Por exemplo, você pode atribuir a um membro tanto a função de administrador de storage quanto a função de administrador de backup e recuperação para uma frota específica.

Para definir o nível de acesso de um membro, associe a categoria da função às responsabilidades do membro e, em seguida, atribua a função no escopo (organização, pasta ou frota) que corresponda à abrangência do acesso que o membro deve ter. "Saiba como diferentes organizações estruturam funções e escopo na implantação local do NetApp Console".

"Saiba mais sobre as funções predefinidas que você pode atribuir aos membros na implantação local do NetApp Console".

Como funciona a herança de funções

Ao atribuir uma função no nível da organização ou da pasta, essa função é herdada pelos escopos filhos dentro dessa parte da hierarquia. Isso significa que as funções no nível da organização se aplicam a toda a organização, as funções no nível da pasta se aplicam a todas as pastas e frotas filhas dessa pasta, e as funções no nível da frota se aplicam somente aos recursos dessa frota.

Use o escopo que corresponda ao acesso que você deseja que o membro mantenha. Por exemplo, atribua uma função no nível da pasta quando o membro precisar do mesmo acesso em várias frotas em uma região. Atribua a função no nível da frota quando o membro precisar acessar apenas uma frota.

Não é possível sobrescrever o acesso herdado em um escopo inferior. Se um membro herdar uma função da organização ou de uma pasta, altere essa atribuição no escopo superior onde você a concedeu originalmente.

"Saiba mais sobre pastas e frotas na implantação local do NetApp Console". "Gerencie o acesso de membros". "Gerencie as atribuições de acesso à frota".

Configure a organização do seu NetApp Console

Adicione pastas e frotas à sua organização de implantação local do NetApp Console

Crie pastas e frotas que correspondam à estrutura da sua empresa, controle o acesso e organize os recursos na implantação local do NetApp Console.

Funções de acesso necessárias

Superadministrador, administrador da organização ou administrador de pasta ou frota. "Saiba mais sobre funções de acesso".

A implantação local do NetApp Console cria uma frota padrão quando você cria uma organização. Você pode adicionar mais frotas e agrupá-las em pastas. "Saiba mais sobre a hierarquia de recursos no NetApp Console".

Utilizando pastas e frotas para organizar recursos

Pastas e frotas são os dois elementos fundamentais que você usa para moldar sua organização de forma que ela reflita a maneira como suas equipes realmente trabalham. Por exemplo, uma pasta por região, com uma frota de produção e uma de desenvolvimento dentro de cada uma.

- As pastas agrupam frotas relacionadas e oferecem suporte à administração delegada e à herança de funções.
- As frotas são onde você associa recursos para gerenciamento e como você concede acesso operacional aos usuários.

Você pode criar pastas e frotas primeiro e adicionar recursos e acesso de membros depois. Isso permite que você planeje sua hierarquia de recursos antes de adicionar usuários e recursos na implantação local do Console. Se sua estrutura já estiver definida, você pode adicionar recursos e atribuir acesso ao criar a frota. Você pode atualizar as frotas a qualquer momento.

Por exemplo, coloque os clusters de produção em uma frota de Produção e os clusters de teste em uma frota de Teste, e conceda a cada equipe acesso apenas à frota que ela possui.

Pastas

As pastas organizam as frotas por estrutura de negócios, como unidade de negócios, região ou equipe. Você pode aninhar pastas para refletir sua organização.

As funções atribuídas no nível de uma pasta são herdadas pelas subpastas e frotas. Você também pode usar uma pasta para delegar tarefas de atribuição de frota a um administrador de pasta ou de frota para essa parte da hierarquia.

> Os membros trabalham em frotas, não em pastas. Um recurso associado apenas a uma pasta não pode ser gerenciado pelos membros até que seja associado a uma frota.

Por exemplo, uma empresa regional poderia usar pastas para organizar o ONTAP por unidade de negócios e carga de trabalho. Ela poderia criar uma pasta de nível superior para North America, subpastas para Production e Development, e frotas para clusters ONTAP que hospedam SAP, VMware e volumes de backup. Os administradores de armazenamento atribuídos à pasta North America herdam acesso a todas as frotas filhas, enquanto as equipes de aplicativos têm acesso apenas às frotas que gerenciam.

Frotas

Associe recursos a frotas para que os membros possam gerenciá-los. Uma frota pode existir diretamente sob a organização ou dentro de uma pasta.

Por exemplo, uma empresa de saúde utiliza o ONTAP storage em frotas separadas para produção e desenvolvimento. A frota de produção executa aplicativos clínicos e bancos de dados de prontuário de pacientes, enquanto a frota de desenvolvimento oferece suporte a testes e validação. Essa separação protege os dados ativos, impõe um acesso mais restrito à produção, oferece suporte à auditabilidade e aos controles de menor privilégio, e permite que as equipes de desenvolvimento trabalhem sem impactar as cargas de trabalho voltadas para o paciente.

Os usuários navegam entre as frotas atribuídas na página **Sistemas** para gerenciar os recursos associados a cada frota.

Adicione uma pasta ou frota

Adicione uma frota sempre que precisar de um novo limite para recursos e acesso de membros, e adicione uma pasta quando quiser agrupar frotas relacionadas e delegar sua administração. Por exemplo, adicione uma `Production` pasta contendo uma `Production-US-East` frota e uma `Production-EU-West` frota, em seguida, atribua a um líder regional a função de administrador da pasta ou da frota apenas para a frota dele.

Você pode criar até sete níveis hierárquicos.

Você pode adicionar recursos e atribuir acesso a membros ao criar uma frota ou pasta, ou pode fazer isso depois.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Organization**.
3. Na página **Organização**, selecione **Adicionar pasta ou frota**.
4. Selecione **Pasta** ou **Frota**.
5. Em **Nome e localização**: insira um nome e escolha uma localização para a pasta ou frota.

1. Opcional: expanda a seção **Recursos** para associar recursos à frota ou pasta.
   a. Marque a caixa de seleção ao lado do recurso que você deseja associar e selecione **Associar à frota**. Se você ainda não adicionou sistemas à implantação local do Console, pode fazer isso mais tarde.

   > Os membros não podem acessar os recursos em uma pasta até que esses recursos sejam atribuídos a uma fleet.

2. Opcional: expanda a seção **Acesso** para atribuir acesso aos membros. Selecione **Adicionar um membro** para atribuir acesso e uma função. Por padrão, o usuário que cria a frota tem acesso a ela.

   "Saiba mais sobre funções de acesso".

3. Selecione **Add**.

Renomear uma pasta ou fleet

Renomeie uma pasta ou frota conforme necessário. A renomeação não afeta os recursos associados nem o acesso dos membros.

Passos

1. Na página **Organização**, navegue até uma frota ou pasta na tabela, selecione ••• e, em seguida, selecione **Editar pasta** ou **Editar frota**.
2. Na página **Editar**, insira um novo nome e selecione **Aplicar**.

Excluir uma pasta ou frota

Exclua pastas e frotas que você não precisa mais, como após uma reestruturação da equipe ou conclusão da frota.

Antes de excluir uma pasta ou frota, realize as seguintes verificações:

- Verifique se a pasta ou frota não contém recursos. "Aprenda como remover associações de recursos".
- Analise os membros que ainda têm acesso à pasta ou à frota. "Visualizar atribuições de acesso de membros".
- Remova ou atualize o acesso de membros conforme necessário. "Modificar atribuições de acesso de membros".
- Se você estiver excluindo uma frota, primeiro transfira recursos para a frota de destino. "Saiba como mover recursos entre frotas".

Passos

1. Na página **Organização**, navegue até uma frota ou pasta na tabela, selecione ••• e, em seguida, selecione **Excluir**.

2. Confirme que você deseja excluir a pasta ou a frota.

Gerencie frotas e pastas na implantação local do NetApp Console

Após a configuração inicial, você pode fazer o seguinte:

- **Gerencie associações de recursos para pastas e frotas**: "Aprenda como associar recursos a frotas e pastas".
- **Visualizar ou atualizar o acesso a uma pasta ou frota**: "Aprenda como conceder acesso de usuários às frotas".
- **Gerencie um membro em várias pastas e frotas**: "Aprenda como gerenciar o acesso de membros".
- **Adicione membros adicionais e atribua permissões iniciais**: "Aprenda a gerenciar membros e permissões".

Informações relacionadas

- "Saiba mais sobre identidade e acesso no NetApp Console"
- "Comece a usar identidade e acesso no NetApp Console"
- "Gerencie as atribuições de acesso à frota"
- "Saiba mais sobre a API de identidade e acesso"

Adicionar sistemas de storage à implantação local do NetApp Console

Adicione sistemas de storage ao NetApp Console implantação local para habilitar o monitoramento, o gerenciamento de inventário e a administração da sua infraestrutura de storage. Após a adição de um sistema de storage, o Console implantação local descobre o sistema e começa a coletar informações que podem ser usadas para tarefas de monitoramento e gerenciamento.

Antes de começar, certifique-se de que você possui as permissões necessárias para adicionar sistemas de storage e que o sistema de storage esteja acessível a partir da implantação local do NetApp Console.

Passos

1. Selecione **Storage > Management**.
2. Na lista suspensa "Escopo", selecione a frota à qual você deseja adicionar um sistema de storage.
3. Selecione **Adicionar sistema**.
4. Insira os detalhes necessários do sistema de storage, incluindo informações de conexão e credenciais.
5. Revise as informações que você inseriu e selecione **Adicionar**.

   O sistema de storage é adicionado à frota selecionada. A implantação local do Console inicia a descoberta e o monitoramento do sistema. Dependendo do ambiente e da conectividade de rede, pode levar alguns minutos para que o sistema apareça como totalmente gerenciado.

> Você também pode adicionar um sistema de storage na página **Administração > Identidade e acesso**, selecionando **Adicionar sistema** e fornecendo as informações necessárias do sistema.

Gerencie recursos em pastas e frotas na implantação local do NetApp Console

Gerencie o acesso a recursos no NetApp Console em implantação local associando os recursos à pasta ou frota correta, o que controla quais equipes podem acessá-los e gerenciá-los.

Funções de acesso necessárias

Superadministrador, administrador da organização ou administrador de pasta ou frota. "Saiba mais sobre funções de acesso".

Coloque os recursos onde as equipes certas possam gerenciá-los, mova-os quando a propriedade mudar e remova as associações quando não forem mais necessárias.

Um *recurso* é uma entidade que a implantação local do Console reconhece, como um recurso de storage ou uma carga de trabalho de Backup e Recovery.

Tipos de recursos do Console

A implantação local do NetApp Console oferece suporte a recursos de storage e cargas de trabalho de backup e recuperação. Associe qualquer tipo de recurso a uma frota para controlar o acesso e o gerenciamento.

Recursos de storage

Os recursos de storage são o tipo de recurso mais comum em sua organização. Ao adicionar um sistema de storage à implantação local do Console, associe-o a uma frota para que as equipes apropriadas possam acessá-lo e gerenciá-lo. Por exemplo, após adicionar um ONTAP cluster, associe-o à `Production-US-East`frota.

Cargas de trabalho de backup e recuperação

As cargas de trabalho de Backup and Recovery também são consideradas recursos. Você pode atribuir permissões de membro para acessar cargas de trabalho de Backup and Recovery associando essas cargas de trabalho a frotas. Por exemplo, atribua o acesso de um membro a uma carga de trabalho de Backup and Recovery associando-a a uma frota à qual o membro possa acessar e concedendo a função apropriada de Backup and Recovery.

Veja os recursos na sua organização

Visualize os recursos da sua organização para encontrar um recurso específico e ver a quais frotas ou pastas ele está associado. Se você não criou nenhuma pasta ou frota, todos os recursos são associados à frota padrão diretamente subordinada à organização.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Recursos**.
3. Selecione **Pesquisa e filtragem avançadas**.
4. Use as opções disponíveis para encontrar um recurso:
   - **Pesquisar por nome do recurso**: digite uma cadeia de texto e selecione **Adicionar**.
   - **Plataforma**: Selecione uma ou mais plataformas, como Amazon Web Services.
   - **Recursos**: Selecione um ou mais recursos, como o Cloud Volumes ONTAP.
   - **Organização, pasta ou frota**: selecione toda a organização, uma pasta específica ou uma frota específica.

5. Selecione **Pesquisar**.

Associe um recurso a uma pasta ou frota

Associe um recurso a uma frota ou pasta para que as equipes apropriadas possam gerenciá-lo. Por exemplo, após adicionar um ONTAP cluster, associe-o à `Production-US-East` frota para que os administradores de storage regionais dessa frota possam gerenciá-lo.

Usuários com a função de administrador da organização podem adicionar recursos a uma pasta para delegar tarefas de associação de frota ao administrador da pasta ou da frota correspondente. "Associe um recurso a uma pasta".

Passos

1. Na página **Recursos**, navegue até um recurso na tabela, selecione ••• e, em seguida, selecione **Associar a uma pasta ou frota**.
2. Selecione uma pasta ou frota e, em seguida, selecione **Aceitar**.
3. Para associar uma pasta ou frota adicional, selecione **Adicionar pasta ou frota** e, em seguida, selecione a pasta ou frota.

   Observe que você só pode selecionar entre as pastas e frotas para as quais você tem permissões de administrador.

4. Selecione **Associar recursos**.
   - Se você associou o recurso a frotas, os membros que têm permissões para essas frotas agora podem acessar o recurso a partir do Console.
   - Se você associou o recurso a uma pasta, um administrador de pasta ou de frota agora pode acessar o recurso e associá-lo a uma frota dentro da pasta. "Associe um recurso a uma pasta".

Veja as pastas e frotas associadas a um recurso

Verifique a quais frotas ou pastas um recurso está associado.

Para verificar quais membros têm acesso ao recurso, consulte os membros atribuídos à pasta ou frota associada. "Gerencie as atribuições de acesso à frota".

Passos

1. Na página **Recursos**, navegue até um recurso na tabela, selecione ••• e, em seguida, selecione **Ver detalhes**.

O exemplo a seguir mostra um recurso associado a uma frota.

Para ver quais membros têm acesso ao recurso, revise a pasta ou frota associada.

"Gerencie as atribuições de acesso à frota". "Gerencie o acesso de membros".

Remover um recurso de uma pasta ou frota

Remova a associação de um recurso a uma pasta ou frota para impedir que os membros o gerenciem lá.

Para remover um sistema de storage de toda a organização, acesse a página **Sistemas** e remova o sistema.

Passos

1. Na página **Recursos**, navegue até um recurso na tabela, selecione ••• e, em seguida, selecione **Ver detalhes**.
2. Para remover um recurso de uma pasta ou frota, selecione 🗑 ao lado da pasta ou frota.
3. Selecione **Excluir** para remover a associação.

Mover um recurso entre frotas

Transfira um recurso de uma frota para outra removendo sua associação com a frota atual e, em seguida, associando-o à frota de destino.

O acesso ao recurso muda assim que a associação muda. Se possível, conclua ambas as etapas em uma única janela de manutenção.

Passos

1. Na página **Recursos**, navegue até um recurso na tabela, selecione ••• e, em seguida, selecione **Ver detalhes**.
2. Selecione 🗑 ao lado da frota atual e selecione **Excluir**.
3. Selecione **Adicionar pasta ou fleet**.
4. Selecione a frota desejada e selecione **Aceitar**.
5. Selecione **Associar recursos**.

Informações relacionadas

- "Saiba mais sobre identidade e acesso no NetApp Console"
- "Comece a usar identidade e acesso no NetApp Console"
- "Gerencie as atribuições de acesso à frota após mover recursos"
- "Saiba mais sobre a API de identidade e acesso"

Adicione membros à sua organização de implantação local do NetApp Console

Adicione membros à sua organização de implantação local do NetApp Console e atribua funções para conceder acesso no nível da organização, pasta ou frota para usuários, contas de serviço e usuários do diretório.

Funções de acesso necessárias

Superadministrador, administrador da organização ou administrador de pastas ou frotas (para pastas e frotas

que estão administrando). "Saiba mais sobre funções de acesso".

Antes de começar

- Crie a hierarquia de pastas e frota que corresponda à sua organização. "Aprenda a organizar seus recursos com pastas e frotas".
- Associe os recursos às frotas corretas antes de atribuir acesso aos membros. "Aprenda a gerenciar recursos em pastas e frotas".
- Se você estiver adicionando um usuário ao diretório, integre primeiro o seu serviço de diretório. "Aprenda como integrar com o seu serviço de diretório".

Entenda como o acesso é concedido na implantação local do NetApp Console

O NetApp Console utiliza controle de acesso baseado em funções (RBAC) para gerenciar permissões. Atribua funções aos membros para fornecer o acesso necessário. Cada função define as ações permitidas para recursos específicos.

Observe o seguinte sobre a concessão de acesso na implantação local do NetApp Console:

- Você deve adicionar explicitamente cada usuário à sua organização e atribuir pelo menos uma função a ele antes que esse usuário possa acessar os recursos.
- Uma função que você atribui no nível da organização ou da pasta é herdada pelos escopos filhos, portanto, escolha o escopo de atribuição com cuidado para conceder ao membro acesso somente onde for necessário. "Saiba mais sobre herança de funções na implantação local do NetApp Console".

Adicione membros à sua organização

O NetApp Console suporta três tipos de membros: contas de usuário, usuários do diretório e contas de serviço.

Primeiro, você precisa configurar um servidor de e-mail para usar com a implantação local do Console antes de adicionar usuários. "Aprenda como configurar um servidor de e-mail."

Os usuários do diretório se autenticam por meio do seu serviço de diretório integrado, mas você ainda precisa adicionar cada usuário do diretório individualmente e atribuir funções na implantação local do Console. Crie contas de serviço diretamente no Console.

Todos os membros devem ter pelo menos uma função explicitamente atribuída a eles para acessar a implantação local do Console.

Ao adicionar um membro, escolha a organização, pasta ou frota à qual o membro precisa de acesso e atribua a função inicial ou funções de que ele precisa.

Adicionar uma conta de usuário

Você precisa ter a função de administrador da organização, pasta ou frota para adicionar um usuário a uma organização, pasta ou frota para que ele possa acessar os recursos.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Members**.
3. Selecione **Adicionar um membro**.

4. Para **Tipo de membro**, mantenha **Usuário** selecionado.
5. Para **E-mail do usuário**, insira o endereço de e-mail do usuário que está associado ao login que ele criou.
6. Use a seção **Selecione uma organização, pasta ou frota** para escolher onde o membro precisa de acesso.

   Observe o seguinte:

   - Você pode selecionar apenas as pastas e frotas para as quais você tem permissões.
   - Ao selecionar uma organização ou pasta, você concede ao membro permissões para todo o seu conteúdo.
   - Você só pode atribuir a função de **Organization admin** no nível da organização.
7. **Selecione uma categoria** e, em seguida, selecione uma **Função** que conceda ao membro as permissões iniciais necessárias para a organização, pasta ou frota que você selecionou.

   "Saiba mais sobre funções de acesso".
8. Para conceder acesso a mais pastas, frotas ou funções, selecione **Adicionar função**, escolha a categoria de pasta, frota ou função e selecione uma função.
9. Selecione **Add**.

   O Console envia instruções ao usuário por e-mail.

Adicionar uma conta de serviço

Adicione uma conta de serviço quando você precisar automatizar tarefas ou se conectar com segurança às APIs do Console. Depois de criar a conta, copie o client ID e o client secret para a integração que irá usá-la.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Members**.
3. Selecione **Adicionar um membro**.
4. Em **Tipo de membro**, selecione **Conta de serviço**.
5. Insira um nome para a conta de serviço.
6. Use a seção **Selecione uma organização, pasta ou frota** para escolher onde a conta de serviço precisa de acesso.

   Observe o seguinte:

   - Você só pode selecionar entre as pastas e frotas para as quais você tem permissões.
   - Selecionar uma organização ou pasta concede ao membro permissões para todo o seu conteúdo.
   - Você só pode atribuir a função de **Organization admin** no nível da organização.
7. Selecione uma **Categoria** e, em seguida, selecione uma **Função** que conceda à conta de serviço as permissões iniciais necessárias para a organização, pasta ou frota que você selecionou.

   "Saiba mais sobre funções de acesso".
8. Para conceder acesso a mais pastas, frotas ou funções, selecione **Adicionar função**, escolha a categoria de pasta, frota ou função e selecione uma função.

9. Baixe ou copie o client ID e o client secret.

   O Console exibe o segredo do cliente apenas uma vez. Copie-o em local seguro; você poderá recriá-lo posteriormente caso o perca.

10. Selecione **Fechar**.

Adicione um usuário de diretório à sua organização

Adicione um usuário do seu serviço de diretório integrado e conceda a ele as primeiras funções. Por exemplo, adicione um novo engenheiro de storage do Active Directory e atribua a função de Storage admin na `Production-US-East` frota para que ele possa trabalhar nessa frota.

Primeiro você precisa configurar o serviço de diretório antes de poder adicionar usuários ao diretório. "Aprenda como integrar com o seu serviço de diretório".

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Members**.
3. Selecione **Adicionar um membro**.
4. Em **Tipo de membro**, selecione **Usuário do diretório**.
5. No campo **E-mail do usuário**, insira o endereço de e-mail do usuário do diretório que você deseja adicionar. Este endereço de e-mail deve corresponder ao endereço de e-mail associado ao login do usuário em seu diretório.
6. Use a seção **Selecione uma organização, pasta ou frota** para escolher onde o usuário do diretório precisa de acesso.

   Observe o seguinte:

   - Você só pode selecionar entre as pastas e frotas para as quais você tem permissões.
   - Selecionar uma organização ou pasta concede ao membro permissões para todo o seu conteúdo.
   - Você só pode atribuir a função de **Organization admin** no nível da organização.
7. Selecione uma **Categoria** e, em seguida, selecione uma **Função** que conceda ao usuário do diretório as permissões iniciais necessárias para a organização, pasta ou frota que você selecionou.

   "Saiba mais sobre funções de acesso".

8. Para conceder ao usuário acesso adicional a outras pastas, frotas ou funções, selecione **Adicionar função**, escolha a pasta ou frota, a categoria da função e selecione uma função.

Funções de acesso

NetApp Console funções de acesso de implantação local

O gerenciamento de identidade e acesso (IAM) na implantação local do NetApp Console fornece funções predefinidas que você pode atribuir aos membros da sua organização em diferentes níveis da sua hierarquia de recursos. Antes de atribuir essas funções, você deve entender as permissões que cada função inclui. As funções se enquadram nas seguintes categorias: plataforma, aplicativo e serviço de dados.

Funções da plataforma

As funções da plataforma concedem ao NetApp Console permissões de administração da implantação local, incluindo atribuição de funções e gerenciamento de usuários. A implantação local do Console possui diversas funções de plataforma.

Função da plataforma	Responsabilidades
"Administrador da organização"	Permite ao usuário acesso irrestrito a todas as frotas e pastas dentro de uma organização, adicionar membros a qualquer frota ou pasta, bem como executar qualquer tarefa e usar qualquer serviço de dados que não tenha uma função explícita associada a ele. Usuários com essa função gerenciam sua organização criando pastas e frotas, atribuindo funções, adicionando usuários e gerenciando sistemas, desde que possuam as credenciais adequadas.
"Administrador de pasta ou de fleet"	Permite ao usuário acesso irrestrito às frotas e pastas atribuídas. Pode adicionar membros às pastas ou frotas que gerencia, bem como executar qualquer tarefa e usar qualquer serviço de dados ou aplicativo nos recursos dentro da pasta ou frota à qual está atribuído.
"Administração da federação"	Permite que um usuário crie e gerencie federações de serviços de diretório com o NetApp Console, para que os usuários possam se autenticar com suas credenciais de diretório existentes.
"Visualizador da federação"	Permite que um usuário visualize as federações de serviço de diretório existentes no Console. Não permite criar ou gerenciar federações.
"Superadministrador"	Concede ao usuário todas as funções de administrador. Essa função foi criada para organizações menores que podem não precisar distribuir as responsabilidades do Console entre vários usuários.
"Super visualizador"	Concede ao usuário todas as funções de visualizador. Essa função foi criada para organizações menores que podem não precisar distribuir as responsabilidades do Console entre vários usuários.

Funções do aplicativo

A seguir, apresentamos uma lista de funções na categoria de aplicativos. Cada função concede permissões específicas dentro do seu escopo designado. Usuários sem a função de aplicativo ou plataforma necessária não podem acessar o respectivo aplicativo.

Função do aplicativo	Responsabilidades
"Analista de suporte operacional"	Fornece acesso a alertas e ferramentas de monitoramento, como a página Audit.
"Administrador de storage"	Administrar as funções de integridade e governança do storage, descobrir recursos de storage, bem como modificar e excluir sistemas existentes.
"Visualizador de storage"	Visualize a integridade do storage e as funções de governança, bem como visualize recursos de storage previamente descobertos. Não é possível descobrir, modificar ou excluir sistemas de storage existentes.
"Especialista em integridade do sistema"	Administrar as funções de armazenamento, integridade e governança, todas as permissões do administrador de armazenamento, exceto não pode modificar ou excluir sistemas existentes.

Funções do serviço de dados

A seguir está uma lista de funções na categoria de serviço de dados. Cada função concede permissões específicas dentro do seu escopo designado. Usuários que não tiverem a função de serviço de dados necessária ou uma função de plataforma não poderão acessar o serviço de dados.

Função do serviço de dados	Responsabilidades
"Superadministrador de backup e recuperação"	Execute quaisquer ações em NetApp Backup and Recovery.
"Administrador de backup e recuperação"	Realize backups para snapshots locais, replique para storage secundário e faça backup para storage de objetos.
"Administrador de backup e recuperação de restauração"	Restaurar cargas de trabalho no Backup e Recovery.
"Administrador de clones de backup e recuperação"	Clone aplicativos e dados no Backup e Recovery.
"Visualizador de backup e recuperação"	Veja as informações de Backup and Recovery.
Visualizador de classificação	Permite que os usuários visualizem os resultados da verificação de NetApp Data Classification. Usuários com essa função podem visualizar informações de conformidade e gerar relatórios para recursos aos quais têm permissão de acesso. Esses usuários não podem habilitar ou desabilitar a verificação de volumes, buckets ou esquemas de banco de dados. Data Classification não possui uma função de administrador.
Administrador do SnapCenter	Fornece a capacidade de fazer backup de snapshots de clusters ONTAP locais usando o NetApp Backup and Recovery para aplicativos. Um membro com essa função pode realizar as seguintes ações: * Concluir qualquer ação em Backup and Recovery > Applications * Gerenciar todos os sistemas nas frotas e pastas para as quais possui permissões * Usar todos os serviços do NetApp Console SnapCenter não possui função de visualizador.

Links relacionados

- "Saiba mais sobre o gerenciamento de identidade e acesso do NetApp Console"
- "Comece a usar identidade e acesso no NetApp Console"
- "Adicione membros e atribua funções em uma organização do NetApp Console"
- "Saiba mais sobre a API do NetApp Console IAM"

NetApp Console funções de acesso à plataforma de implantação local

Atribua funções de plataforma aos usuários para conceder permissões para gerenciar a implantação local do NetApp Console, atribuir funções, adicionar usuários, criar frotas e gerenciar autenticação.

Exemplo de funções organizacionais para uma grande organização multinacional

A XYZ Corporation organiza o acesso ao storage por região — América do Norte, Europa e Ásia-Pacífico — proporcionando controle regional com supervisão centralizada.

O **Administrador da organização** na implantação local do Console da XYZ Corporation cria uma organização inicial e pastas separadas para cada região. O **Administrador de pastas ou frotas** de cada região organiza as frotas (com os recursos associados) dentro da pasta da região.

Os administradores regionais com a função de **Administrador de pastas ou frotas** gerenciam ativamente suas pastas, adicionando recursos e usuários. Esses administradores regionais também podem adicionar, remover ou renomear pastas e frotas que gerenciam. O **Administrador da organização** herda permissões para quaisquer novos recursos, mantendo a visibilidade do uso de storage em toda a organização.

Dentro da mesma organização, um usuário recebe a função de **Federation admin** para gerenciar a federação da organização com seu IdP corporativo. Esse usuário pode adicionar ou remover organizações federadas, mas não pode gerenciar usuários ou recursos dentro da organização. O **Organization admin** atribui a um usuário a função de **Federation viewer** para verificar o status da federação e visualizar as organizações federadas.

As tabelas a seguir indicam as ações que cada função da plataforma de implantação local do NetApp Console pode executar.

Funções de administração organizacional

Tarefa	Administrador da organização	Administrador de pasta ou de fleet
Criar, modificar ou excluir sistemas da implantação local do NetApp Console (adicionar ou descobrir sistemas)	Sim	Sim
Criar pastas e frotas, incluindo a exclusão	Sim	Não
Renomeie pastas e frotas existentes	Sim	Sim
Atribua funções e adicione usuários	Sim	Sim
Associe recursos a pastas e frotas	Sim	Sim
Cadastre-se para receber suporte e envie solicitações pelo Console	Sim	Sim
Utilize serviços de dados que não estejam associados a uma função de acesso explícita	Sim	Sim
Veja a página Audit e as notificações	Sim	Sim

Funções da federação

Tarefa	Administração da federação	Visualizador da federação
Criar e atualizar integrações de serviço de diretório	Sim	Não
Veja as federações e seus detalhes	Sim	Sim

Funções de superadministrador e visualizador

A função **Superadministrador** oferece acesso completo para gerenciar os recursos do NetApp Console, o storage e os serviços de dados. Essa função é adequada para quem supervisiona a administração e a governança. Em contrapartida, a função **Supervisualizador** oferece acesso somente leitura, ideal para auditores ou partes interessadas que precisam de visibilidade sem fazer alterações.

As organizações devem usar o acesso de **Super admin** com parcimônia para minimizar os riscos de segurança e estar em conformidade com o princípio do menor privilégio. A maioria das organizações deve atribuir funções com permissões específicas, concedendo apenas as permissões necessárias para reduzir riscos e melhorar a auditabilidade.

Exemplo de super roles

A ABC Corporation possui uma pequena equipe de cinco pessoas que utiliza o NetApp Console para serviços de dados e gerenciamento de storage. Em vez de distribuir várias funções, eles atribuem a função de **Super admin** a dois membros seniores da equipe, que cuidam de todas as tarefas administrativas, incluindo gerenciamento de usuários e configuração de recursos. Os três membros restantes da equipe recebem a função de **Super viewer**, o que lhes permite monitorar a integridade do storage e o status do serviço de dados sem a possibilidade de modificar as configurações.

Papel	Papéis herdados
Superadministrador	• Administrador da organização • Administrador de pasta ou de fleet • Superadministrador de backup e recuperação • Administrador de storage
Super visualizador	• Visualizador de organização • Visualizador de backup • Visualizador de storage

Função de acesso de analista de suporte operacional na implantação local do NetApp Console

Na implantação local do NetApp Console, você pode atribuir a função de analista de suporte operacional aos usuários para fornecer acesso a alertas e monitoramento.

Analista de suporte operacional

Tarefa	Pode realizar
Veja os sistemas de armazenamento	Sim
Veja a página Audit e as notificações	Sim
Visualizar, baixar e configurar alertas	Sim

Funções de acesso ao storage para NetApp Console implantação local

Você pode atribuir as seguintes funções aos usuários para conceder a eles acesso aos recursos de gerenciamento de storage no NetApp Console em implantação local. Você pode atribuir aos usuários uma função administrativa para gerenciar storage ou uma função de visualizador para monitoramento.

Os administradores podem atribuir funções de armazenamento aos usuários para os seguintes recursos de storage e funcionalidades:

Recursos de storage:

- Clusters ONTAP locais

Serviços e funcionalidades do NetApp Console:

- Funções de integridade de storage

Exemplo de funções de armazenamento no NetApp Console em implantação local

A XYZ Corporation, uma empresa multinacional, possui uma grande equipe de engenheiros de storage e administradores de storage. Eles permitem que essa equipe gerencie os ativos de storage de suas regiões, enquanto limitam o acesso a tarefas essenciais de implantação local do Console, como gerenciamento de usuários e gerenciamento de licenças.

Em uma equipe de 12 pessoas, dois usuários recebem a função de **Storage viewer**, que permite a eles monitorar os recursos de storage associados às frotas de implantação local do Console às quais estão atribuídos. Os nove restantes recebem a função de **Storage admin**, que inclui a capacidade de gerenciar atualizações de software, acessar o ONTAP System Manager por meio da implantação local do Console, assim como descobrir recursos de storage (adicionar sistemas). Uma pessoa da equipe recebe a função de **System health specialist**, para que possa gerenciar a integridade dos recursos de storage em sua região, mas não pode modificar ou excluir nenhum sistema. Essa pessoa também pode realizar atualizações de software nos recursos de storage das frotas às quais está atribuída.

A organização possui dois usuários adicionais com a função de **Organization admin**, que podem gerenciar todos os aspectos da implantação local do Console, incluindo o gerenciamento de usuários e o gerenciamento de licenças, bem como vários usuários com a função de **Folder or fleet admin**, que podem executar tarefas de administração da implantação local do Console para as pastas e frotas às quais estão atribuídos.

A tabela a seguir mostra as ações que cada função de storage executa.

Recurso e ação	Administrador de storage	Especialista em integridade do sistema	Visualizador de storage
Gerenciamento de storage:			
Descobrir novos recursos (adicionar sistemas)	Sim	Sim	Não
Veja os sistemas adicionados	Sim	Sim	Não
Excluir sistemas do NetApp Console	Sim	Não	Não
Modificar sistemas	Sim	Não	Não
Acesso do System Manager			
Pode inserir credenciais	Sim	Sim	Não

Funções do NetApp Backup and Recovery na implantação local do NetApp Console

Na implantação local do NetApp Console, você pode atribuir as seguintes funções aos usuários para conceder a eles acesso ao NetApp Backup and Recovery dentro do Console. As funções de Backup and Recovery oferecem a você flexibilidade para atribuir aos usuários uma função específica para as tarefas que eles precisam realizar em sua organização. A forma como você atribui as funções depende das suas próprias práticas de negócios e de gerenciamento de storage.

O serviço utiliza as seguintes funções específicas para o NetApp Backup and Recovery.

- **Superadministrador de backup e recuperação**: Executar quaisquer ações em NetApp Backup and Recovery.
- **Administrador de backup do Backup and Recovery**: Execute backups para snapshots locais, replique para storage secundário e faça backup para storage de objetos em ações no NetApp Backup and Recovery.
- **Administrador de restauração de backup e recuperação**: restaure cargas de trabalho usando o NetApp Backup and Recovery.
- **Backup and recovery clone admin**: clone aplicativos e dados usando o NetApp Backup and Recovery.
- **Visualizador de backup e recuperação**: Exibe informações no NetApp Backup and Recovery, mas não permite executar nenhuma ação.

Para obter detalhes sobre todos os papéis de acesso ao NetApp Console, consulte "A documentação de configuração e administração do NetApp Console".

Funções usadas para ações comuns

A tabela a seguir indica as ações que cada função de NetApp Backup and Recovery pode executar para todas as cargas de trabalho.

Recurso e ação	Superadministrador de backup e recuperação	Backup e recuperação administrador de backup	Administrador de backup e recuperação de restauração	Administrador de clones de backup e recuperação	Visualizador de backup e recuperação
Adicionar, editar ou excluir hosts	Sim	Não	Não	Não	Não
Instale plugins	Sim	Não	Não	Não	Não
Adicionar credenciais (host, instância, vCenter)	Sim	Não	Não	Não	Não
Visualizar o painel de controle e todas as abas	Sim	Sim	Sim	Sim	Sim
Inicie o teste gratuito	Sim	Não	Não	Não	Não

Recurso e ação	Superadministrador de backup e recuperação	Backup e recuperação administrador de backup	Administrador de backup e recuperação de restauração	Administrador de clones de backup e recuperação	Visualizador de backup e recuperação
Iniciar a descoberta de cargas de trabalho	Não	Sim	Sim	Sim	Não
Ver informações da licença	Sim	Sim	Sim	Sim	Sim
Ativar licença	Sim	Não	Não	Não	Não
Ver hosts	Sim	Sim	Sim	Sim	Sim
Horários:					
Ativar horários	Sim	Sim	Sim	Sim	Não
Suspender horários	Sim	Sim	Sim	Sim	Não
Políticas e proteção:					
Veja os planos de proteção	Sim	Sim	Sim	Sim	Sim
Criar, modificar ou excluir planos de proteção	Sim	Sim	Não	Não	Não
Restaurar cargas de trabalho	Sim	Não	Sim	Não	Não
Criar, dividir ou excluir clones	Sim	Não	Não	Sim	Não
Criar, modificar ou excluir política	Sim	Sim	Não	Não	Não
Relatórios:					
Ver relatórios	Sim	Sim	Sim	Sim	Sim
Criar relatórios	Sim	Sim	Sim	Sim	Não
Excluir relatórios	Sim	Não	Não	Não	Não
Importar do SnapCenter e gerenciar o host:					
Visualizar dados importados do SnapCenter	Sim	Sim	Sim	Sim	Sim

Recurso e ação	Superadministrador de backup e recuperação	Backup e recuperação administrador de backup	Administrador de backup e recuperação de restauração	Administrador de clones de backup e recuperação	Visualizador de backup e recuperação
Importar dados do SnapCenter	Sim	Sim	Não	Não	Não
Gerenciar (migrar) host	Sim	Sim	Não	Não	Não
Configurar configurações:					
Configurar diretório de logs	Sim	Sim	Sim	Não	Não
Associar ou remover credenciais de instância	Sim	Sim	Sim	Não	Não
Buckets:					
Ver buckets	Sim	Sim	Sim	Sim	Sim
Criar, editar ou excluir bucket	Sim	Sim	Não	Não	Não

Funções usadas para ações específicas da carga de trabalho

A tabela a seguir indica as ações que cada função de NetApp Backup and Recovery pode executar para cargas de trabalho específicas.

Cargas de trabalho do Kubernetes

Esta tabela indica as ações que cada função de NetApp Backup and Recovery pode executar para ações específicas de cargas de trabalho do Kubernetes.

Recurso e ação	Superadministrador de backup e recuperação	Backup e recuperação administrador de backup	Administrador de backup e recuperação de restauração	Visualizador de backup e recuperação
Visualize clusters, namespaces, classes de armazenamento e recursos da API	Sim	Sim	Sim	Sim
Adicionar novos clusters Kubernetes	Sim	Sim	Não	Não
Atualizar configurações do cluster	Sim	Não	Não	Não
Remover clusters do gerenciamento	Sim	Não	Não	Não

Recurso e ação	Superadministrador de backup e recuperação	Backup e recuperação administrador de backup	Administrador de backup e recuperação de restauração	Visualizador de backup e recuperação
Ver aplicativos	Sim	Sim	Sim	Sim
Criar e definir novos aplicativos	Sim	Sim	Não	Não
Atualize as configurações do aplicativo	Sim	Sim	Não	Não
Remover aplicativos do gerenciamento	Sim	Sim	Não	Não
Visualize os recursos protegidos e o status do backup	Sim	Sim	Sim	Sim
Crie backups e proteja aplicativos com políticas	Sim	Sim	Não	Não
Desproteger aplicativos e excluir backups	Sim	Sim	Não	Não
Visualizar pontos de recuperação e resultados do visualizador de recursos	Sim	Sim	Sim	Sim
Restaurar aplicativos a partir de pontos de recuperação	Sim	Não	Sim	Não
Visualizar políticas de backup do Kubernetes	Sim	Sim	Sim	Sim
Criar políticas de backup do Kubernetes	Sim	Sim	Sim	Não
Atualize as políticas de backup	Sim	Sim	Sim	Não
Excluir políticas de backup	Sim	Sim	Sim	Não
Visualizar hooks de execução e fontes de hooks	Sim	Sim	Sim	Sim
Crie ganchos de execução e fontes de gancho	Sim	Sim	Sim	Não
Atualize os ganchos de execução e as fontes de ganchos	Sim	Sim	Sim	Não

Recurso e ação	Superadministrador de backup e recuperação	Backup e recuperação administrador de backup	Administrador de backup e recuperação de restauração	Visualizador de backup e recuperação
Excluir hooks de execução e fontes de hooks	Sim	Sim	Sim	Não
Visualizar modelos de hook de execução	Sim	Sim	Sim	Sim
Criar modelos de hook de execução	Sim	Sim	Sim	Não
Atualizar modelos de hook de execução	Sim	Sim	Sim	Não
Excluir modelos de hook de execução	Sim	Sim	Sim	Não
Visualize o resumo da carga de trabalho e os painéis de análise	Sim	Sim	Sim	Sim
Visualize os buckets do StorageGRID e os destinos de storage	Sim	Sim	Sim	Sim

Configurar as integrações e os serviços do NetApp Console

Integre a implantação local do NetApp Console com o Active Directory

Integre a implantação local do NetApp Console com o Active Directory para login e pesquisa de usuários baseados em diretório. Use seu serviço de diretório para autenticar usuários e, em seguida, atribua acesso a esses usuários na implantação local do NetApp Console.

Funções de acesso necessárias

Superadministrador ou administrador da organização. "Saiba mais sobre funções de acesso".

Ao integrar com o Active Directory, a implantação local do Console autentica os usuários por meio do seu diretório existente. Depois de adicionar um usuário ao diretório, atribua funções de acesso ao Console para controlar o que esse usuário pode acessar.

A integração com o Active Directory também ajuda você a atender aos requisitos de conformidade, aplicando seus controles, trilhas de auditoria e políticas existentes ao acesso de implantação local do Console.

- A integração com o Active Directory não cria grupos federados, não sincroniza atribuições de diretório-grupo e não concede acesso automaticamente. Os administradores ainda adicionam usuários do diretório à organização e atribuem funções na implantação local do Console.
- Apenas uma integração com o Active Directory é suportada por vez. Depois que uma integração é configurada, o botão **Adicionar integração** fica desabilitado. Para alternar para um diretório diferente, desabilite ou exclua a integração existente primeiro.
- Os usuários do diretório não configuram nem utilizam autenticação multifator (MFA). A implantação local do console oferece suporte à MFA somente para usuários locais. "Aprenda a gerenciar as configurações de segurança dos membros".

Antes de começar

Antes de integrar com o Active Directory, confirme se você possui:

- Um domínio do Active Directory e credenciais que podem consultar o diretório
- O endereço do servidor LDAP e o nome diferenciado (DN) base para a árvore de diretórios
- Acesso à rede a partir da implantação local do Console para o seu servidor LDAP na porta 389 (LDAP) ou 636 (LDAPS)
- Certificados SSL/TLS, caso você planeje usar LDAPS

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Serviços de diretório** para abrir a página Federações.
3. Selecione **Adicionar integração**.
4. Insira os detalhes de conexão do seu servidor Active Directory:
   - Um nome descritivo para a integração.
   - O **host LDAP**: nome do host ou endereço IP do seu servidor LDAP. Para vários servidores, insira o primário.
   - A porta: 389 para LDAP ou 636 para LDAPS.
   - O **tempo limite de conexão** em milissegundos. O padrão é 1000 ms.
5. Selecione **Usar SSL/TLS** para usar LDAPS. Confirme se o seu servidor LDAP é compatível com LDAPS e se o NetApp Console pode acessar os certificados necessários.
6. Teste a conexão. Se falhar, verifique o host LDAP, a porta, a conectividade de rede e os certificados SSL/TLS.
7. Após o teste ser bem-sucedido, insira o diretório e os detalhes do usuário:
   - **Associação DN base**: Insira o nome diferenciado de associação para a conta LDAP/AD que este aplicativo usará para se conectar ao diretório e insira a credencial (senha) para essa conta. O NetApp Console usa esses detalhes para se associar ao servidor LDAP e validar a conexão.
   - **DN do usuário**: uma conta de usuário com permissão para consultar o diretório. Por exemplo, `CN=ldap-reader,OU=Service Accounts,DC=example,DC=com`.
8. Selecione **Adicionar** para salvar a integração.

Depois que você terminar

Após salvar a integração, adicione usuários do diretório à sua organização e atribua funções. Você deve

configurar e habilitar pelo menos uma integração com o Active Directory antes de poder adicionar usuários do diretório. "Aprenda como adicionar usuários ao diretório e atribuir funções".

Desativar ou ativar a integração com o Active Directory

Desative uma integração para suspender temporariamente a autenticação baseada em diretório sem excluir a configuração. Ao desativar um serviço de diretório, os usuários do diretório não poderão fazer login por meio do diretório.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Serviços de diretório** para abrir a página Federações.
3. Na lista de integrações, localize a integração e selecione o menu de ações para essa linha.
4. Selecione **Desativar** para suspender a integração ou **Ativar** para restaurá-la.

Excluir uma integração com o Active Directory

Exclua uma integração para remover permanentemente a configuração do serviço de diretório. Antes de excluir, revise quaisquer avisos sobre usuários do diretório vinculados à integração, pois o acesso deles será afetado.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Serviços de diretório** para abrir a página Federações.
3. Na lista de integrações, localize a integração e selecione o menu de ações para essa linha.
4. Selecione **Excluir** e confirme a exclusão.

Conecte seu LLM e habilite o assistente do NetApp Console na implantação local do NetApp Console

Conecte seu modelo de linguagem amplo (LLM) à implantação local do NetApp Console para habilitar o assistente do Console e o gerenciamento de storage assistido por IA.

> Esta documentação sobre como conectar um LLM ao assistente do Console para habilitar recursos de IA é fornecida como uma prévia da tecnologia. Com esta oferta de prévia, NetApp reserva-se o direito de modificar os detalhes, o conteúdo e o cronograma da oferta antes da Disponibilidade Geral.

Funções de acesso necessárias

Superadministrador ou administrador da organização. "Saiba mais sobre funções de acesso".

Após a configuração, os usuários abrem o assistente do Console no painel de controle e escolhem um modo de acesso:

- No modo **somente leitura**, o assistente responde a perguntas e fornece orientações sem fazer alterações.
- No modo **Leitura/Gravação**, o assistente pode operar na infraestrutura de storage. Ele exibe detalhes para revisão e confirmação antes de cada alteração. Para operações assíncronas, como a criação de volumes, ele cria uma tarefa que os usuários podem verificar no assistente.

Para conectar seu LLM, selecione um caminho de provedor, insira os detalhes do endpoint e a chave da API e, em seguida, selecione um modelo em **Administração > Ferramentas de IA**. As ações do assistente

permanecem dentro das suas políticas de storage e dos controles de acesso baseado em funções.

Reúna tudo o que você precisa antes de conectar um LLM

Antes de conectar seu LLM, reúna o seguinte:

- Sua decisão quanto ao tipo de provedor: OpenAI ou compatível com OpenAI. "Conheça as opções de provedores."
- Uma chave de API válida para o caminho do provedor que você selecionar.
- A URL do endpoint para o caminho do seu provedor.
- A URL do seu proxy ou gateway, caso sua organização exija uma.
- Seu nome de usuário ou ID de single sign-on (SSO) para a conta do provedor de LLM, se necessário.
- Acesso à rede a partir da implantação local do NetApp Console para o endpoint selecionado.
- Classes de armazenamento e controles de acesso baseados em funções para as ações do assistente que você planeja permitir.

Para obter detalhes sobre os modelos compatíveis, consulte "Saiba mais sobre os provedores e modelos de LLM compatíveis na implantação local do NetApp Console".

Conectar um LLM ao NetApp Console em uma implantação local

Insira as configurações do provedor, a chave da API e o modelo para conectar seu LLM à implantação local do Console.

Passos

1. Faça login na implantação local do NetApp Console.
2. Selecione **Administração > Ferramentas de IA**.
3. Selecione o menu e, em seguida, selecione **Editar**.
4. Em **Tipo de provedor**, selecione um tipo de provedor.

   "Saiba mais sobre a integração do LLM na implantação local do NetApp Console".

5. Caso seja solicitado o endpoint do provedor, insira a URL do endpoint para o caminho do provedor que você selecionou.
6. Insira a URL e as credenciais do proxy ou gateway.
7. No campo **Nome de usuário**, insira seu nome de usuário ou ID de SSO se o caminho do seu provedor exigir isso.
8. No campo **Chave de API**, cole a chave de API do seu caminho de provedor selecionado.
9. Selecione um modelo da lista.
10. Revise a configuração e selecione **Salvar**.

    Se a operação de salvar ou testar falhar, verifique o tipo de provedor, o URL do endpoint, a chave da API e o modelo selecionado e tente novamente.

"Solucione problemas na integração do seu LLM".

Verifique se a integração do LLM funciona

Após salvar a configuração, verifique a disponibilidade e o comportamento do assistente.

Passos

1. Confirme se o botão **Assistente do Console** aparece no painel de implantação local do NetApp Console.
2. Abra o assistente no modo **Somente leitura** e execute uma consulta básica.
3. Abra o assistente no modo **Leitura/gravação** e confirme que as ações que alteram o storage exigem confirmação do usuário antes da execução.
4. Verifique se os usuários que precisam executar fluxos de trabalho têm os controles de acesso baseado em funções necessários.

Após concluir a validação, os usuários podem abrir o assistente do Console no painel e descrever tarefas em linguagem simples. Para exemplos de uso e fluxos de trabalho do usuário final, consulte "Use o assistente do NetApp Console".

Proteja as credenciais e monitore o uso do LLM

- Use uma chave de API dedicada para a integração de implantação local do Console sempre que possível.
- Gire as chaves de API de acordo com a política da sua organização.
- Restrinja quem pode editar as configurações do AI Tools apenas às funções de administrador necessárias.
- Monitore o uso da API do lado do provedor e alertas para rastrear atividades anormais ou picos de custo.

Solucione problemas de integração do LLM na implantação local do NetApp Console

Utilize este fluxo de triagem rápida para diagnosticar e resolver problemas comuns de integração do LLM na implantação local do NetApp Console.

> Esta documentação sobre como conectar um LLM ao assistente do Console para habilitar recursos de IA é fornecida como uma prévia da tecnologia. Com esta oferta de prévia, NetApp reserva-se o direito de modificar os detalhes, o conteúdo e o cronograma da oferta antes da Disponibilidade Geral.

Se você ainda não concluiu a configuração, consulte "Conecte seu LLM e ative o assistente do NetApp Console".

Solucione rapidamente problemas de integração do LLM

1. Valide a configuração das Ferramentas de IA em **Administração > Ferramentas de IA**.

   Confirme o tipo de provedor, URL do endpoint, chave da API, modelo selecionado e acesso à rede de saída.

2. Valide a disponibilidade do assistente no painel de controle.

   Confirme se o botão **Assistente do Console** aparece para os usuários e organizações esperados.

3. Valide o comportamento em tempo de execução.

   Execute uma solicitação simples de leitura e confirme a acessibilidade do endpoint do provedor, a disponibilidade do modelo e a integridade do serviço do provedor.

Solução de problemas por sintoma

Sintoma	Causa provável	O que verificar	Próxima ação
Salvar ou testar falha em Ferramentas de IA	Incompatibilidade de configuração ou conectividade	Tipo de provedor, URL do endpoint, formato da chave da API, modelo selecionado e acesso de saída	Corrija o valor que não passou na validação e salve novamente
O botão **Console assistant** está faltando.	Status de integração inadequado, incompatibilidade organizacional ou incompatibilidade de RBAC	Salvamento bem-sucedido das ferramentas de IA, status de integração, organização atual e função de acesso esperada	Atualize a sessão e verifique com uma conta de administrador conhecida e válida
O assistente abre, mas a solicitação falha	Problema com o provedor ou caminho de runtime	Acessibilidade do endpoint, disponibilidade do modelo nesse endpoint, limites do provedor e status temporário do provedor	Tente novamente após corrigir problemas de incompatibilidade de endpoint/modelo ou de limite do lado do provedor
A resposta do assistente está lenta ou inconsistente	Tamanho do prompt, desempenho do endpoint ou instabilidade da rede/proxy	Teste rápido, integridade do serviço do provedor e estabilidade da rede/proxy	Use um prompt mais curto, tente outro modelo compatível e estabilize o roteamento de rede ou proxy

Responder à exposição ou uso indevido de credenciais de LLM

Se você suspeitar de exposição ou uso não autorizado da chave de API:

1. Revogue a chave de API existente no sistema do seu provedor.
2. Crie uma nova chave de API.
3. Atualize a chave em **Administração > Ferramentas de IA**.
4. Verifique se a reconexão foi bem-sucedida com um teste de assistente somente leitura.

Configure os canais de entrega de notificações na implantação local do NetApp Console

Na implantação local do NetApp Console, você pode configurar vários canais para notificações de alerta, incluindo e-mail e webhooks.

Funções de acesso necessárias

Superadministrador ou administrador da organização. "Saiba mais sobre funções de acesso".

Por padrão, a implantação local do Console exibe notificações por meio de seu sistema de notificações incorporado. Configurar canais de entrega adicionais permite que você receba notificações da maneira que melhor se adapte ao seu fluxo de trabalho.

Você pode enviar todas as notificações pelos mesmos canais ou usar canais diferentes para diferentes tipos de notificação. Por exemplo, você pode enviar alertas urgentes de storage por e-mail enquanto direciona outros alertas para uma ferramenta de monitoramento de terceiro por meio de um webhook.

Após configurar os canais de entrega de notificações, você pode configurar as regras de notificação e atribuí-las a diferentes canais "Aprenda como configurar regras de notificação".

Configurar um servidor de e-mail

Ao configurar um servidor de e-mail, a implantação local do Console envia notificações, alertas e convites de usuários por meio dele. A implantação local do Console é compatível com servidores de e-mail SMTP, que podem ser seu servidor de e-mail corporativo existente ou um serviço de e-mail de terceiro.

Passos

1. Selecione **Administração > Console**.
2. Selecione **Configuração** para abrir a página de configurações do sistema.
3. Na seção **Servidor de e-mail**, selecione **Configurar**.
4. Insira os detalhes de conexão do seu servidor de e-mail:
   - Adicione um nome de remetente e um endereço de e-mail do remetente.
   - O **host SMTP**: nome do host ou endereço IP do seu servidor SMTP. Para vários servidores, insira o principal.
   - Selecione o protocolo de conexão na lista suspensa **Segurança da conexão**. A porta já está configurada para você e é somente leitura: 25 para SMTP com STARTTLS, ou 465 para SMTPS.

     SMTPS (porta 465) estabelece uma conexão criptografada imediatamente e é recomendado para ambientes sensíveis à segurança. STARTTLS (porta 25) faz upgrade a partir de uma conexão não criptografada e pode voltar à transmissão não criptografada se a negociação de criptografia falhar.
5. Selecione **E-mail de teste** para enviar um e-mail de teste para um destinatário que você especificar.
6. Após o teste ser bem-sucedido, selecione **Salvar** para salvar a configuração.

   Se o teste falhar, verifique novamente as configurações inseridas e certifique-se de que a implantação local do Console tenha acesso à rede ao servidor de e-mail.

Atualizar a configuração de um servidor de e-mail

Você pode atualizar a configuração de um servidor de e-mail existente se desejar usar um servidor de e-mail diferente.

Passos

1. Selecione **Administração > Console**.
2. Selecione **Configuração** para abrir a página de configurações do sistema.
3. Na seção **Servidor de e-mail**, selecione **Configurar**.
4. Selecione **Limpar campos** para limpar a configuração existente.
5. Insira os novos detalhes de conexão para o seu servidor de e-mail.
6. Selecione **E-mail de teste** para enviar um e-mail de teste para um destinatário que você especificar.
7. Após o teste ser bem-sucedido, selecione **Salvar** para salvar a nova configuração.

   Se o teste falhar, verifique novamente as configurações inseridas e certifique-se de que a implantação local do Console tenha acesso à rede ao servidor de e-mail.

Remover uma configuração de servidor de e-mail

Você pode remover a configuração do servidor de e-mail se não quiser mais que a implantação local do NetApp Console envie e-mails.

Passos

1. Selecione **Administração > Console**.
2. Selecione **Configuração** para abrir a página de configuração do sistema.
3. Na seção **Servidor de e-mail**, selecione **Configurar**.
4. Selecione **Limpar campos** para limpar a configuração existente.
5. Selecione **Salvar** para salvar a configuração limpa, o que remove a configuração do servidor de e-mail da implantação local do Console.

Configurar um webhook

Configure webhooks para enviar notificações da implantação local do Console para outras ferramentas ou serviços. Você pode configurar vários webhooks, cada um apontando para um endpoint diferente. Por exemplo, um para um SIEM e outro para um serviço de paginação de plantão.

Após criar um webhook, os usuários com a função de administrador de armazenamento podem atribuí-lo a regras de alerta específicas. Por exemplo, eles podem enviar alertas críticos por e-mail enquanto enviam todos os alertas para uma ferramenta de monitoramento de terceiro por meio de um webhook.

> A implantação local do Console não impõe controle de acesso aos endpoints do webhook. Qualquer usuário ou sistema que consiga acessar a URL do endpoint recebe os dados de alerta. Certifique-se de que o acesso ao aplicativo receptor seja restrito a usuários autorizados por meio dos controles de acesso do próprio aplicativo.

Antes de começar

Confirme se a implantação local do Console consegue alcançar o aplicativo receptor pela rede e colete o URL do endpoint, o método HTTP e quaisquer detalhes de autenticação ou certificado exigidos por esse aplicativo.

Passos

1. Selecione **Administração > Console**.
2. Selecione **Configuração** para abrir a página de configurações do sistema.
3. Na seção **Integração de Webhook**, selecione **Configurar**.
4. Insira os detalhes necessários para o webhook:
   - Um nome descritivo para o webhook.
   - A URL do endpoint fornecida pelo aplicativo receptor.
   - Método HTTP
   - Opcional: um certificado autoassinado em formato PEM.
   - Quaisquer cabeçalhos ou segredos necessários (credenciais de autenticação).
   - O formato a ser usado ao enviar o webhook. JSON e OTEL (OpenTelemetry) são suportados.

     Use JSON para webhooks de uso geral e endpoints REST personalizados. Use OTEL para plataformas de observabilidade que consomem sinais OpenTelemetry nativamente, como o Grafana ou outros coletores compatíveis com OpenTelemetry.

5. Selecione **Test webhook** para testar a conexão do webhook e garantir que a implantação local do Console possa enviar mensagens com sucesso para o aplicativo receptor.
6. Após o teste ser bem-sucedido, selecione **Salvar** para criar o webhook.

   Após salvar o webhook, ele fica disponível para os usuários selecionarem onde os webhooks são suportados, como nas opções de entrega de alertas. "Aprenda como criar regras de alerta e atribuir webhooks para entrega de alertas."

Use o NetApp Console

Faça login na implantação local do NetApp Console

Você pode acessar a NetApp Console implantação local depois que o administrador da sua organização convidar você para sua conta de usuário da organização na implantação local do Console. Para fazer login, você usa o endereço de e-mail associado ao seu login.

Se você fizer login, mas não visualizar nenhum recurso, entre em contato com o administrador da sua organização. "Entre em contato com o administrador da sua organização".

Passos

1. Abra um navegador da web e acesse o endereço IP onde a implantação local do NetApp Console está instalada.
2. Na página de **login**, insira o endereço de e-mail que está associado ao seu login.
3. Dependendo do método de autenticação associado ao seu login, você será solicitado a inserir suas credenciais.

   - Uma conta da NetApp Console usando seu endereço de e-mail e uma senha

   - Se a autenticação multifator (MFA) estiver ativada: após inserir sua senha, você será solicitado a inserir um código TOTP (do seu aplicativo autenticador) ou usar um código de recuperação.
   - Se você estiver fazendo login com códigos de recuperação, use-os na ordem exibida na interface do usuário durante a solicitação do código de recuperação.

   +

   - Uma conta do Active Directory usando seu endereço de e-mail e senha

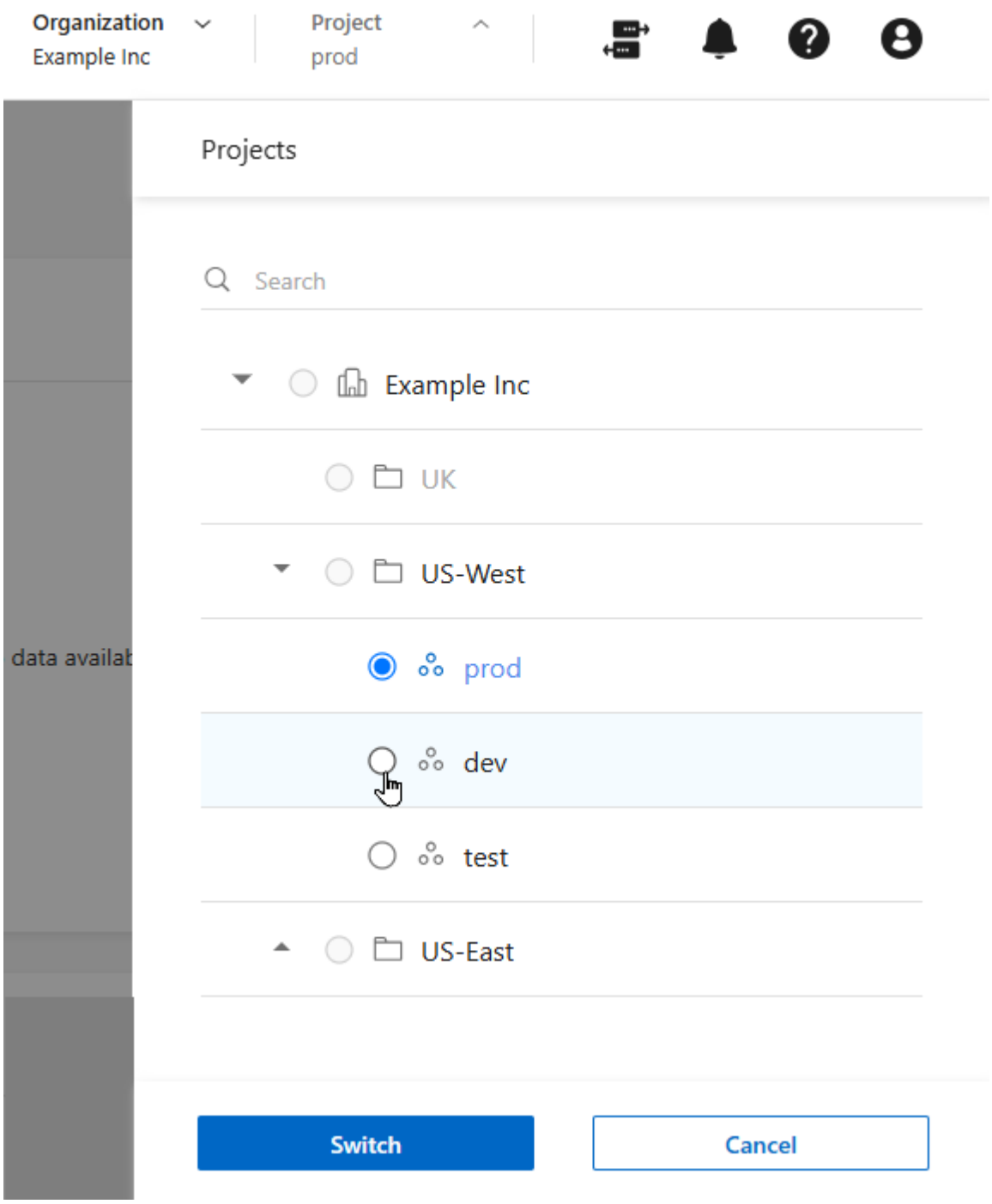
Alternar entre frotas na implantação local do NetApp Console

Na implantação local do NetApp Console, se você tiver acesso a várias frotas, poderá alternar entre elas a qualquer momento.

Você não pode alternar para outra frota enquanto estiver visualizando qualquer uma das páginas de **Identidade e acesso**.

Passos

1. No cabeçalho superior da implantação local do Console, selecione **Scope**.
2. Navegue pelas frotas da sua organização, selecione a frota que você deseja e, em seguida, selecione **Switch**.



Gerencie as configurações de usuário da sua implantação local do NetApp Console

Na implantação local do NetApp Console, você pode modificar seu perfil de implantação local do Console, incluindo alterar sua senha, ativar a autenticação multifator (MFA) e ver quem é o administrador do seu Console.

Altere seu nome de exibição

Você pode alterar o nome de exibição da sua implantação local do NetApp Console, que identifica você para outros usuários. Você não pode alterar seu nome de usuário ou endereço de e-mail.

Passos

1. Selecione o ícone de perfil no canto superior direito da implantação local do NetApp Console para visualizar o painel de configurações do usuário.
2. Selecione o ícone **Editar** ao lado do seu nome.
3. Insira seu novo nome de exibição no campo **Nome**.

Configurar autenticação multifator

Configure a autenticação multifator (MFA) para melhorar a segurança, exigindo um segundo método de verificação ao fazer login na implantação local do NetAppConsole.

Usuários que acessam a conta pelo NetApp Support Site não podem ativar a MFA. Se isso se aplica a você, você não verá a opção para ativar a MFA nas configurações do seu perfil.

Não habilite MFA se sua conta de usuário for usada para acesso à API. A autenticação multifator impede o acesso à API quando habilitada para uma conta de usuário. Use contas de serviço para todo o acesso à API.

Não é possível configurar MFA para sua conta por meio da implantação local do Console se sua conta usar o Active Directory ou outro serviço de diretório integrado para autenticação.

Antes de começar

- Você já deve ter baixado um aplicativo de autenticação, como o Google Authenticator ou o Microsoft Authenticator, para o seu dispositivo.
- Você precisará da sua senha para configurar a autenticação multifator (MFA).

Se você não tiver acesso ao seu aplicativo de autenticação ou perder seu código de recuperação, entre em contato com o administrador do seu Console para obter ajuda.

Passos

1. Selecione o ícone de perfil no canto superior direito do NetApp Console para visualizar o painel de configurações do usuário.
2. Selecione **Configurar** ao lado do cabeçalho **autenticação multifator**.
3. Siga as instruções para configurar a autenticação multifator (MFA) para sua conta.
4. Ao concluir, você será solicitado a salvar seus códigos de recuperação. Escolha copiar os códigos ou baixar um arquivo de texto contendo os códigos. Guarde esses códigos em um local seguro. Você precisará dos códigos de recuperação caso perca o acesso ao seu aplicativo de autenticação.

   Se você precisar iniciar sessão com um código de recuperação, use-os na ordem exibida na interface do usuário durante a solicitação do código de recuperação.

   Após configurar a MFA, a implantação local do Console solicitará que você insira um código único do seu aplicativo de autenticação sempre que fizer login.

Regenerar seu código de recuperação MFA

Você só pode usar um código de recuperação uma vez. Se você perder o seu, crie um novo.

Passos

1. Selecione o ícone de perfil no canto superior direito da implantação local do NetApp Console para visualizar o painel de configurações do usuário.
2. Selecione ••• ao lado do cabeçalho **Autenticação Multifator**.
3. Selecione **Regenerar código de recuperação**.
4. Copie os códigos de recuperação gerados e guarde-os em um local seguro.

Exclua sua configuração de MFA

Ao excluir a autenticação multifator (MFA), você remove a segunda etapa de verificação para seu próximo login. Para usar a MFA novamente, você precisa configurá-la novamente nas suas configurações de usuário.

Caso não consiga acessar seu aplicativo de autenticação ou código de recuperação, você precisará entrar em contato com o administrador da sua organização para redefinir sua configuração de MFA.

Passos

1. Selecione o ícone de perfil no canto superior direito da implantação local do NetApp Console para visualizar o painel de configurações do usuário.
2. Selecione ••• ao lado do cabeçalho **Autenticação Multifator**.
3. Selecione **Delete**.

Entre em contato com o administrador da sua organização

Se precisar entrar em contato com o administrador da sua organização, você pode enviar um e-mail diretamente do NetApp Console. O administrador gerencia as contas de usuário e as permissões dentro da sua organização.

Você precisa ter um aplicativo de e-mail padrão configurado no seu navegador para usar o recurso **Contatar administradores**.

Passos

1. Selecione o ícone de perfil no canto superior direito da implantação local do NetApp Console para visualizar o painel de configurações do usuário.
2. Selecione **Contatar administradores** para enviar um e-mail ao administrador da sua organização.
3. Selecione o aplicativo de e-mail que você deseja usar.
4. Finalize o e-mail e selecione **Enviar**.

Configurar modo escuro (tema escuro)

Você pode configurar a implantação local do Console para ser exibida no modo escuro.

Passos

1. Selecione o ícone de perfil no canto superior direito da implantação local do NetApp Console para visualizar o painel de configurações do usuário.

2. Mova o controle deslizante **Tema escuro** para ativá-lo.

Use o assistente do NetApp Console na implantação local do NetApp Console

Use o assistente do NetApp Console na implantação local do NetApp Console para gerenciar o storage e obter respostas em linguagem natural. Descreva o que você precisa em linguagem simples, e a implantação local do NetApp Console executa as ações dentro das suas políticas de storage e do acesso baseado em funções.

> Esta documentação sobre como conectar um LLM ao assistente do Console para habilitar recursos de IA é fornecida como uma prévia da tecnologia. Com esta oferta de prévia, NetApp reserva-se o direito de modificar os detalhes, o conteúdo e o cronograma da oferta antes da Disponibilidade Geral.

As ações do assistente são limitadas pelo acesso baseado em funções atribuído a você. "Saiba mais sobre funções de acesso".

Veja o que você pode fazer com o assistente do NetApp Console

O assistente do Console é uma interface de linguagem natural para o NetApp Console em implantação local. Faça uma pergunta ou descreva uma tarefa, e ele retorna uma resposta ou uma ação proposta. O assistente oferece estas capacidades:

- **Provisionar armazenamento** Descreva uma carga de trabalho em linguagem simples. O assistente recomenda uma classe de armazenamento e um local adequado e, em seguida, cria o volume ou LUN depois que você confirma os detalhes. Por exemplo, peça para criar um volume CIFS com uma capacidade específica. O assistente identifica o cluster e a máquina virtual de storage (SVM), preenche os parâmetros necessários e provisiona o armazenamento.
- **Pesquise e obtenha orientação** Faça perguntas sobre seu ambiente de storage, encontre recursos de implantação local do Console e obtenha respostas contextuais da documentação da NetApp e do estado atual da frota.
- **Investigar alertas** Peça ao assistente para investigar um alerta ativo. Ele analisa o problema e sugere uma solução ou, com sua confirmação, executa uma ação corretiva.

O assistente envia solicitações apenas para o endpoint LLM configurado pelo seu administrador na implantação local do Console. Ele solicita confirmação antes de executar ações que alteram o storage, e todas as ações respeitam os controles de acesso baseado em funções atribuídos à sua conta.

Confirme que você pode usar o assistente do NetApp Console

- Um administrador da organização ou superadministrador deve habilitar o assistente do Console conectando um large language model (LLM) à implantação local do Console. Se você não vir o botão **Assistente do Console** no painel, peça ao seu administrador para habilitá-lo. Para mais informações, consulte "Conecte seu LLM e ative o assistente do NetApp Console".
- Certifique-se de que você tenha os controles de acesso baseado em funções necessários para as ações que deseja que o assistente execute.

Faça uma pergunta ao assistente do Console ou solicite uma ação

Abra o assistente do Console, escolha um modo de acesso e insira um prompt que descreva sua solicitação.

Passos

1. No painel de implantação local do NetApp Console, selecione o botão **Console assistant**.
2. Selecione um modo de acesso:
   - Selecione **Somente leitura** para fazer perguntas e obter orientações sem fazer alterações.
   - Selecione **Leitura/gravação** para permitir que o assistente atue na sua infraestrutura de storage.
3. Digite um prompt que descreva sua pergunta ou tarefa e, em seguida, selecione **Enviar**.

   Por exemplo: `Create a 10GiB volume for home directories named home, and share it with Everyone set to FULL_CONTROL.`
4. Analise a resposta do assistente:
   - Para uma pergunta, o assistente retorna uma resposta na qual você pode agir.
   - Para uma ação, o assistente exibe a ação sugerida, solicita detalhes ausentes, como o nível de permissão, e então pede confirmação antes de prosseguir.
5. Confirme a ação. Para operações assíncronas, como a criação de volumes, o assistente cria uma tarefa para concluir a solicitação.
6. Para verificar o status de uma solicitação, pergunte ao assistente. Por exemplo, digite `Let me know when the job completes`, e o assistente retorna o status atual.

Gerencie o armazenamento no NetApp Console

Saiba mais sobre gerenciamento de frotas na implantação local do NetApp Console

O gerenciamento de frota no NetApp Console em implantação local é a prática de organizar sistemas de storage em grupos lógicos para que você possa aplicar políticas consistentes, controlar o acesso e monitorar a integridade em clusters relacionados. Em vez de gerenciar cada cluster de forma independente, o gerenciamento de frota permite que você trate sua frota como um pool comum de recursos para apoiar seus objetivos de storage.

À medida que seu ambiente de storage cresce, gerenciar clusters individuais torna-se impraticável. O gerenciamento de frota resolve esse problema, oferecendo uma maneira estruturada de agrupar sistemas relacionados, delegar responsabilidades e garantir que todos os clusters operem sob os mesmos padrões.

Por que o gerenciamento de fleet é importante

O gerenciamento de frotas aborda três desafios principais:

- **Simplificação por meio da abstração** - O gerenciamento de frota abstrai a complexidade do gerenciamento de infraestrutura de storage. Em vez de lidar com a configuração cluster por cluster, você gerencia seu ambiente de storage como um todo unificado, reduzindo a sobrecarga operacional e a fadiga de tomada de decisões.
- **Consistência e escalabilidade** - Sem uma organização clara, diferentes equipes tomam decisões diferentes para cargas de trabalho semelhantes, o que leva a configurações fragmentadas. O gerenciamento de frotas permite que você aplique padrões em dezenas de sistemas ao mesmo tempo, garantindo que novas cargas de trabalho partam da mesma base em todas as equipes e frotas.
- **Governança e controle** - À medida que as equipes crescem, você precisa de limites claros para quem

pode gerenciar o quê. O gerenciamento de frotas fornece esses limites por meio de estrutura organizacional e controle de acesso, garantindo que as decisões de storage permaneçam governadas e auditáveis.

Como as frotas organizam seus recursos

A hierarquia de recursos da sua organização consiste em pastas e frotas:

Para uma visão geral detalhada da hierarquia e do modelo de acesso, consulte "Saiba mais sobre pastas e frotas na implantação local do NetApp Console".

- **Organização** - o nível mais alto que representa sua empresa.
- **Pastas** - Ajudam você a organizar frotas relacionadas. Por exemplo, você pode criar uma pasta para cada região ou unidade de negócios, depois criar frotas dentro de cada pasta. As pastas podem conter outras pastas ou frotas. Quando você atribui uma função no nível da pasta, os membros herdam essa função para todas as frotas dentro da pasta.
- **Frotas** - Agrupe os sistemas de storage que você gerencia. Você associa sistemas de storage a frotas e atribui membros às frotas para conceder acesso a eles.

As pastas são uma ferramenta organizacional e não são visíveis para membros que não possuem permissões do IAM, como as funções de administrador da organização, administrador de pastas ou administrador de frota. Os membros acessam frotas, não pastas.

Padrões comuns de organização de frotas

A forma como você organiza suas frotas depende do seu modelo operacional:

- **Por ambiente** - Crie frotas separadas para cargas de trabalho de produção, desenvolvimento e teste. Isso mantém o storage de produção sob políticas mais rigorosas, ao mesmo tempo que permite maior flexibilidade em ambientes de menor criticidade.
- **Por unidade de negócio** - Agrupe clusters que atendem a um departamento específico, como finanças, engenharia ou RH, em uma frota dedicada. Você pode então atribuir responsabilidades de gerenciamento de storage a membros da equipe dentro dessa unidade de negócio, sem expor outras frotas a eles.
- **Por localização ou data center** - Quando os clusters estão distribuídos em vários locais, a organização por localização permite monitorar a integridade em nível de site, aplicar políticas específicas da região e acompanhar o consumo de capacidade por site.
- **Por camada de aplicativos** - Agrupe clusters que hospedam uma classe específica de carga de trabalho, como bancos de dados, compartilhamentos de arquivos ou máquinas virtuais, para que você possa aplicar padrões consistentes ajustados a esse tipo de carga de trabalho em toda a frota.

Utilize pastas para adicionar mais um nível de organização. Por exemplo, crie uma pasta para cada região e depois crie frotas baseadas em ambiente dentro de cada pasta regional.

Como o gerenciamento de fleet possibilita o controle de acesso

Frotas e pastas servem como limites para o acesso do usuário e a responsabilidade administrativa:

- **Acesso em nível de pasta** - Ao atribuir uma função em nível de pasta, o membro herda essa função para todas as frotas e recursos dentro da pasta. Isso permite delegar responsabilidades administrativas sem conceder acesso a toda a organização.
- **Acesso em nível de frota** - Ao atribuir uma função em nível de frota, o membro terá acesso apenas aos

sistemas de storage dentro dessa frota. Isso permite delegar o gerenciamento de storage a membros da equipe ou proprietários de aplicativos sem expor partes não relacionadas da sua infraestrutura.

A implantação local do NetApp Console fornece monitoramento de integridade e desempenho em nível de frota, permitindo que você veja o status de todos os clusters em uma frota a partir de uma única visualização, identifique problemas precocemente e aja antes que eles afetem as cargas de trabalho.

Como o gerenciamento de storage funciona

O gerenciamento de storage é a prática de definir padrões de storage, aplicá-los de forma consistente e operar as cargas de trabalho para que permaneçam alinhadas ao longo do tempo. Na implantação local do NetApp Console, esses padrões são expressos como políticas de classe de storage e classes de storage, com escopo definido para frotas e aplicados por meio de fluxos de trabalho de provisionamento regidos por RBAC e registro de auditoria.

O deployment local do Console conecta quatro conceitos em um único fluxo de trabalho:

- **Frotas** definem o escopo em que você gerencia o storage. Uma frota agrupa sistemas para que você possa controlar o acesso, aplicar padrões de forma consistente e gerenciar recursos como uma unidade.
- **As políticas de classe de armazenamento** definem padrões como blocos de construção reutilizáveis (desempenho, capacidade, segurança, proteção de dados).
- **Classes de armazenamento** expressam a intenção da carga de trabalho. Uma classe de armazenamento é um modelo nomeado montado a partir de uma ou mais políticas.
- **Fluxos de trabalho de provisionamento** criam armazenamento dentro de limites definidos. Diferentes fluxos de trabalho tomam decisões de configuração de maneiras distintas, mas todos podem impor classes de armazenamento e permanecer regidos por RBAC e registro de auditoria.

Abordagens de provisionamento

A implantação local do NetApp Console oferece suporte a três abordagens de provisionamento, todas regidas por RBAC, registro de auditoria e padrões de classe de armazenamento:

- **Provisionamento manual** - Você seleciona o sistema de destino e especifica os detalhes de configuração diretamente. Use esta opção quando você precisar de controle explícito sobre a seleção e configuração do sistema.
- **Provisionamento automatizado** - Você fornece as informações da carga de trabalho e, opcionalmente, seleciona uma classe de armazenamento. A implantação local no Console recomenda o posicionamento mais adequado e aplica configurações baseadas em classe para reduzir decisões manuais.
- **Provisionamento assistido por IA (agente)** - você descreve o que precisa em linguagem natural. A implantação local no NetApp Console propõe um plano limitado por RBAC e classes de armazenamento, e só faz o provisionamento depois que você revisa e aprova.

Para onde ir a seguir

- Para entender os padrões de storage, consulte "Saiba mais sobre classes e políticas de armazenamento na implantação local do NetApp Console".
- Para criar e gerenciar frotas, consulte "Gerencie pastas e frotas".
- "Provisionar storage manualmente"
- "Provisionar storage automaticamente"
- "Provisione storage com assistência de IA"

Padronizar o comportamento de storage

Saiba mais sobre classes e políticas de armazenamento na implantação local do NetApp Console

Uma classe de armazenamento é um modelo reutilizável que define como o armazenamento deve se comportar. Ao provisionar armazenamento usando uma classe de armazenamento, a implantação local do NetApp Console aplica automaticamente os padrões codificados nessa classe, sem exigir que os administradores tomem decisões de configuração individuais para cada carga de trabalho.

As classes de armazenamento são construídas a partir de políticas de classe de armazenamento, que definem dimensões individuais do comportamento do armazenamento. Juntas, elas permitem que você capture os padrões de armazenamento da sua organização uma única vez e os aplique de forma consistente em toda a sua frota.

O que são as políticas de classe de armazenamento

Uma política de classe de armazenamento define uma dimensão do comportamento do armazenamento. As políticas são blocos de construção reutilizáveis que você combina para criar classes de armazenamento.

Os tipos de políticas mais comuns incluem:

- **Políticas de desempenho** - Defina metas de latência, IOPS ou requisitos de taxa de transferência.
- **Políticas de capacidade** - Defina o modo de provisionamento, alertas de limite ou limites de crescimento.
- **Políticas de segurança** - Defina os requisitos de criptografia, conformidade ou controle de acesso.
- **Políticas de proteção de dados** - Defina cronogramas de snapshots, destinos de replicação ou períodos de retenção.

Você define as políticas de forma independente e, em seguida, as combina ao criar uma classe de storage. Isso permite reutilizar a mesma política de desempenho em várias classes ou atualizar uma política de capacidade em um único local e aplicar essa alteração a todas as classes que a utilizam.

O que são classes de armazenamento

Uma classe de armazenamento é um modelo nomeado, composto por uma ou mais políticas. Ela representa os padrões de storage da sua organização para um tipo específico de carga de trabalho.

Por exemplo, você pode criar uma classe de storage **Production Database** que combine alto desempenho, alta disponibilidade e políticas rigorosas de proteção de dados, ou uma classe de storage **Development File Share** que combine desempenho moderado, capacidade flexível e políticas básicas de proteção de dados.

Os administradores de armazenamento definem classes de armazenamento para codificar requisitos empresariais. Todas as atividades de provisionamento, sejam elas manuais, por meio de fluxos de trabalho guiados ou automatizadas, utilizam a biblioteca de classes aprovadas por esses administradores.

Como as classes de armazenamento impõem padrões

Ao provisionar storage, você seleciona uma classe de storage em vez de configurar definições individuais. A implantação local do NetApp Console usa as políticas dessa classe para identificar quais clusters em sua frota têm a capacidade e o desempenho necessários para suportar a carga de trabalho, recomendar a melhor opção de posicionamento e aplicar automaticamente as configurações baseadas na classe durante o provisionamento.

Após o provisionamento, a implantação local do Console avalia continuamente cada carga de trabalho em relação aos padrões de sua classe de storage.

Desvio e conformidade da storage class

Quando uma carga de trabalho deixa de corresponder à sua intenção de classe de armazenamento, a implementação local do Console a sinaliza para investigação e correção.

Os problemas se dividem em duas categorias:

- **Desvio de configuração**: As configurações de storage regidas pela política de classe de storage deixam de corresponder à configuração pretendida. Isso pode ocorrer quando as alterações são feitas diretamente no cluster ONTAP ou fora dos fluxos de trabalho de provisionamento padrão.
- **Não conformidade de desempenho**: o comportamento de tempo de execução da carga de trabalho não atende mais à intenção de desempenho da classe de armazenamento (por exemplo, pressão sustentada próxima a um limite de QoS ou latência de cauda elevada).

Uma visualização de análise explica o que mudou e por quê. Ações de remediação guiadas (por exemplo, **Corrigir**) podem estar disponíveis para ajudar você a restaurar a conformidade. Algumas remediações podem ser aplicadas no local, enquanto outras podem exigir alinhar a carga de trabalho a uma classe de storage diferente para restaurar o comportamento pretendido.

Onde investigar

Normalmente, você pode investigar desvios e não conformidades a partir de um destes locais (a disponibilidade depende da sua implementação e permissões):

- **Classes de armazenamento:** Deriva / Conformidade
- **Alertas:** analisar

Para obter instruções passo a passo, consulte Corrigir a deriva da storage class.

Fluxo de trabalho de ponta a ponta

Os passos a seguir descrevem o processo de utilização de classes de storage para padronizar e governar o storage em seu ambiente:

1. **Criar políticas de classe de armazenamento** - As políticas definem as dimensões individuais do comportamento do storage (metas de desempenho, configurações de capacidade, requisitos de segurança, cronogramas de proteção de dados). Crie políticas antes de criar uma classe de armazenamento.
2. **Criar uma classe de armazenamento** - Monte uma classe de armazenamento combinando uma política de cada categoria aplicável. Você pode usar uma classe de armazenamento predefinida ou criar uma personalizada de acordo com os padrões da sua organização.
3. **Associe a classe de armazenamento a uma frota** - Depois de criar uma classe de armazenamento, associe-a à frota onde ela será usada para provisionamento e monitoramento de conformidade.
4. **Provisionar storage usando a classe de storage** - Ao provisionar um volume ou LUN, selecione uma classe de storage em vez de configurar definições individuais. A implementação local do NetApp Console usa a classe para recomendar o posicionamento de cluster mais adequado e, em seguida, provisiona com as configurações definidas na classe.
5. **Monitore cargas de trabalho para detecção de desvios** - A implantação local do NetApp Console avalia continuamente cada carga de trabalho em relação aos padrões codificados em sua classe de storage. Se ocorrer desvio de configuração ou não conformidade de desempenho, o sistema sinaliza o problema e

pode gerar um alerta.

6. **Corrigir desvios para restaurar a conformidade** - Quando desvios ou não conformidades de desempenho são detectados, você pode seguir etapas guiadas para corrigir o problema manualmente, deixar que a implantação local do Console resolva automaticamente as condições comuns de desvio ou desassociar uma carga de trabalho de sua classe de armazenamento caso precise alterar suas configurações.

Como as classes de armazenamento funcionam com frotas

As classes de armazenamento são associadas a frotas. Quando você associa uma classe de armazenamento a uma frota, essa classe fica disponível para todo o provisionamento dentro da frota. Isso garante que todas as cargas de trabalho provisionadas na frota sigam os mesmos padrões, tornando as frotas a principal maneira de impor storage consistente em clusters relacionados.

Para obter detalhes sobre como organizar frotas, consulte "Saiba mais sobre gerenciamento de frotas na implantação local do NetApp Console".

Para onde ir a seguir

- Para entender a organização da frota, consulte "Saiba mais sobre gerenciamento de frotas na implantação local do NetApp Console".
- Para criar políticas e classes de armazenamento, consulte "Gerenciar classes de storage e políticas".
- "Provisionar storage manualmente"
- "Provisionar storage automaticamente"
- "Provisione storage com assistência de IA"
- Para analisar e remediar a deriva, consulte "Corrigir a deriva da storage class"

Entendendo as políticas de classe de armazenamento na implantação local do NetApp Console

As políticas de classe de armazenamento são os blocos de construção que você usa para criar uma classe de armazenamento. Cada política controla um aspecto específico do comportamento do armazenamento. Ao combinar políticas em uma classe de armazenamento, você cria um modelo reutilizável que o NetApp Console implantação local aplica automaticamente no momento do provisionamento e monitora continuamente durante todo o ciclo de vida de uma carga de trabalho.

Políticas como elementos fundamentais

Uma classe de armazenamento é composta por uma ou mais políticas, cada uma regendo uma dimensão diferente do comportamento do armazenamento. Os administradores de armazenamento definem políticas para codificar padrões corporativos — expectativas de desempenho, limites de capacidade, regras de posicionamento de dados — e então reúnem essas políticas em modelos de classe de armazenamento. Quando uma carga de trabalho é provisionada usando uma classe de armazenamento, ela herda todas as políticas dessa classe. Esse design separa a responsabilidade de definir padrões do ato de provisionar, permitindo que o armazenamento seja provisionado de forma consistente por fluxos de trabalho automatizados sem a necessidade de decisões de configuração individuais.

Tipos de políticas de classe de armazenamento

NetApp A implantação local do NetApp Console inclui quatro tipos de políticas que você pode usar para construir classes de storage:

Política de desempenho

Uma política de desempenho define as metas esperadas de IOPS/TB, IOPS/TB de pico, IOPS mínimo absoluto e latência esperada para uma carga de trabalho. A implantação local do Console usa esses valores para recomendar clusters com margem suficiente no momento do provisionamento e para detectar desvios de IOPS ou latência após o provisionamento.

Política de capacidade

Uma política de capacidade controla como um volume consome e gerencia espaço. Ela define a reserva de espaço (espessa, fina ou padrão do sistema), o comportamento de crescimento automático, o tiering do FabricPool e se as cargas de trabalho NAS devem ser provisionadas como volumes FlexVol ou FlexGroup.

Política de segurança

Uma política de segurança define os requisitos de criptografia, proteção contra ransomware e FIPS para uma carga de trabalho. Cada atributo pode ser definido com um valor obrigatório ou deixado como "qualquer" para aceitar o padrão do sistema.

Política de proteção de dados

Uma política de proteção de dados define o número de snapshots retidos em cada intervalo para garantir que as cargas de trabalho que utilizam a política recebam um cronograma de backup consistente.

Políticas padrão

A implantação local do Console inclui políticas definidas pelo sistema para todos os quatro tipos de política. Você pode usar essas políticas como estão ao criar uma classe de armazenamento ou copiá-las como ponto de partida para políticas personalizadas, adaptadas aos requisitos da sua organização.

Políticas de desempenho

Nome	Tipo	IOPS/TB esperados	Pico de IOPS/TB	IOPS mínimos absolutos	Latência esperada (ms)	Resumo
Extremo para dados de banco de dados	Sistema definido	12.288	24.576	2.000	1	Use para volumes de dados de transação de banco de dados que exigem IOPS elevado e sustentado e latência inferior a um milissegundo.
Extreme para logs de banco de dados	Sistema definido	22.528	45.056	4.000	1	Use para volumes de log de transação de banco de dados que exigem o maior piso de IOPS para evitar gargalos de gravação.
Extremo para dados compartilhados de banco de dados	Sistema definido	16.384	32.768	2.000	1	Use para volumes de banco de dados compartilhados acessados por vários hosts que exigem alta taxa de transferência e latência consistente.

Nome	Tipo	IOPS/TB esperados	Pico de IOPS/TB	IOPS mínimos absolutos	Latência esperada (ms)	Resumo
Desempenho Extremo	Sistema definido	6.144	12.288	1.000	1	Use para cargas de trabalho de HPC, IA/ML e análise que exigem alto IOPS em rajadas e latência baixa previsível.
Desempenho	Sistema definido	2.048	4.096	500	2	Use para aplicações virtualizadas e empresariais que exigem desempenho confiável sem demandas extremas de IOPS.
Valor	Sistema definido	128	512	75	17	Use para cargas de trabalho com restrições de custo, como diretórios pessoais, compartilhamentos de arquivos e arquivos de arquivamento.

Políticas de capacidade

Nome	Tipo	Reserva de espaço	Modo de crescimento automático	Política de tiering	Tipo de volume (NAS)	Resumo
padrão	Sistema definido	Padrão do sistema	Padrão do sistema	nenhum	Padrão do sistema	Utilize para cargas de trabalho gerais quando o comportamento de capacidade padrão da plataforma for aceitável.
produção	Sistema definido	Padrão do sistema	crescer	nenhum	Padrão do sistema	Utilize para cargas de trabalho de produção que precisam se expandir automaticamente para evitar falhas por falta de espaço.

Políticas de segurança

Nome	Tipo	Criptografia	Proteção contra ransomware	FIPS	Resumo
padrão	Sistema definido	qualquer	qualquer	qualquer	Utilize para cargas de trabalho em que o comportamento de segurança padrão da plataforma seja aceitável.

Nome	Tipo	Criptografia	Proteção contra ransomware	FIPS	Resumo
anti-ransomware	Sistema definido	qualquer	sobre	qualquer	Utilize para cargas de trabalho que contenham dados essenciais aos negócios e que exijam proteção ativa contra ransomware.
produção	Sistema definido	habilitado	qualquer	qualquer	Utilize em cargas de trabalho de produção onde a criptografia é exigida para conformidade.

Políticas de proteção de dados

Nome	Tipo	Instantâneos de hora em hora	Instantâneos diários	Snapshots semanais	Instantâneos mensais	Resumo
padrão	Sistema definido	6	2	2	0	Utilize para cargas de trabalho padrão que exigem pontos de recuperação de curto prazo sem a sobrecarga de retenção de longo prazo.
3 meses por hora	Sistema definido	23	6	4	3	Utilize para cargas de trabalho regulamentadas ou críticas para os negócios que exigem pontos de recuperação intradia granulares e três meses de retenção histórica.

Analise as políticas de classe de armazenamento predefinidas na NetApp Console implantação local

NetApp Console local inclui políticas definidas pelo sistema em todos os quatro tipos de política. Use esta referência para identificar qual política melhor se adapta aos requisitos da sua carga de trabalho ao criar ou personalizar uma classe de armazenamento.

Políticas de desempenho

Desempenho Extremo

Use para cargas de trabalho de HPC, IA/ML e análise que exigem alto IOPS em rajadas e latência baixa previsível.

Extremo para dados de banco de dados

Use para volumes de dados de transação de banco de dados que exigem IOPS elevado e sustentado e latência inferior a um milissegundo.

Extreme para logs de banco de dados

Use para volumes de log de transação de banco de dados que exigem o maior piso de IOPS para evitar gargalos de gravação.

Extremo para dados compartilhados de banco de dados

Use para volumes de banco de dados compartilhados acessados por vários hosts que exigem alta taxa de transferência e latência consistente.

Desempenho

Use para aplicações virtualizadas e empresariais que exigem desempenho confiável sem demandas extremas de IOPS.

Valor

Use para cargas de trabalho com restrições de custo, como diretórios pessoais, compartilhamentos de arquivos e arquivos de arquivamento.

Políticas de capacidade

Capacidade de autogrow

Utilize para cargas de trabalho de produção que precisam se expandir automaticamente para evitar falhas por falta de espaço.

Políticas de segurança

Criptografia em repouso

Utilize em cargas de trabalho de produção onde a criptografia é exigida para conformidade.

Proteção contra ransomware

Utilize para cargas de trabalho que contenham dados essenciais aos negócios e que exijam proteção ativa contra ransomware.

Segurança padrão

Utilize para cargas de trabalho em que o comportamento de segurança padrão da plataforma seja aceitável.

Políticas de proteção de dados

padrão

Utilize para cargas de trabalho padrão que exigem pontos de recuperação de curto prazo sem a sobrecarga de retenção de longo prazo.

3 meses por hora

Utilize para cargas de trabalho regulamentadas ou críticas para os negócios que exigem pontos de recuperação intradia granulares e três meses de retenção histórica.

Recuperação de 30 dias

Utilize para cargas de trabalho padrão que exigem pontos de recuperação de curto prazo sem a sobrecarga de retenção de longo prazo.

Recuperação de 90 dias

Utilize para cargas de trabalho regulamentadas ou críticas para os negócios que exigem pontos de recuperação intradia granulares e três meses de retenção histórica.

Crie classes de armazenamento na implantação local do NetApp Console

Crie uma classe de armazenamento na implantação local do NetApp Console para

padronizar como o storage é provisionado e gerenciado em suas frotas. Uma classe de armazenamento é um modelo reutilizável que agrupa políticas de classe de armazenamento, como metas de desempenho, comportamento de capacidade, requisitos de segurança e cronogramas de proteção de dados, em uma única definição nomeada.

Quando os usuários (ou a automação) provisionam um volume ou LUN usando uma classe de armazenamento, a implantação local do NetApp Console aplica as políticas da classe automaticamente. Após o provisionamento, a implantação local do Console monitora continuamente as cargas de trabalho em relação à classe de armazenamento para detectar desvios e pode orientar ou automatizar a correção para restaurar a conformidade.

Antes de começar

- Descubra pelo menos um cluster ONTAP para que a implantação local do NetApp Console tenha alvos para recomendações de posicionamento.
- Certifique-se de ter a função de administrador da organização (ou uma função que conceda permissões de gerenciamento de classe de storage em seu ambiente).
- Crie (ou identifique) as políticas de classe de armazenamento que você planeja usar — desempenho, capacidade, segurança e proteção de dados — porque as classes de armazenamento são montadas a partir de políticas.

Crie uma storage class

Você precisa ter a função de Organization admin, Folder admin ou fleet admin para adicionar uma classe de armazenamento.

Passos

1. Selecione **Storage > Management**.
2. Selecione **Classes de armazenamento**.
3. Selecione **Add**.
4. Em **Informações básicas**, insira o seguinte:
   - **Nome da classe de armazenamento**: insira um nome exclusivo para a classe de armazenamento.
   - **Descrição**: (Opcional) Insira uma descrição da classe de storage.
   - **Aplicativos recomendados**: (Opcional) Insira uma lista de aplicativos recomendados para a classe de armazenamento.
5. Em **Políticas de armazenamento**, selecione uma ou mais políticas para associar à classe de armazenamento.
6. Selecione **Add**.

Personalize uma classe de armazenamento existente

Você precisa ter a função de administrador da organização, da pasta ou da frota para personalizar uma classe de armazenamento existente.

Passos

1. Selecione **Storage > Management**.
2. Selecione **Classes de armazenamento**.

3. Para a classe de armazenamento que você deseja personalizar, selecione **…** e, em seguida, selecione **Duplicar**.
4. Em **Informações básicas**, atualize o seguinte conforme necessário:
   - **Nome da classe de armazenamento**: insira um nome exclusivo para a classe de armazenamento.
   - **Descrição**: (Opcional) Insira uma descrição da classe de storage.
   - **Aplicativos recomendados**: (Opcional) Insira uma lista de aplicativos recomendados para a classe de armazenamento.
5. Em **Políticas de armazenamento**, selecione uma ou mais políticas para associar à classe de armazenamento.
6. Selecione **Add**.

Editar uma classe de armazenamento definida pelo usuário

Você precisa ter a função de administrador da organização, da pasta ou da frota para editar uma classe de storage definida pelo usuário.

Passos

1. Selecione **Storage > Management**.
2. Selecione **Classes de armazenamento**.
3. Para a storage class que você deseja editar, selecione **…** e depois selecione **Editar**.
4. Em **Informações básicas**, edite o seguinte conforme necessário:
   - **Nome da classe de armazenamento**: insira um nome exclusivo para a classe de armazenamento.
   - **Descrição**: (Opcional) Insira uma descrição da classe de storage.
   - **Aplicativos recomendados**: (Opcional) Insira uma lista de aplicativos recomendados para a classe de armazenamento.
5. Em **Políticas de armazenamento**, selecione uma ou mais políticas para associar à classe de armazenamento.
6. Selecione **Editar**.

Excluir uma classe de armazenamento definida pelo usuário

Você precisa ter a função de Organization admin, Folder admin ou fleet admin para excluir uma classe de armazenamento definida pelo usuário.

Passos

1. Selecione **Storage > Management**.
2. Selecione **Classes de armazenamento**.
3. Para a classe de armazenamento que você deseja excluir, selecione **…** e depois selecione **Excluir**.
4. Selecione **Delete**.

   Observe que esta ação não pode ser desfeita. Se você excluir uma classe de armazenamento que esteja em uso, quaisquer volumes ou LUNs provisionados com essa classe continuarão a operar, mas não estarão mais associados à classe excluída.

Provisionar armazenamento na implantação local do NetApp Console

Provisione volumes e LUNs na implantação local do NetApp Console para disponibilizar recursos de storage para suas cargas de trabalho. Durante o provisionamento, você pode opcionalmente selecionar uma classe de storage para aplicar políticas de storage predefinidas e padrões organizacionais.

Funções de acesso necessárias

Superadministrador, administrador da organização, administrador de pasta ou frota, ou administrador de armazenamento. "Saiba mais sobre funções de acesso".

Provisionar um volume

Passos

1. Selecione **Storage > Management**.
2. Selecione **Fleets**.
3. Selecione a frota na qual você deseja provisionar.
4. Selecione **Add**.
5. No menu, selecione **Volume**.
6. Em **Detalhes do volume**:
   a. Digite o nome do volume.
   b. Insira a capacidade (e escolha as unidades se necessário).
   c. (Opcional) Selecione uma classe de armazenamento para aplicar políticas de classe de armazenamento. Se você não selecionar uma, o volume será provisionado sem políticas de classe de armazenamento.
7. Em **Detalhes do sistema**:
   a. Selecione um sistema dentre os sistemas elegíveis para a frota selecionada.
   b. Selecione uma máquina virtual de armazenamento.
8. Em **Detalhes do host (NAS)**, escolha como os hosts acessam o volume:
   a. Exportação via NFS (as políticas de exportação controlam quais hosts NFS podem acessar o volume)
   b. Compartilhar por SMB/CIFS
9. Selecione **Add**.

Provisione um LUN

Passos

1. Selecione **Storage > Management**.
2. Selecione **Fleets**.
3. Selecione a frota na qual você deseja provisionar.
4. Selecione **Add**.
5. No menu, selecione **LUNs**.
6. Em **Detalhes de armazenamento LUN**:
   a. Insira um nome de prefixo.

b. Insira o número de LUNs a serem criadas com esse prefixo.

c. Insira a capacidade por LUN (e escolha as unidades se necessário).

d. (Opcional) Selecione uma classe de armazenamento para aplicar políticas de classe de armazenamento. Se você não selecionar uma, os LUNs serão provisionados sem políticas de classe de armazenamento.

7. Em **Detalhes do sistema**:

   a. Selecione um sistema (se solicitado).

   b. Selecione uma máquina virtual de armazenamento.

8. Em **Detalhes do host (SAN)**, escolha como os hosts acessam o volume:

   a. Selecione o sistema operacional do host (por exemplo, Windows ou Linux) para definir os valores padrão recomendados para alinhamento de LUN e tamanho de bloco.

   b. Escolha o grupo de mapeamento de hosts para controlar quais iniciadores podem acessar os LUNs.

9. Selecione **Add**.

Monitore a integridade do storage

Monitoramento de storage na implantação local do NetApp Console

NetApp Console local deployment ajuda você a monitorar o storage em toda a sua frota com dashboards, alertas, análises detalhadas e remediação, para que você possa identificar e resolver problemas antes que eles afetem as workloads.

Monitore a saúde de toda a frota com dashboards

Comece pelos painéis para uma visão rápida da integridade e do desempenho do sistema de storage. Use a página inicial para ver métricas rapidamente, abra a tabela de painéis para acessar painéis predefinidos e personalizados e acesse alertas, investigação e correção quando precisar de mais detalhes.

- "Visualize as métricas da página inicial na implantação local do NetApp Console"
- "Mantenha os painéis atualizados na implantação local do NetApp Console"
- "Saiba mais sobre painéis personalizados na implantação local do NetApp Console"

Investigue problemas de desempenho

Use o Workload Analyzer para investigar problemas de desempenho em volumes individuais. Ele correlaciona latência, taxa de transferência, IOPS e alterações de configuração para que você possa identificar as causas principais.

- "Saiba mais sobre o Workload Analyzer de implantação local do NetApp Console"
- "Investigue alta latência em um volume na implantação local do NetApp Console"
- "Investigue a alta demanda de taxa de transferência em um volume na implantação local do NetApp Console"
- "Saiba mais sobre as métricas do Workload Analyzer na implantação local do NetApp Console"

Configure alertas e notificações

Configure políticas de alerta e canais de notificação para que as pessoas certas sejam informadas sobre as condições de storage que exigem atenção. Por exemplo, encaminhe um aviso de capacidade para a equipe de storage e um alerta de proteção para o administrador de backup, que pode agir sobre ele.

"Configure as notificações e as políticas de alertas na implantação local do NetApp Console". "Visualize os alertas de armazenamento na implantação local do NetApp Console".

Corrigir problemas

Quando você detectar um problema, corrija-o diretamente a partir da implantação local do NetApp Console:

- **Correção automatizada** — A implantação local do NetApp Console aplica ações corretivas automaticamente com base em regras predefinidas.
- **Remediação guiada** — Siga recomendações passo a passo para resolver problemas com controle total sobre cada ação.

Monitoramento com dashboards

Visualize as métricas da página inicial na implantação local do NetApp Console

Use o painel da página inicial na implantação local do NetApp Console como seu ponto de partida padrão para monitorar a integridade e o desempenho do storage. Ele fornece métricas de alto nível para integridade da frota, alertas, segurança, uso da capacidade, latência, taxa de transferência e IOPS.

O painel da página inicial é automaticamente configurado para exibir apenas as frotas e os sistemas que você está autorizado a visualizar. Você também pode adicionar um painel personalizado à página inicial para monitoramento específico da sua função.

Use os cartões como um fluxo de trabalho de triagem em camadas. Comece com **Saúde da frota** e **Alertas** para encontrar pontos críticos de risco. Use **Status de saúde do sistema** e **Remediações recomendadas** para identificar os recursos afetados. Use **Uso de capacidade**, **Latência**, **Taxa de transferência** e **IOPS** para investigar as causas principais.

Saúde da frota

O cartão **Saúde da Frota** exibe um resumo de alto nível do status das cinco principais frotas, incluindo contagens de sistemas, capacidade utilizada, conformidade de segurança e alertas críticos. Use este cartão para identificar quais frotas precisam de atenção imediata. Selecione o nome da frota para visualizar um painel somente da frota selecionada.

Remediações recomendadas

O cartão **Remediações recomendadas** lista problemas ativos e ações sugeridas. O cartão prioriza as remediações com base na pressão sobre a capacidade, recursos offline e riscos relacionados à proteção.

Alertas

O cartão **Alertas** resume o volume de alertas no período selecionado e os agrupa por gravidade. Use este cartão para entender a carga atual de incidentes e identificar mudanças recentes em alertas críticos, de aviso ou informativos.

Segurança

O cartão **Segurança** resume as métricas de conformidade e proteção, como a conformidade do sistema e os controles relacionados a ransomware. Use esta visualização para monitorar as tendências de segurança em seus recursos.

Utilização da capacidade

O cartão **Utilização da capacidade** exibe as tendências de utilização projetadas e históricas em frotas ou sistemas selecionados. Use este cartão para identificar padrões de crescimento e planejar capacidade adicional.

Latência

O cartão **Latência** monitora o comportamento do tempo de resposta ao longo do tempo nos sistemas selecionados. Use essa tendência para detectar atrasos de desempenho emergentes e comparar a latência entre os recursos.

Capacidade de processamento

O cartão **Throughput** exibe as taxas de transferência de dados ao longo do tempo para sistemas selecionados. Use este cartão para entender a intensidade da carga de trabalho e monitorar as mudanças na demanda de throughput.

IOPS

O cartão **IOPS** exibe as taxas de operação de entrada/saída ao longo do tempo. Use este cartão para comparar os níveis de atividade entre sistemas e identificar a demanda de E/S contínua ou intermitente.

Cartão do dashboard (exemplo de cartão de métrica)

A área inferior do **Dashboard** pode conter um dashboard personalizado selecionado por você, como a latência média para um escopo de produção selecionado. Use esses cards para monitoramento direcionado por equipe, carga de trabalho ou objetivo.

Estado de saúde do sistema

O cartão **Estado de integridade do sistema** lista os sistemas individuais com seu estado de integridade atual. Use este cartão para identificar rapidamente sistemas com problemas e correlacionar as alterações de estado com alertas e sinais de desempenho.

Informações relacionadas

- "Saiba mais sobre painéis personalizados na implantação local do NetApp Console"
- "Saiba mais sobre cartões de dashboard personalizados e métricas na implantação local do NetApp Console"

Use painéis personalizados

Saiba mais sobre painéis personalizados na implantação local do NetApp Console

Use painéis personalizados na implantação local do NetApp Console para criar visualizações de monitoramento focadas para equipes, frotas, cargas de trabalho e objetivos operacionais específicos. Os painéis personalizados complementam o painel

da página inicial, adicionando visibilidade direcionada ao monitoramento amplo e sempre disponível.

Como os tipos de dashboard funcionam juntos

Painel da página inicial

Painéis de monitoramento prontos para uso para capacidade, alertas, capacidade de desempenho, licenças e status de proteção de dados. As visualizações são pré-configuradas e atualizadas automaticamente. "Visualize as métricas da página inicial na implantação local do NetApp Console".

Painéis personalizados

Visualizações de monitoramento específicas para cada função, criadas a partir de cartões predefinidos, incluindo escopo selecionável, métricas, recursos de destino, e janelas de tempo.

Use ambos em conjunto: * Comece na página inicial para monitoramento diário de referência. * Use painéis personalizados para investigação focada por equipe, frota, carga de trabalho ou questão operacional.

Você pode adicionar um painel personalizado à página inicial por vez.

Entenda os painéis personalizados

Um painel personalizado é uma coleção salva de cartões que você organiza em uma grade. Cada cartão é baseado em um modelo predefinido de cartão com uma métrica e um tipo de gráfico. Ao adicionar um cartão, você configura o escopo, os objetos de destino, a agregação e o período de tempo.

Painéis e cartões personalizados são privados para você. Cada cartão exibe dados apenas dos recursos de storage que você está autorizado a visualizar.

Você pode remover o painel personalizado da sua página inicial e adicionar um diferente conforme as prioridades de monitoramento mudam.

Monitore o que importa

Os modelos de cartão são organizados por tipo de métrica, permitindo que você concentre um painel em uma área operacional específica. Por exemplo, use cartões de capacidade para monitorar um volume que está crescendo mais rápido do que o esperado ou use cartões de alerta para rastrear falhas repetidas em um cluster com alta carga.

Desempenho

Latência, IOPS, taxa de transferência, utilização e capacidade de desempenho em toda a frota, sistemas, SVMs, volumes e LUNs.

Capacidade

Capacidade utilizada, capacidade livre, percentual de capacidade utilizada e capacidade de snapshot em toda a frota, sistemas, SVMs, volumes, LUNs e camadas locais.

Saúde

Estado de saúde, contagem de objetos degradados ou críticos, discos com falha, erros de interface de rede e objetos ativos.

Alertas

Contagem de alertas críticos, alertas por gravidade, alertas por área de impacto, alertas recentes e tendências de alertas ao longo do tempo.

Para um catálogo completo de cartões predefinidos e métricas, consulte "Saiba mais sobre cartões de dashboard personalizados e métricas na implantação local do NetApp Console".

Tipos de recursos

Você pode definir o escopo dos cartões para qualquer nível da hierarquia de armazenamento do ONTAP: frota, cluster, sistema (nó), SVM, volume, LUN e camada local (agregado). Os tipos de recursos disponíveis dependem do modelo de cartão que você selecionar.

Visualizações do painel do plano

Organize painéis personalizados em torno de objetivos de administração de storage, como triagem de desempenho de carga de trabalho, planejamento de capacidade, detecção de riscos e priorização de alertas.

Informações relacionadas

- "Comece a usar dashboards na implantação local do NetApp Console"
- "Visualize as métricas da página inicial na implantação local do NetApp Console"
- "Saiba mais sobre cartões de dashboard personalizados e métricas na implantação local do NetApp Console"

Comece a usar dashboards na implantação local do NetApp Console

Na implantação local do NetApp Console, siga este fluxo de trabalho para monitorar desde visões amplas até visões mais específicas: revise o painel da página inicial, revise os painéis predefinidos, crie painéis personalizados e mantenha os painéis atualizados.

Funções de acesso necessárias

Todas as funções. Os painéis mostram apenas os recursos que você está autorizado a visualizar. Se você não vir um recurso na lista de recursos disponíveis, você não tem permissão para visualizá-lo.

Verifique o estado geral de saúde na página inicial

Utilize o painel de controle da página inicial para analisar a capacidade, alertas, desempenho e o status da proteção de dados em nível organizacional.

- "Visualize as métricas da página inicial na implantação local do NetApp Console"
- "Saiba mais sobre o monitoramento de armazenamento na implantação local do NetApp Console"

Analise outros painéis predefinidos

Abra **Armazenamento > Painéis** para revisar os painéis predefinidos e obter visualizações adicionais específicas para cada função.

- "Gerencie painéis na implantação local do NetApp Console"

Crie painéis personalizados para monitoramento direcionado

Crie painéis personalizados quando precisar de visualizações específicas para recursos, métricas e períodos de tempo selecionados.

- "Crie um painel personalizado"
- "Personalize os cartões do painel de controle na implantação local do NetApp Console"

4 Mantenha os painéis atualizados

Atualize os painéis conforme as prioridades mudam, editando, duplicando ou excluindo painéis personalizados.

- "Gerencie painéis na implantação local do NetApp Console"
- "Saiba mais sobre cartões de dashboard personalizados e métricas na implantação local do NetApp Console"

Informações relacionadas

- "Saiba mais sobre painéis personalizados na implantação local do NetApp Console"
- "Visualize as métricas da página inicial na implantação local do NetApp Console"

Crie painéis para monitorar metas na implantação local do NetApp Console

Crie um painel personalizado na implantação local do NetApp Console, adicione cartões e salve uma visualização de monitoramento para operações diárias.

Se você precisa apenas de monitoramento em nível organizacional pronto para uso, comece com os painéis predefinidos da página inicial. Crie um painel personalizado quando você precisar de uma visualização específica para uma função, segmentação em nível de recurso ou um layout de cartão personalizado.

Diretrizes para o painel de implantação local do NetApp Console

- Somente o usuário que cria o painel pode visualizá-lo. Você não pode compartilhar painéis com outros usuários, mesmo quando os adiciona à página inicial do Console.
- Você só pode visualizar os recursos que você tem permissão para visualizar. Se você não vir um recurso na lista de recursos disponíveis, você não tem permissão para visualizá-lo.
- Antes de começar, identifique os tipos de métricas e recursos que você deseja que o painel monitore. "Saiba mais sobre cartões de dashboard personalizados e métricas na implantação local do NetApp Console"

Crie um painel de controle para seus objetivos de monitoramento

Crie um painel de controle quando você precisar de um local centralizado para monitorar as métricas importantes para sua função, como a saúde da frota, pontos críticos de desempenho e tendências de alertas.

Passos

1. Selecione **Armazenamento > Painéis**.
2. Selecione **Adicionar painel**.

   A implantação local do NetApp Console cria um novo painel com um nome padrão e sem descrição.

3. Selecione **Adicionar cartão**.
4. Selecione o **Tipo de recurso** para o cartão, como frota, sistema ou volume e então escolha os recursos na lista de recursos disponíveis.
5. Selecione **Próximo** para continuar para escolher uma métrica e um tipo de cartão.

6. Selecione uma métrica para exibir. Você pode filtrar as métricas disponíveis por tipo: o **Tipo de Métrica**: **Desempenho**, **Capacidade**, **Saúde** ou **Alertas**, ou pesquisar uma métrica específica pelo nome. As métricas disponíveis dependem do tipo de recurso que você selecionou.

   "Saiba mais sobre as métricas disponíveis."

7. Selecione um cartão para incluir no painel e selecione **Avançar**.

   Você só pode selecionar um cartão por vez. A pré-visualização do cartão mostra dados em tempo real para a métrica e o tipo de recurso selecionados.

8. Dê um nome ao seu cartão. O nome deve ser único no painel de controle.
9. Revise a prévia do cartão, insira um nome e uma descrição para o cartão e selecione **Adicionar**.
10. Repita estas etapas para os cartões adicionais.
11. Selecione o ícone de lápis para editar o nome e a descrição do painel e descrever sua finalidade.
12. Selecione o menu de ações à direita do botão Adicionar cartão e selecione **Salvar dashboard**.

    O painel salvo está disponível em **Armazenamento > Painéis**.

13. Opcionalmente, adicione este painel à sua página inicial selecionando **Adicionar à página inicial** no menu de ações. O painel é adicionado à página inicial. Somente você pode visualizar os painéis personalizados que criar. Ele não é compartilhado com outras pessoas.

Informações relacionadas

- "Visualize as métricas da página inicial na implantação local do NetApp Console"
- "Saiba mais sobre painéis personalizados na implantação local do NetApp Console"
- "Personalize os cartões do painel de controle na implantação local do NetApp Console"
- "Gerencie painéis na implantação local do NetApp Console"

Personalize os cartões na implantação local do NetApp Console

Na implantação local do NetApp Console, personalize os cartões do painel quando você precisar direcionar os operadores para os sinais que mais importam, como risco de SLA, pressão de capacidade ou ruído de alertas recorrentes. Use este tópico para estruturar as visualizações do painel em torno das decisões operacionais que sua equipe precisa tomar.

Antes de começar

- Crie ou abra um painel onde você deseja colocar os cartões.
- Analise os modelos disponíveis e as métricas em "Saiba mais sobre cartões de dashboard personalizados e métricas na implantação local do NetApp Console".

Adicione cartões enquanto aprimora um painel existente

Use esta opção quando você estiver aprimorando um painel existente e precisar adicionar rapidamente cartões que respondam a uma pergunta operacional específica.

Passos

1. Abra o painel ao qual você deseja adicionar um cartão.
2. Selecione **Adicionar cartão**.
3. Selecione o **Tipo de recurso** para o cartão, como frota, sistema ou volume e então escolha os recursos na lista de recursos disponíveis.
4. Selecione **Próximo** para continuar para escolher uma métrica e um tipo de cartão.
5. Selecione uma métrica para exibir. Você pode filtrar as métricas disponíveis por tipo: o **Tipo de Métrica**: **Desempenho**, **Capacidade**, **Saúde** ou **Alertas**, ou pesquisar uma métrica específica pelo nome. As métricas disponíveis dependem do tipo de recurso que você selecionou.

   "Saiba mais sobre as métricas disponíveis."

6. Selecione um cartão para incluir no painel e selecione **Avançar**.

   Você só pode selecionar um cartão por vez. A pré-visualização do cartão mostra dados em tempo real para a métrica e o tipo de recurso selecionados.

7. Dê um nome ao seu cartão. O nome deve ser único no painel de controle.
8. Revise a prévia do cartão, insira um nome e uma descrição para o cartão e selecione **Adicionar**.
9. Repita estas etapas para os cartões adicionais.
10. Salve o dashboard.

Informações relacionadas

- "Visualize as métricas da página inicial na implantação local do NetApp Console"
- "Saiba mais sobre painéis personalizados na implantação local do NetApp Console"
- "Crie um painel personalizado"
- "Gerencie painéis personalizados"
- "Saiba mais sobre cartões de dashboard personalizados e métricas na implantação local do NetApp Console"

Referência de painéis predefinidos e cartões de painel personalizados na implantação local do NetApp Console

Na implantação local do NetApp Console, painéis predefinidos e modelos de cartões de painel personalizados fornecem cobertura de monitoramento para o desempenho, capacidade, integridade e operações de alerta do ONTAP.

Painéis predefinidos

Os seguintes painéis predefinidos estão disponíveis imediatamente.

Nome	Descrição
Volumes	Desempenho do volume, capacidade, QoS, FabricPool, taxa de crescimento e métricas de previsão.
Tempo até o enchimento	Previsões de tempo até a capacidade máxima (time-till-full) do ONTAP para clusters, volumes e agregados.
Segurança	Conformidade com segurança, criptografia, proteção autônoma contra ransomware e visão geral de autenticação.

Nome	Descrição
SVMs	Monitoramento do desempenho, capacidade, volume, LIF, protocolo (CIFS, FCP, iSCSI, NFS, NVMe/FC), QoS e mapa de calor de latência do ONTAP SVM.
Energia	Monitoramento do consumo de energia, temperatura e velocidade da ventoinha do cluster ONTAP para nós, prateleiras e agregados.
Nós	Desempenho do nó ONTAP, CPU, rede e monitoramento do backend.
Rede	Métricas de desempenho de rede, incluindo Ethernet, FibreChannel, NVMe/FC, grupos de agregação de links e rotas.
LUNs	Monitoramento do desempenho, capacidade e eficiência das LUNs do ONTAP.
Saúde	Monitoramento da integridade do cluster ONTAP, incluindo erros, avisos, alertas do EMS, problemas de HA, integridade de nós/discos/shelfs, volumes, licenças e portas de rede.
Agregados	Monitoramento da capacidade agregada do ONTAP, dos índices de eficiência e da taxa de crescimento.

Janelas de tempo e agregação em nível de dashboard

Os intervalos de tempo disponíveis são de 30 minutos, 1 hora, 24 horas, 48 horas, 7 dias e 30 dias. As opções de agregação variam conforme o modelo e incluem visualizações como consolidação de toda a frota ou resultados no estilo "top-N". O intervalo de tempo e a agregação são configurados no nível do painel e se aplicam a todos os cartões do painel.

Modelos de cartões do painel e métricas

Os cartões são os blocos de construção dos painéis personalizados. Cada cartão usa um modelo predefinido com uma métrica e um tipo de gráfico, depois mapeia essa visualização para objetos específicos do ONTAP e objetivos de monitoramento.

Os modelos de cartão são predefinidos e não criados pelo usuário.

Índice de métricas de operações de armazenamento (em resumo)

Os tipos de métricas estão alinhados a resultados comuns de administração de armazenamento, incluindo gargalos de desempenho, pressão de capacidade, risco de integridade e volume de alertas.

Tipo de métrica	Métricas compatíveis	Caso de uso do administrador de armazenamento	Modelos detalhados
Desempenho	Latência média, latência de pico, IOPS, taxa de transferência (MB/s), utilização, capacidade de desempenho	Identifique gargalos, pressão constante e margem de desempenho	Acesse os modelos

Tipo de métrica	Métricas compatíveis	Caso de uso do administrador de armazenamento	Modelos detalhados
Capacidade	Capacidade utilizada, capacidade livre, capacidade utilizada (%), capacidade de snapshot utilizada	Acompanhe o crescimento, identifique áreas com baixa capacidade disponível e monitore o impacto de snapshots	Acesse os modelos
Saúde	Estado de saúde, objetos degradados/críticos, discos com falha, erros de interface de rede, objetos ativos (por latência)	Detectar regressões de saúde e priorizar a triagem operacional	Acesse os modelos
Alertas	Alertas (Críticos), alertas por gravidade, alertas por área de impacto, alertas recentes, tendência de alertas	Monitore os incidentes ativos e a tendência do volume de alertas ao longo do tempo	Acesse os modelos

Hierarquia de objetos ONTAP suportada (tipos de recursos)

Os dados do cartão podem ser representados em vários níveis de objeto do ONTAP, desde a visibilidade em nível de frota até a solução de problemas em nível de objeto.

As configurações de **Tipo de recurso** correspondem a um ou mais dos seguintes níveis de recurso:

- Frota
- Cluster
- Sistema (nó)
- SVM
- Volume
- LUN
- Nível local (agregado)

Os níveis de recursos disponíveis dependem do template e da métrica que você selecionar.

Tipos de gráficos para análise operacional

O tipo de gráfico afeta a rapidez com que você consegue interpretar tendências, comparações, distribuições e valores de ponto no tempo.

Tipo de gráfico	Ideal para
Gráfico de linhas	Tendências em séries temporais, como latência, IOPS, throughput, utilização e tendências de alertas ao longo do tempo.
Gráfico de barras	Comparação e distribuição categórica, como alertas por gravidade ou área de impacto.
Pizza ou doughnut	Distribuição proporcional, como porcentagem da capacidade utilizada.
Tabela	Dados detalhados em várias colunas, como capacidade utilizada, status de integridade e alertas recentes.

Tipo de gráfico	Ideal para
Número único (stat)	Um único valor-chave visível num relance, como contagens de alertas críticos ou discos com falha.

Modelos de desempenho para triagem de carga de trabalho

Os modelos de desempenho se concentram em sinais de latência, taxa de transferência e utilização que indicam a pressão da carga de trabalho.

Modelo	Tipo de gráfico	Descrição
Latência média	Linha	Latência média entre os alvos selecionados durante o período de tempo escolhido.
Latência de pico	Linha	Latência máxima observada nos alvos selecionados durante o período de tempo escolhido.
IOPS	Linha	Soma das operações de E/S por segundo nos alvos selecionados.
Taxa de transferência (MB/s)	Linha	Soma da taxa de transferência de dados entre os alvos selecionados.
Utilização	Linha	Utilização média da CPU ou do disco nos destinos selecionados.
Capacidade de desempenho	Tabela	Análise da margem livre comparando a utilização atual com o ponto ideal.

Modelos de capacidade para crescimento e margem de segurança

Os modelos de capacidade focam no espaço consumido e disponível para apoiar o planejamento do crescimento e a detecção de riscos.

Modelo	Tipo de gráfico	Descrição
Capacidade utilizada	Tabela	Soma da capacidade utilizada nos alvos selecionados.
Capacidade livre	Tabela	Soma da capacidade livre ou disponível nos alvos selecionados.
Capacidade utilizada (%)	Pizza ou doughnut	Proporção média de uso em relação ao total nos alvos selecionados.
Capacidade de Snapshot utilizada	Tabela	Soma do espaço de Snapshot consumido nos destinos selecionados.

Modelos de saúde para detecção de riscos

Os modelos de saúde focam no estado do objeto e em indicadores de falha para apoiar a triagem operacional.

Modelo	Tipo de gráfico	Descrição
Estado de saúde	Tabela	Estado de saúde mais recente para cada objeto alvo selecionado.

Modelo	Tipo de gráfico	Descrição
Objetos degradados/críticos	Número único	Contagem de objetos cujo estado de saúde não é OK.
Discos com falha	Número único	Soma dos discos com falha nos sistemas selecionados.
Erros na interface de rede	Pizza ou doughnut	Soma dos contadores de erros da interface de rede nos destinos selecionados.
Objetos Quentes (por latência)	Tabela	Recursos classificados por latência máxima, em ordem decrescente.

Modelos de alertas para priorização de incidentes

Os modelos de alertas focam no volume de incidentes, gravidade e área de impacto para auxiliar no monitoramento e na priorização.

Modelo	Tipo de gráfico	Descrição
Alertas (Crítico)	Número único	Contagem de alertas de gravidade crítica dentro do período analisado.
Alertas por gravidade	Bar	Alertas agrupados por nível de gravidade.
Alertas por área de impacto	Bar	Alertas agrupados por área de impacto, como capacidade, desempenho ou segurança.
Alertas recentes	Tabela	Alertas mais recentes, ordenados por horário em ordem decrescente.
Tendência de alerta	Linha	Contagem de alertas por intervalo de tempo na janela de tempo escolhida.

Informações relacionadas

- "Visualize as métricas da página inicial na implantação local do NetApp Console"
- "Saiba mais sobre painéis personalizados na implantação local do NetApp Console"
- "Crie um painel personalizado"
- "Personalize os cartões do painel de controle na implantação local do NetApp Console"
- "Gerencie painéis personalizados"

Gerencie painéis personalizados

Gerencie painéis na implantação local do NetApp Console

Gerencie painéis personalizados na implantação local do NetApp Console para manter as visualizações alinhadas às operações. Você pode editar, duplicar e excluir painéis conforme as equipes, frotas e prioridades mudam.

Esta tarefa aplica-se apenas a dashboards personalizados em **Armazenamento > Dashboards**. Os dashboards predefinidos da página inicial não podem ser editados da mesma forma.

Visualizar painéis

Visualize painéis personalizados e predefinidos para encontrar o painel que você deseja abrir, editar, duplicar ou excluir.

Você pode duplicar um painel predefinido para criar uma versão personalizada que você pode editar.

Passos

1. Selecione **Armazenamento > Painéis**.
2. Analise a tabela do dashboard para encontrar o dashboard que você deseja abrir.
3. Selecione o nome do painel para abri-lo e visualizar suas métricas.
4. Se necessário, use as ações disponíveis para editar, duplicar ou excluir painéis personalizados.

Atualize o painel conforme as prioridades mudam

Edite um painel quando suas prioridades operacionais mudarem e você precisar ajustar quais cartões e métricas estão visíveis.

Passos

1. Selecione **Armazenamento > Painéis**.
2. Abra o painel que você deseja editar.
3. Modifique um cartão existente no painel selecionando Editar no menu de ações do cartão.
4. Adicione um novo cartão ao painel selecionando **Adicionar cartão**.

   "Personalize os cartões na implantação local do NetApp Console".

5. Selecione **Salvar alterações** para salvar o painel.
   - Você também pode optar por salvar suas alterações como um novo painel selecionando **Salvar como novo painel** no menu de ações. Essa opção é útil quando você deseja manter o painel original para outras equipes ou frotas enquanto cria uma nova versão para suas necessidades de monitoramento atuais.
   - Você também pode optar por descartar suas alterações selecionando **Descartar alterações** no menu de ações. Essa opção é útil quando você deseja reverter para a última versão salva do painel.

Reutilize um painel personalizado para outro recurso ou frota

Duplique um painel quando quiser reutilizar um layout comprovado para outra equipe, frota ou cenário de monitoramento sem precisar recriá-lo do zero.

Você pode duplicar um painel predefinido para criar uma versão personalizada que você pode editar.

Passos

1. Selecione **Armazenamento > Painéis**.
2. Para o painel que você deseja duplicar, selecione **Duplicar** no menu de ações.

   A implantação local no NetApp Console cria uma cópia que inclui todos os cartões do painel original.

3. Forneça um nome e uma descrição para o painel duplicado.
4. Selecione o painel duplicado que você acabou de criar. Altere as métricas, os recursos e os tipos de cartão para adequá-los ao seu novo cenário de monitoramento.

   "Personalize os cartões na implantação local do NetApp Console".

Remova painéis que você não usa mais

Exclua um painel quando ele não for mais compatível com as operações atuais e você quiser manter sua lista de painéis focada em casos de uso ativos.

Passos

1. Selecione **Armazenamento > Painéis**.
2. Para o painel que você deseja remover, selecione **Excluir**.
3. Confirme a exclusão.

Informações relacionadas

- "Visualize as métricas da página inicial na implantação local do NetApp Console"
- "Comece a usar dashboards na implantação local do NetApp Console"
- "Saiba mais sobre painéis personalizados na implantação local do NetApp Console"
- "Crie um painel personalizado"
- "Personalize os cartões do painel de controle na implantação local do NetApp Console"

Monitore frotas usando o inventário na implantação local do NetApp Console

Na implantação local do NetApp Console, use o inventário para monitorar a integridade da frota e investigar recursos de storage em todo o seu ambiente. O inventário fornece visualizações de capacidade, segurança e desempenho que ajudam você a identificar problemas, entender a utilização de recursos e rastrear sistemas de storage gerenciados.

O Inventário é principalmente um espaço de trabalho informativo e de diagnóstico. A partir do Inventário, você pode revisar sistemas, volumes e outros objetos de storage em suas frotas e executar ações comuns, como provisionar recursos de storage. Para operações avançadas de gerenciamento de storage, a implantação local do NetApp Console redireciona você para o System Manager.

Acessar inventário

Você pode acessar o **Inventário** em diversas áreas da implantação local do NetApp Console, incluindo:

- A página inicial
- Páginas de visão geral da frota
- Cartões de saúde da frota e visualizações de inventário relacionadas

Dependendo de onde você inserir **Inventory**, o escopo exibido pode ser no nível da organização ou no nível da frota.

Visualizações de inventário

O **Inventário** oferece múltiplas visualizações que ajudam você a analisar diferentes aspectos do seu ambiente de storage.

Capacidade
: Visualize a utilização da capacidade e identifique sistemas, volumes e outros objetos de storage que consomem recursos de storage.

Segurança
: Analise as informações relacionadas à segurança e o status de conformidade em todos os recursos de storage.

Desempenho
: Analise métricas relacionadas ao desempenho e identifique recursos que possam exigir investigação adicional.

As informações exibidas variam dependendo da visualização selecionada e do tipo de objeto.

Investigue recursos de storage

Use **Inventário** para:

- Monitorar a saúde da frota
- Analise o uso da capacidade de storage
- Acompanhe sistemas de storage gerenciados
- Identifique volumes e outros objetos que consomem capacidade
- Investigue possíveis problemas de segurança ou desempenho
- Localize os recursos que requerem atenção administrativa

O **Inventário** ajuda você a passar de uma visão de alto nível do seu ambiente para uma investigação mais detalhada de recursos de storage.

Provisionar recursos de storage

O recurso de inventário inclui fluxos de trabalho que permitem provisionar recursos de storage, como volumes e LUNs.

Ao provisionar recursos, você seleciona um sistema de storage gerenciado existente e fornece as configurações necessárias para a carga de trabalho.

Inventário e alertas

Alertas são gerados para objetos de storage e condições específicas dentro do seu ambiente.

Ao selecionar um alerta, a implantação local do Console pode direcionar você ao System Manager para investigação adicional ou ações de gerenciamento. O **Inventário** complementa os alertas, fornecendo uma visibilidade mais ampla do estado geral do seu ambiente de storage e dos recursos gerenciados.

Tarefas de gerenciamento avançado

O **Inventário** ajuda você a identificar recursos que exigem ação, mas algumas operações avançadas de

gerenciamento de storage são realizadas no System Manager.

Exemplos incluem:

- Gerenciamento avançado de carga de trabalho
- Tarefas de realocação e otimização de recursos
- Atividades detalhadas de administração do sistema

Utilize o recurso **Inventário** para identificar e investigar problemas e, em seguida, use o System Manager quando forem necessárias funcionalidades de gerenciamento mais avançadas.

Corrigir alertas

Saiba mais sobre alertas na implantação local do NetApp Console

NetApp Console local gera alertas que identificam problemas de integridade em seus clusters ONTAP locais e para operações de NetApp Backup and Recovery.

A implantação local do Console consolida alertas de clusters ONTAP e operações de Backup and Recovery em uma única visualização. A página de alertas inclui um painel, uma lista de alertas e uma visualização de sistemas, para que você possa revisar alertas em toda a organização ou restringi-los a uma frota ou sistema específico. Cada alerta identifica o sistema afetado, sua gravidade e sua área de impacto.

Utilize alertas na implantação local do Console para:

- Detectar problemas de capacidade, conectividade, proteção de dados, desempenho e segurança.
- Priorize os alertas por gravidade e área de impacto.
- Abra um alerta no System Manager ou no Workload Analyzer e, em seguida, execute uma ação Fix-It guiada ou automatizada quando a página oferecer uma.
- Encaminhe notificações por e-mail para usuários com funções de acesso específicas ou envie dados de alerta para um sistema externo por meio de um webhook.
- Exporte a lista de alertas para um arquivo CSV para análise offline.

Gravidade do alerta e áreas de impacto

Cada alerta inclui uma classificação de gravidade e uma área de impacto:

- **Gravidade** indica a urgência, da mais alta para a mais baixa: Crítica, Grave, Leve, Aviso e Informativa.
- **Área de impacto** identifica o domínio afetado: capacidade, conectividade, proteção de dados, desempenho e segurança.

Fontes e âmbito dos alertas

- **Os alertas do ONTAP** têm origem no ONTAP Event Management System (EMS) nos clusters locais que a implantação local do Console descobriu. "Saiba mais sobre o ONTAP EMS e os alertas disponíveis."
- **Os alertas de NetApp Backup and Recovery** são originados por ações de Backup and Recovery. "Saiba mais sobre os alertas de NetApp Backup and Recovery."
- Suas permissões determinam quais frotas você pode visualizar. Defina o escopo da visualização para toda a organização, uma frota específica ou um sistema individual. A guia **Integridade dos sistemas** mostra o status de cada sistema e a guia **Alertas** mostra a lista de alertas atual para o escopo selecionado.

- A exportação em CSV reflete o escopo atual, o texto da pesquisa e os filtros.

Regras de notificação de alerta

Crie regras de notificação para determinar quais alertas geram notificações e quem as recebe. Uma regra de notificação possui as seguintes características:

- Ele relaciona alertas do serviço (como gerenciamento do ONTAP ou NetApp Backup and Recovery), gravidade, área de impacto e sistema de destino.
- Para o envio de e-mails, ele envia notificações para usuários com as funções de acesso especificadas. Para o envio via webhook, ele envia dados de alerta para o endpoint configurado; o acesso a esses dados é controlado pelo aplicativo receptor, não pela implantação local do Console.
- Aplica-se a sistemas específicos, não a frotas.
- Pode ser silenciado durante uma janela de manutenção planejada para suprimir alertas esperados.

A implantação local do Console inclui uma regra de notificação padrão que é ativada imediatamente após a instalação. A regra padrão monitora todos os serviços e sistemas em busca de alertas de gravidade crítica e envia notificações apenas para a Central de Notificações do Console; o envio por e-mail ou webhook não é configurado até que você o configure. Você pode visualizar e ajustar essa regra, além de criar regras personalizadas para adequá-las ao seu ambiente.

Os alertas de nível informativo são visíveis na página de Alertas, mas não são enviados por notificação a menos que você crie explicitamente uma regra que inclua o nível de gravidade informativo.

Informações relacionadas

- "Monitorar e investigar alertas"
- "Crie e gerencie regras de notificação de alerta"
- "Saiba mais sobre os alertas do ONTAP na implantação local do NetApp Console"

Monitore e investigue alertas na implantação local do NetApp Console

Monitore e investigue alertas na implantação local do NetApp Console para manter seu armazenamento íntegro e minimizar interrupções.

Visualize alertas ativos em toda a sua organização ou em uma frota específica, priorize-os por gravidade e área de impacto e investigue as causas principais para que você possa resolver problemas antes que eles escalem. Quando um alerta inclui uma ação recomendada ou a opção Fix It, você pode passar da investigação diretamente para a remediação.

Função de acesso necessária

Todas as funções, exceto administrador da Federação e visualizador da Federação. Usuários com a função de administrador da Federação ou visualizador da Federação não podem visualizar alertas. "Saiba mais sobre funções de acesso".

Para os alertas do ONTAP, você pode acessar ferramentas como o System Manager e o Workload Analyzer diretamente da página de Alertas para investigar e resolver problemas.

Para relatórios externos, você pode exportar a lista de alertas para um arquivo CSV para análise offline.

Você também pode configurar regras de notificação para receber alertas por e-mail ou webhook. "Saiba como configurar notificações de alerta".

Alertas disponíveis

A implantação local do NetApp Console suporta alertas para o ONTAP e o NetApp Backup and Recovery.

- "Saiba mais sobre os alertas do ONTAP na implantação local do NetApp Console"
- "Saiba mais sobre os alertas de NetApp Backup and Recovery."

Veja o painel de alertas

Use o painel de alertas para obter uma visão geral rápida da atividade de alertas atual para o escopo que você selecionou. O painel resume os alertas ativos por gravidade e área de impacto e inclui um gráfico que mostra a distribuição dos alertas nas últimas 24 horas, para que você possa identificar tendências rapidamente.

Você pode filtrar o painel para se concentrar em alertas críticos ou alertas para uma área de impacto específica.

Passos

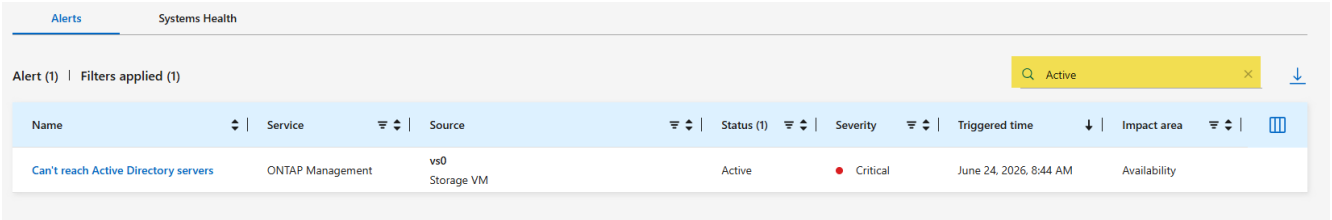
1. Selecione **Health > Alerts > Overview**.
2. No seletor de escopo, escolha uma das seguintes opções:
   - **Todos** (padrão) para ver alertas em todas as frotas às quais você tem acesso
   - Uma frota específica para ver alertas somente para essa frota
3. Filtre o painel de acordo com os alertas que você precisa visualizar, incluindo:
   - Gravidade (Crítica, Atenção ou Informativa)
   - Alertas críticos agrupados por área de impacto
   - Área de impacto (Segurança, Proteção, Disponibilidade, Desempenho, Capacidade ou Configuração)

Ver todos os alertas

Use a guia Alertas para visualizar a lista completa de alertas ativos para o escopo que você selecionou. A lista é atualizada para refletir o escopo atual da organização ou frota, e você pode pesquisar na lista alertas específicos por nome ou descrição.

Passos

1. Selecione **Health > Alerts > Overview**.
2. No seletor de escopo, escolha uma das seguintes opções:
   - **Todos** (padrão) para ver alertas em todas as frotas às quais você tem acesso
   - Uma frota específica para ver alertas somente para essa frota
3. Selecione a aba **Alertas** para visualizar a lista completa de alertas ativos para o escopo selecionado.
4. Opcionalmente, pesquise na lista um alerta específico por nome ou descrição.



Visualizar alertas por sistema

Você pode visualizar alertas para um sistema específico dentro de uma frota ou da sua organização.

Passos

1. Selecione **Health > Alerts > Overview**.
2. No seletor de escopo, escolha uma das seguintes opções:
   - **Todos** (padrão) para ver alertas em todas as frotas às quais você tem acesso
   - Uma frota específica para ver alertas somente para essa frota
3. Selecione a guia **Saúde do sistema** para visualizar um resumo dos alertas associados aos sistemas dentro do escopo que você selecionou.
4. Selecione **Exibir alertas** na linha do respectivo sistema para visualizar a lista completa de alertas ativos associados a esse sistema.

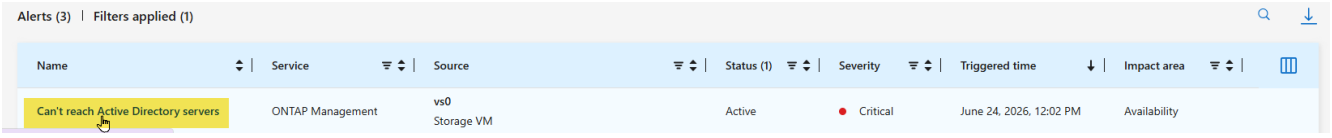
Investigar um alerta

Você pode investigar um alerta para ver o que o desencadeou e quem recebeu a notificação.

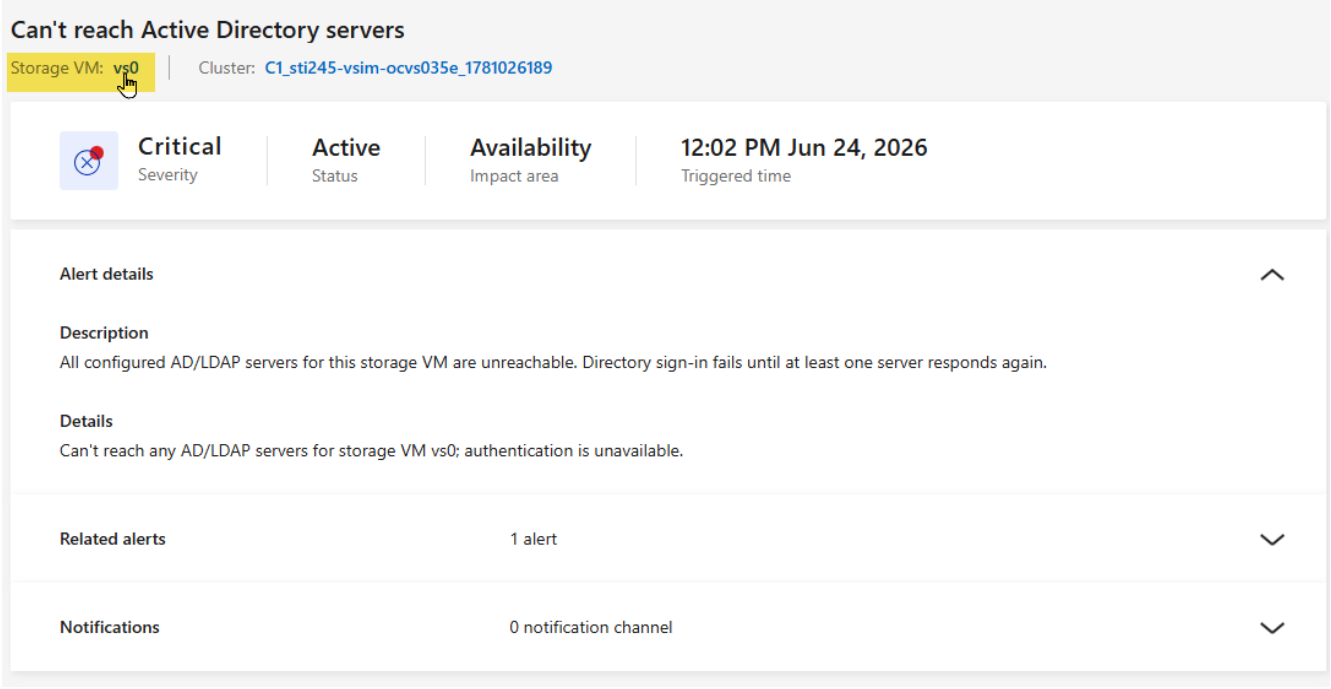
Ao investigar um alerta do ONTAP, você também pode acessar diretamente a interface do System Manager do sistema que gerou o alerta para visualizar detalhes adicionais e tomar as medidas necessárias.

Passos

1. Selecione **Health > Alerts > Overview**.
2. No seletor de escopo, escolha uma das seguintes opções:
   - **Todos** (padrão) para ver alertas em todas as frotas às quais você tem acesso
   - Uma frota específica para ver alertas somente para essa frota
3. Em qualquer uma das abas, selecione o nome do alerta que você deseja investigar para visualizar seus detalhes.



4. Se aplicável, selecione o nome da VM ou do cluster para abrir a interface do System Manager para o sistema que gerou o alerta.



Corrigir um alerta

Quando um alerta incluir uma ação recomendada ou uma opção de Fix It, use-a para passar da investigação para a remediação sem sair dos detalhes do alerta.

Passos

1. Selecione **Health > Alerts > Overview**.
2. No seletor de escopo, escolha uma das seguintes opções:
   - **Todos** (padrão) para ver alertas em todas as frotas às quais você tem acesso
   - Uma frota específica para ver alertas somente para essa frota
3. Selecione o alerta que você deseja corrigir.
4. Analise os detalhes do alerta e selecione a ação recomendada ou a opção **Corrigir** se estiver disponível.
5. Siga os passos guiados para aplicar a correção e, em seguida, retorne aos detalhes do alerta para confirmar o estado do alerta.

Se a ação resolver o problema, o alerta deixará de aparecer como ativo para esse escopo. Se o alerta permanecer ativo, revise os detalhes do alerta novamente e continue a investigação.

Analisar um alerta

Você pode analisar um alerta do ONTAP no Workload Analyzer para entender o que o desencadeou.

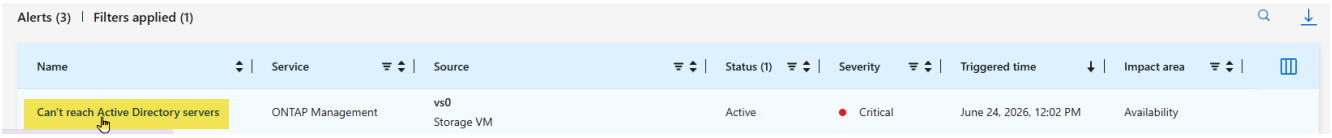
Ao investigar um alerta do ONTAP, você também pode acessar diretamente a interface do System Manager do sistema que gerou o alerta para visualizar detalhes adicionais e tomar as medidas necessárias.

Passos

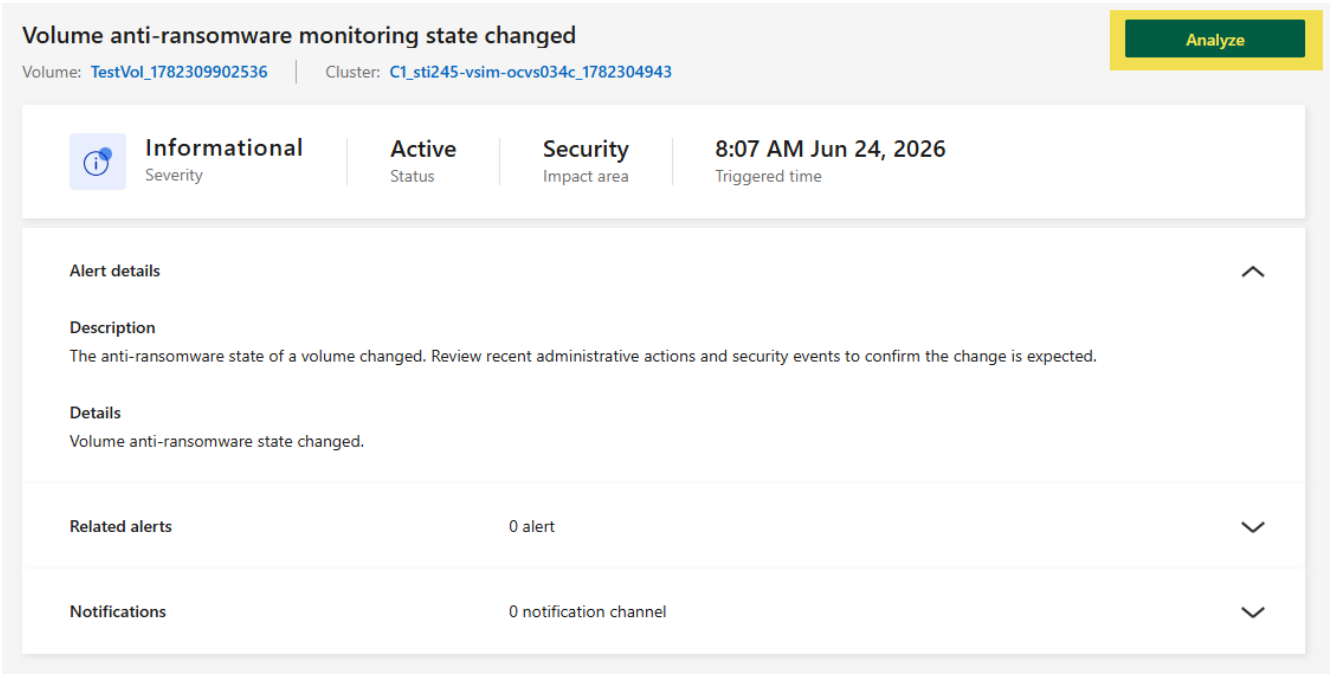
1. Selecione **Health > Alerts > Overview**.
2. No seletor de escopo, escolha uma das seguintes opções:
   - **Todos** (padrão) para ver alertas em todas as frotas às quais você tem acesso

- Uma frota específica para ver alertas somente para essa frota

3. Selecione a guia **Saúde do sistema** para visualizar a lista completa de alertas ativos para o escopo selecionado.
4. Em qualquer uma das abas, selecione o nome do alerta que você deseja investigar para visualizar seus detalhes.



5. Se aplicável, selecione **Analisar** para abrir a interface Workload Analyzer do sistema que gerou o alerta.



6. Insira o intervalo de tempo que abrange o período em que o alerta foi acionado, depois selecione **Analisar** para visualizar os resultados da análise. "Saiba mais sobre o Workload Analyzer."

Exportar alertas para CSV

Exporte a lista de alertas na implantação local do NetApp Console para um arquivo CSV para análise ou geração de relatórios offline. A exportação reflete o escopo atual (organização ou frota), o texto da pesquisa e os filtros.

Passos

1. Selecione **Saúde > Alertas** e, em seguida, selecione a guia **Alertas**.
2. Defina o escopo (organização ou frota) e aplique quaisquer filtros ou texto de pesquisa que você quiser incluir na exportação.
3. Selecione o ícone de download para exportar a lista de alertas para um arquivo CSV.

Configure regras de notificação para alertas na implantação local do NetApp Console

Configure as regras de notificação na implantação local do NetApp Console para

controlar quais alertas geram notificações, quem as recebe e como elas são entregues.

Funções de acesso necessárias

Superadministrador, administrador da organização, administrador de storage, analista de suporte de operações ou qualquer uma das funções administrativas do NetApp Backup and Recovery. "Saiba mais sobre funções de acesso".

Use regras de notificação para encaminhar os alertas certos para as pessoas certas pelos canais adequados ao seu ambiente, enquanto reduz o ruído de alertas que não são relevantes para você. As regras de notificação complementam a página de Alertas: você investiga ou resolve o alerta no fluxo de trabalho de Alertas e, em seguida, usa regras para controlar como alertas semelhantes são entregues no futuro.

Uma regra de notificação corresponde a alertas com base em condições definidas por você, como serviço, gravidade e área de impacto, e então envia uma notificação pelos canais que você selecionar. A implantação local do NetApp Console inclui regras de notificação padrão que você pode visualizar e ajustar, e você pode criar suas próprias regras personalizadas. Você também pode silenciar regras para suprimir temporariamente as notificações durante eventos planejados, como janelas de manutenção.

- "Saiba mais sobre o ONTAP EMS e os alertas disponíveis."

Antes de começar

- Para enviar notificações por e-mail, o administrador da sua organização deve configurar um servidor de e-mail na implantação local do Console. Para enviar notificações para um sistema externo, o administrador da sua organização deve configurar um webhook. Para obter as etapas, consulte "Configurar o envio de notificações".
- O Centro de Notificações da implantação local do Console exibe notificações por padrão, portanto, nenhuma configuração adicional é necessária para notificações no console.

Ver regras de notificação

A página de regras de notificação é o local central para revisar e gerenciar todas as regras aplicáveis à sua organização. Cada regra exibe seus principais atributos para que você possa avaliar e ajustar rapidamente o comportamento dos seus alertas.

Passos

1. Na barra de navegação à esquerda, selecione **Saúde > Alertas**.
2. Selecione **Configurações de notificação**.
3. Analise as regras na lista. Cada regra mostra seu status ativo, nome, os serviços e níveis de gravidade que monitora, as funções autorizadas a receber notificações, os canais de entrega habilitados, quando foi modificada pela última vez e qualquer período de silenciamento programado.
4. Para encontrar uma regra específica, use os controles de filtro e pesquisa para filtrar por status ativo, serviço, gravidade, função, canal ou status de silenciamento.

Criar uma regra de notificação

Crie uma regra de notificação para definir as condições que acionam uma notificação e como essa notificação é entregue.

Não é possível definir regras de notificação para frotas. Você só pode defini-las para sistemas específicos. Em ambientes grandes com muitos sistemas, considere criar regras mais abrangentes por gravidade, em vez de duplicar regras por sistema. Por exemplo, uma regra Crítica que abranja todos os sistemas funciona como uma regra geral, com regras adicionais direcionadas para sistemas que precisam de roteamento ou destinatários diferentes.

Exemplo de regra de notificação para alertas críticos em todos os sistemas

Suponha que você queira garantir que nenhum alerta crítico passe despercebido, independentemente do sistema de origem. Você pode criar uma regra abrangente que encaminhe todos os alertas críticos para a Central de Notificações do NetApp Console para administradores de storage.

Neste exemplo, você cria uma regra com as seguintes configurações:

- **Serviços**: todos
- **Gravidade**: crítica
- **Função do IAM**: Administrador de armazenamento
- **Sistema**: (Deixe este campo em branco para aplicar a todos os sistemas)
- **Método de entrega**: Central de Notificações do Console

Com essa regra implementada, os administradores de storage veem uma notificação no NetApp Console para cada alerta crítico em todos os sistemas. Essa regra serve como base, que você pode complementar com regras mais específicas.

Exemplo de uma regra de notificação direcionada para alertas de capacidade de administrador de storage

Suponha que seus administradores de storage precisem responder imediatamente a problemas críticos de capacidade em um sistema de produção específico, mas você não queira que alertas de menor gravidade inundem suas caixas de entrada. Você pode criar uma regra direcionada que envie e-mails aos administradores de storage somente quando um alerta crítico de capacidade for acionado nesse sistema.

Neste exemplo, você cria uma regra com as seguintes configurações:

- **Serviços**: gerenciamento do ONTAP
- **Gravidade**: crítica
- **Área de impacto**: Capacidade
- **Função do IAM**: Administrador de armazenamento
- **Sistema**: <system_name>
- **Método de entrega**: e-mail

Com essa regra em vigor, a implantação local do NetApp Console envia e-mails para todos os administradores de storage do sistema especificado quando ocorre um alerta de capacidade crítica. Alertas com menor gravidade, como aviso ou informativo, não geram e-mail, assim a equipe pode se concentrar nos problemas que exigem atenção urgente.

Passos

1. Na barra de navegação à esquerda, selecione **Saúde > Alertas**.
2. Selecione **Configurações de notificação** e, em seguida, selecione **Adicionar regra**.
3. Defina as condições que a regra corresponde:
    - **Nome da regra**: insira um nome conciso e descritivo. Este campo é obrigatório.

- **Descrição da regra**: opcionalmente, insira contexto adicional sobre o propósito da regra.
- **Serviços**: selecione um ou mais serviços ONTAP ou de plataforma aos quais a regra se aplica.
- **Funções**: selecione as funções de acesso que os usuários devem ter para receber notificações quando a regra for acionada.
- **Níveis de gravidade**: selecione quais níveis de gravidade a regra monitora, como Crítico, Aviso, Erro ou Informação.
- **Área de impacto**: selecione as áreas operacionais para corresponder, como Capacidade ou Desempenho.
- **Nome do alerta**: selecione os tipos de alerta específicos que acionam a regra.
- **Sistema**: selecione o contexto do sistema ao qual a regra se aplica.

4. Selecione os canais de entrega para a notificação:
   - **E-mail**: envia e-mails de alerta para usuários que possuem as funções selecionadas. Requer um servidor de e-mail configurado.
   - **Webhook**: envia dados de alerta para um sistema externo. Requer selecionar uma integração de webhook configurada.
   - **Central de Notificações do Console**: exibe alertas em tempo real para usuários que possuem as funções selecionadas.
5. Opcionalmente, para suprimir as notificações desta regra durante um período planejado, como uma janela de manutenção, defina um agendamento **Silenciar notificações** e escolha uma recorrência se você quiser que o período de silenciamento se repita. Você pode adicionar várias janelas de silenciamento por regra, o que é útil para ciclos de manutenção recorrentes, como a aplicação de patches semanais.
6. Selecione **Criar**.

Ativar ou desativar uma regra de notificação

Ative ou desative regras de notificação individuais para controlar quais condições geram notificações. Desative regras que não são relevantes para o seu ambiente para reduzir o ruído e ative regras para voltar a receber suas notificações.

Passos

1. Na barra de navegação à esquerda, selecione **Saúde > Alertas**.
2. Selecione **Configurações de notificação**.
3. Localize a regra que você deseja alterar.
4. Ative ou desative a opção **Ativo** da regra. A alteração entra em vigor imediatamente.

Silenciar uma regra de notificação

Silencie uma regra de notificação para suprimir o envio de alertas durante um evento planejado, como uma janela de manutenção, sem desativar a regra. Os alertas continuam a aparecer na página de Alertas durante o período de silenciamento; apenas as notificações por e-mail, webhook e no console são suprimidas. Quando o período de silenciamento expira, as notificações são retomadas automaticamente.

Você pode adicionar várias janelas de silenciamento a uma única regra e configurar cada uma para se repetir em uma programação.

Exemplos de janelas silenciosas

- **Janela de manutenção única**: você está executando uma atualização de firmware em um sistema de

storage na noite de sábado e deseja suprimir os alertas esperados durante essa janela. Defina uma janela de silenciamento de sábado, às 22h, até domingo, às 2h, sem recorrência. Quando a janela expirar, as notificações serão retomadas automaticamente.

- **Janela de atualização semanal recorrente**: Sua equipe aplica patches nos sistemas todos os domingos, da meia-noite às 4:00. Adicione uma janela de silenciamento com recorrência semanal para que as notificações sejam suprimidas automaticamente a cada semana sem intervenção manual. Se um segundo sistema tiver seu próprio cronograma de aplicação de patches em um horário diferente, adicione uma segunda janela de silenciamento à mesma regra com seu próprio horário de início e recorrência.

Passos

1. Na barra de navegação à esquerda, selecione **Saúde > Alertas**.
2. Selecione **Regras de notificação**.
3. Na lista de regras, localize a regra que você deseja silenciar e selecione o menu de ações para essa regra.
4. Selecione **Editar**.
5. Na seção **Silenciar notificações**, defina a data e a hora de início e término do período de silêncio.
6. Opcionalmente, selecione uma recorrência para repetir a janela em um cronograma.
7. Para adicionar mais janelas silenciadas, selecione **Adicionar janela silenciada** e repita os passos anteriores.
8. Selecione **Salvar**.

Excluir uma regra de notificação

Exclua uma regra de notificação se você não precisar mais dela. Excluir uma regra a remove permanentemente, portanto, você não poderá recuperá-la.

Passos

1. Na barra de navegação à esquerda, selecione **Saúde > Alertas**.
2. Selecione **Configurações de notificação**.
3. Na lista de regras, localize a regra que você deseja excluir e selecione o menu de ações para essa regra.
4. Selecione **Excluir** no menu de ações.

Informações relacionadas

- "Configurar o envio de notificações"
- "Saiba mais sobre os alertas do Console"
- "Ver alertas"

Corrigir a discrepância de classe de armazenamento na implantação local do NetApp Console

Na implantação local do NetApp Console, encontre alertas relacionados a desvios, analise as descobertas sobre desvios e corrija as cargas de trabalho que não correspondem mais à intenção da classe de armazenamento.

Funções necessárias

Administrador de storage

Você só pode visualizar e corrigir cargas de trabalho em frotas nas quais você tem permissão.

Corrigir a deriva

Quando uma carga de trabalho deixa de corresponder à sua intenção de classe de armazenamento, a implantação local do NetApp Console gera um alerta. Use o alerta para analisar a discrepância e aplicar a remediação recomendada.

Você pode aplicar algumas correções diretamente do alerta. Para outros problemas, atualize a configuração da carga de trabalho ou atribua uma classe de armazenamento diferente para restaurar a conformidade. O fluxo de trabalho de correção mostra o impacto esperado antes de você aplicar as alterações.

Passos

1. Selecione **Armazenamento > Classes de armazenamento**.

   Um resumo da variação de classe de armazenamento aparece na seção **Variações por classe de armazenamento**. A lista completa aparece na tabela.

2. Na coluna **Desvios**, selecione **Exibir** para a classe de armazenamento relevante.

   A página **Alertas > Visão geral** é aberta com filtros aplicados.

3. Selecione um alerta para abrir a página de detalhes do alerta.
4. Selecione **Analyze**.
5. Analise os resultados no **Workload analyzer**.

   Para identificar desvios de configuração, compare as configurações pretendidas e as reais para determinar o que mudou.

6. Selecione a ação corretiva recomendada, como **Fix it**.
7. Analise as alterações propostas e aplique a remediação.
8. Retorne a **Armazenamento > Classes de armazenamento** e verifique se a carga de trabalho não aparece mais como desalinhada.

   As avaliações de conformidade podem levar vários minutos para refletir as alterações de configuração recentes. Se a carga de trabalho ainda estiver listada como desalinhada, retorne à página de detalhes do alerta e selecione **Analisar** para revisar quaisquer descobertas restantes.

Informações relacionadas

- "Saiba mais sobre desvio de classe de armazenamento e conformidade na implantação local do NetApp Console"
- "Saiba mais sobre alertas de storage"
- "Ver alertas"

Ações de correção de alertas na implantação local do NetApp Console

Use esta referência para entender as ações de correção disponíveis em **Corrigir** na NetApp Console implantação local. Para cada ação, a tabela descreve o que a ação faz e o alerta relacionado. Revise os detalhes da ação na caixa de diálogo de confirmação

antes de executá-la.

Ações corretivas

Ação corretiva	Nome do alerta	Descrição do alerta	Área de impacto	Resumo da remediação
Ativar o crescimento automático do volume	Volume cheio	O volume está com pouco espaço disponível e está quase atingindo sua capacidade máxima.	Capacidade	Aumenta automaticamente o tamanho de um volume (até um limite configurado) para reduzir o risco de ficar sem espaço.
Redimensionar volume	Volume cheio	O volume está com pouco espaço disponível e está quase atingindo sua capacidade máxima.	Capacidade	Aumenta o tamanho de um volume para proporcionar mais espaço imediatamente.
Colocar volume online	Volume off-line	O volume está off-line e não está fornecendo dados.	Disponibilidade	Coloca um volume off-line online para que ele possa retomar o fornecimento de dados.
Coloque o agregado online	Agregado off-line	O agregado não está online e os volumes nele hospedados podem estar indisponíveis.	Disponibilidade	Coloca um agregado off-line online para restaurar o acesso aos volumes que ele hospeda.
Coloque a LUN online	LUN off-line	O LUN está off-line e o acesso do host está indisponível.	Disponibilidade	Coloca um LUN off-line em funcionamento para que os hosts possam retomar o acesso e as operações de E/S.
Remover restrição de volume	Volume restrito	O volume está em estado restrito e pode não servir I/O normalmente.	Disponibilidade	Restaura um volume restrito ao estado online para que os clientes possam acessá-lo novamente.
Colocar o namespace NVMe online	O namespace NVMe está off-line	O namespace NVMe está off-line e o acesso do host está indisponível.	Disponibilidade	Coloca um namespace NVMe off-line em funcionamento para restaurar o acesso do host.
Ativar LIF entre clusters	LIF entre clusters inativa	Uma LIF entre clusters está inativa e a comunicação entre clusters pode ser afetada.	Conectividade	Ativa uma LIF entre clusters para restaurar a conectividade entre clusters usada para replicação.

Ação corretiva	Nome do alerta	Descrição do alerta	Área de impacto	Resumo da remediação
Reativar o MetroCluster AUSO	MetroCluster switchover automática não planejada desativada	O switchover não planejado automático está desativado neste cluster.	Disponibilidade	Reativa o switchover automático não planejado (AUSO) para que a proteção do MetroCluster funcione conforme o esperado.
Configurar a rede do Service Processor	O Service Processor não está configurado	A rede do Service Processor (SP) não está configurada.	Gerenciabilidade	Configura as definições de rede do SP para permitir o acesso de gerenciamento fora da banda.
Atribuir discos não atribuídos	Discos não atribuídos detectados	Existem discos não atribuídos e a capacidade disponível pode não estar sendo utilizada. Atribua os discos a um nó para que possam ser usados para storage.	Disponibilidade	Atribui discos atualmente não atribuídos a um nó para que possam ser usados para storage.
Recuperação do espaço do volume raiz	Espaço do volume raiz do nó baixo	O espaço disponível no volume raiz do nó é baixo e pode afetar o funcionamento normal do sistema.	Saúde do sistema	Libera espaço no volume raiz do nó excluindo o maior snapshot ou o maior arquivo de despejo de memória. As exclusões são permanentes.

Investigue problemas de desempenho

Saiba mais sobre o NetApp Console local deployment Workload Analyzer

Use o NetApp Console Workload Analyzer de implantação local para visualizar o comportamento de um único volume ao longo do tempo. Você pode investigar a degradação de desempenho, tendências de capacidade e problemas de contenção de recursos a partir do próprio volume, de um alerta ou do inventário.

Como o Workload Analyzer identifica as causas raiz

Use o Workload Analyzer para correlacionar métricas de um único volume em seis seções para que você possa identificar rapidamente as causas principais. Selecione um volume e um intervalo de tempo para visualizar eventos, desempenho e capacidade juntos na mesma janela. Essa visualização pode ajudar você a determinar se o storage é a provável origem de um problema no aplicativo ou se outra camada, como a rede, está causando o problema.

O analisador é mais útil quando você já sabe qual volume está afetado. Se você o abrir a partir de um alerta ou do inventário de volumes, a implantação local do NetApp Console abrirá o analisador com o volume selecionado para que você possa se concentrar na janela de análise e nos gráficos.

O analisador rastreia um volume por vez, então use-o para investigar um problema específico em vez de

comparar vários volumes.

Analise a seção de capacidade como parte desta avaliação. Quando um sistema ONTAP está com mais de 85% de sua capacidade ocupada, a alta utilização pode, por si só, causar problemas de desempenho, então a baixa capacidade disponível pode explicar a latência que os gráficos de desempenho, por si só, não consideram.

Após identificar a causa raiz, você pode agir diretamente a partir do analisador. Quando as opções automatizadas estiverem disponíveis, o Console local deployment fornecerá recomendações Fix-It com etapas guiadas ou remediação com um clique.

Os gráficos de carga de trabalho para LUNs não fornecem o mesmo nível de detalhe que os gráficos para volumes, então você verá menos estatísticas ao analisar uma LUN.

Analisador de carga de trabalho de acesso

Você pode abrir o Analisador de Carga de Trabalho de diversas maneiras:

- No menu **Saúde**, selecione **Analisador de Carga de Trabalho** e, em seguida, procure e selecione o volume que você deseja analisar no campo **Volume**.
- Na página **Armazenamento > Frotas > Inventário**, navegue até o volume que você deseja analisar e selecione **Analisar** no menu de ações.
- Na página **Alertas > Visão geral**, selecione um alerta para o volume que você deseja investigar e, em seguida, selecione **Analisar** nos detalhes do alerta.

Você também pode analisar LUNs, mas elas mostram menos estatísticas do que volumes.

Analise a latência, a taxa de transferência e a capacidade de storage

Utilize estas seis seções para investigar um volume:

Seleção de volume
: Escolha o volume e o intervalo de tempo para investigar, assim todos os gráficos e eventos ficam alinhados à mesma carga de trabalho e janela de análise.

Linha do tempo do evento
: Visualize as alterações de configuração atuais e históricas, alertas de aviso e alertas críticos para o volume selecionado durante a janela de análise. Use esta seção para correlacionar "o que mudou" com alterações no desempenho ou no comportamento da capacidade.

Análise de latência
: Visualize a latência do volume ao longo do tempo, seja no total ou detalhada por centro de atraso—rede, processamento de dados, operações agregadas, interconexão de cluster e outros. Se o volume usar uma política de QoS, o analisador exibirá os limites de latência máxima e mínima da política como linhas de referência, para que você possa ver o quão próxima a carga de trabalho está de um limite de limitação. Ative a previsão para projetar se a latência está se aproximando de um limite de aviso ou crítico.

Análise de taxa de transferência
: Visualize IOPS e MB/s ao longo do tempo, com uma divisão opcional de leitura/gravação/outros. Se o volume usar uma política de QoS, o analisador exibirá as linhas de limite de IOPS e de limite de taxa de transferência. Ative a previsão para projetar se a demanda está se aproximando dos limites de QoS.

Utilização de recursos

Veja como estão ocupados os nós e agregados que atendem ao volume durante o período de análise. O analisador plota cada recurso como uma linha independente, em vez de empilhar os valores, assim você pode identificar se um nó ou agregado específico é uma fonte de contenção. Alterne a previsão para projetar se algum recurso está se aproximando de um limite de alta utilização.

Análise de capacidade

Veja como o espaço físico e o espaço disponível no volume mudaram ao longo do tempo. Passe o cursor para ver um detalhamento da eficiência de storage, incluindo economias com deduplicação, compressão e compactação. Ative a previsão para projetar quando o volume atingirá os limites de capacidade de aviso ou críticos. Alterne para a visualização de snapshot para ver como o espaço de snapshot está em relação à reserva de snapshot configurada.

Preveja tendências de capacidade e desempenho

Use a opção de previsão em cada seção de análise para estender a linha do tempo do gráfico além do momento atual e projetar valores futuros com base na tendência observada. Uma linha tracejada distingue os valores previstos dos dados reais. O analisador também exibe uma mensagem de insight quando a previsão indica que uma violação de limite é provável, juntamente com o tempo estimado para essa violação.

Informações relacionadas

"Investigar alta latência em um volume". "Investigar a alta demanda de taxa de transferência em um volume". "Investigar o crescimento da capacidade em um volume". "Saiba mais sobre as métricas do Workload Analyzer na implantação local do NetApp Console".

Investigue alta latência em um volume na implantação local do NetApp Console

Utilize o Workload Analyzer na implantação local do NetApp Console para encontrar a origem dos tempos de resposta lentos de um volume.

Se você abrir o analisador a partir de um alerta ou do inventário de volume, o volume já estará selecionado e você pode se concentrar no intervalo de tempo e nas análises detalhadas do gráfico.

Quando o desempenho do aplicativo se degrada, identifique qual parte do caminho de E/S está causando a lentidão. A seção de análise de latência detalha o tempo de resposta por centro de atraso, permitindo que você distinga entre problemas de rede, sobrecarga de processamento de dados, contenção de agregados e outros fatores.

Passos

1. Abra o Workload Analyzer usando um dos seguintes métodos:
   - No menu **Saúde**, selecione **Analisador de Carga de Trabalho** e, em seguida, procure e selecione o volume que você deseja analisar no campo **Volume**.
   - Na página **Armazenamento > Frotas > Inventário**, navegue até o volume que você deseja analisar e selecione **Analisar** no menu de ações.
   - Na página **Alertas > Visão geral**, selecione um alerta relacionado à capacidade para o volume que você deseja investigar e, em seguida, selecione **Analisar** nos detalhes do alerta.
2. Defina o **Intervalo de tempo** para abranger o período em que o problema de desempenho ocorreu, depois selecione **Analisar**.
3. Consulte a seção **Linha do tempo de eventos** para ver as alterações de configuração e os alertas que coincidem com o aumento da latência.

O analisador plota eventos de alteração de configuração (ícone de chave inglesa) e eventos de alerta (ícones de aviso e crítico) ao longo do mesmo eixo temporal que o gráfico de latência, facilitando a visualização se uma alteração precedeu a degradação.

4. Na seção **Latência**, abra o menu suspenso **Exibir** e selecione **Detalhamento por centro de atraso**. O gráfico mostra a contribuição de cada centro de atraso para a latência ao longo do tempo. Os centros de atraso incluem:
   - Latência de leitura
   - Latência de gravação
   - Outra latência
5. Passe o cursor sobre um ponto no gráfico onde a latência é mais alta para ver o valor de cada centro de atraso e sua porcentagem do total da latência.

   O maior centro de atraso geralmente aponta para o recurso em disputa. Quando um recurso compartilhado não consegue atender à demanda, os volumes que o utilizam esperam mais tempo por I/O. Reduza a carga nesse recurso, por exemplo, movendo cargas de trabalho ou ajustando um limite de QoS, para diminuir a latência.

6. Identifique o principal fator contribuinte e utilize o valor para determinar os próximos passos:
   - Alta **latência de leitura** pode indicar contenção de disco. Verifique a seção **Utilização de recursos** para confirmar a porcentagem de ocupação total.
   - Uma alta **latência de gravação** pode indicar saturação da NIC ou problemas no caminho da rede fora do cluster.
   - Alta **Outra latência** pode indicar que as configurações de eficiência em linha estão consumindo mais CPU do que a carga de trabalho pode tolerar. Considere ajustar as configurações de eficiência ou QoS.
   - Uma alta **latência do Cloud** pode indicar que a carga de trabalho está acessando frequentemente dados inativos na camada de capacidade. Considere ajustar a política de tiering.
7. Se os centros de atraso não forem responsáveis pela lentidão, verifique a seção **Análise de Capacidade**. Quando o sistema ONTAP estiver com mais de 85% de sua capacidade ocupada, a alta utilização pode causar problemas de desempenho, independentemente da divisão dos centros de atraso.
8. Se a latência aumentar imediatamente após um evento de alteração, use os detalhes do evento e os gráficos relacionados em conjunto para validar a causa provável:
   - Para alterações de QoS, compare a linha de latência com as linhas de limite de QoS e revise os gráficos de throughput para verificar se a demanda está atendendo ao limite máximo estabelecido pela política.
   - Para movimentações de agregado ou de volume, compare o pico de latência com os valores de utilização do nó e do agregado mostrados para o mesmo período.
   - Para alterações na política de hierarquização, revise a contribuição da latência na nuvem para determinar se o acesso a dados frios aumentou após a alteração.

Depois que você terminar

Se o problema foi causado por uma configuração ou um problema de posicionamento, e a implantação local do Console pode resolvê-lo, o alerta no volume pode oferecer uma opção de Fix-It.

"Saiba mais sobre as métricas do Workload Analyzer na implantação local do NetApp Console".

Investigue alta taxa de transferência em um volume na implantação local do NetApp Console

Utilize o Analisador de Carga de Trabalho na implantação local do NetApp Console para examinar a demanda de IOPS e de taxa de transferência de um volume ao longo do tempo.

Quando a carga de trabalho de um volume está consumindo mais IOPS ou taxa de transferência do que o esperado, identifique o que está impulsionando a demanda. A seção de análise de taxa de transferência mostra IOPS e MB/s com uma discriminação opcional de leitura, gravação e outras, para que você possa identificar qual tipo de E/S está gerando alta demanda e se essa demanda está se aproximando de um limite de QoS.

Se você abrir o analisador a partir de um alerta ou do inventário de volume, o volume já estará selecionado e você pode se concentrar nos gráficos de intervalo de tempo e de taxa de transferência.

Passos

1. Abra o Workload Analyzer usando um dos seguintes métodos:
   - No menu **Saúde**, selecione **Analisador de Carga de Trabalho** e, em seguida, procure e selecione o volume que você deseja analisar no campo **Volume**.
   - Na página **Armazenamento > Frotas > Inventário**, navegue até o volume que você deseja analisar e selecione **Analisar** no menu de ações.
   - Na página **Alertas > Visão geral**, selecione um alerta para o volume que você deseja investigar e, em seguida, selecione **Analisar** nos detalhes do alerta.
2. Defina o **Intervalo de Tempo** para abranger o período de alta demanda e, em seguida, selecione **Analisar**.
3. Deslize a página até a seção **Análise de Throughput**.
4. Abra o menu suspenso **Exibir** e selecione **Detalhamento (RWO)**.

   Os gráficos são divididos em componentes de leitura, gravação e outros, tanto para IOPS quanto para MB/s. Isso permite que você determine se padrões de acesso com alta demanda de leitura, alta demanda de gravação ou uma combinação dos dois estão impulsionando a demanda.

5. Use o seletor de componentes para ativar ou desativar as métricas que você deseja analisar:
   - **IOPS de leitura** e **IOPS de gravação** — operações por segundo por direção de E/S
   - **Leitura em MB/s** e **Gravação em MB/s** — taxa de transferência em megabytes por segundo por direção de E/S
   - **Outras IOPS** e **Outros MB/s** — metadados e outras operações não relacionadas a dados
   - **Limite de IOPS de QoS** e **Limite de MB/s de QoS** — limites de política que aparecem somente quando o volume usa uma política de QoS
   - **Taxa de transferência na nuvem** — MB/s gravados e lidos da nuvem, exibidos apenas para cargas de trabalho que distribuem a capacidade para a nuvem por meio do FabricPool
6. Passe o cursor sobre um pico no gráfico para ver o valor exato e a divisão percentual de cada componente naquele momento.

   A dica de ferramenta ao passar o cursor também mostra o tamanho médio de E/S (taxa de transferência dividida por IOPS) para cada categoria, o que pode indicar se a carga de trabalho está executando E/S sequencial grande ou E/S aleatória pequena.

7. Ative a opção **Mostrar Previsão** para projetar se as tendências atuais de throughput atingirão o limite de IOPS ou MB/s do QoS.

   Se a linha de previsão estiver se aproximando de uma linha de limite de QoS, o ONTAP poderá limitar a carga de trabalho em breve.

8. Se você quiser visualizar a demanda agregada sem a discriminação, abra o menu suspenso **Exibir** e selecione **Totais**.

   A visualização de totais mostra uma única linha de IOPS e uma única linha de MB/s, o que é útil para um resumo rápido da demanda geral.

Depois que você terminar

Utilize os padrões de throughput que você observar para decidir o que fazer em seguida:

- Se as operações de IOPS de leitura forem muito altas em relação às operações de IOPS de gravação, considere se as configurações de leitura antecipada ou armazenamento em cache podem reduzir a carga no volume.
- Se a carga de trabalho estiver se aproximando ou já tiver atingido o limite de IOPS ou MB/s de QoS, use as linhas de limite de QoS e as definições de métricas relacionadas para confirmar a limitação e decidir se você precisa ajustar o limite.
- Se a taxa de transferência for alta e a latência também estiver elevada, verifique a seção **Utilização de recursos** para determinar se o nó ou agregado subjacente está sob disputa. Compare os picos de taxa de transferência, os picos de latência e a utilização de recursos durante o mesmo período.
- Se o analisador mostrar um crescimento rápido da capacidade ou do instantâneo enquanto a demanda está aumentando, revise as métricas de capacidade e de instantâneo para entender como esse crescimento pode afetar o volume.

"Investigar alta latência em um volume". "Saiba mais sobre as métricas do Workload Analyzer na implantação local do NetApp Console".

Investigue o crescimento da capacidade em um volume na implantação local do NetApp Console

Utilize o Analisador de Carga de Trabalho na implantação local do NetApp Console para investigar por que um volume está ficando sem espaço.

Quando um volume está ficando cheio ou as cópias de Snapshot estão consumindo mais espaço do que o esperado, examine a capacidade e as tendências de Snapshot ao longo do tempo. A seção de análise de capacidade mostra como o espaço físico e disponível muda, detalha as economias de eficiência de storage e projeta quando o volume atingirá um limite de capacidade.

Se você abrir o analisador a partir de um alerta ou do inventário de volume, o volume já estará selecionado e você pode se concentrar nas tendências de capacidade e na janela de previsão.

Passos

1. Abra o Workload Analyzer usando um dos seguintes métodos:
   - No menu **Saúde**, selecione **Analisador de Carga de Trabalho** e, em seguida, procure e selecione o volume que você deseja analisar no campo **Volume**.
   - Na página **Armazenamento > Frotas > Inventário**, navegue até o volume que você deseja analisar e selecione **Analisar** no menu de ações.

- Na página **Alertas > Visão geral**, selecione um alerta para o volume que você deseja investigar e, em seguida, selecione **Analisar** nos detalhes do alerta.

2. Defina o **Intervalo de Tempo** para abranger o período de crescimento da capacidade e, em seguida, selecione **Analisar**.
3. Deslize a página até a seção **Análise de Capacidade**.
4. Selecione **Capacity view** no menu suspenso **View**.

   O gráfico mostra a capacidade física como a área empilhada na parte inferior e a capacidade disponível como a área empilhada na parte superior. Juntas, elas equivalem ao tamanho total do volume, assim você pode ver com que rapidez o espaço disponível está diminuindo.

5. Passe o cursor sobre um ponto no gráfico para ver a análise da eficiência de storage, incluindo as economias com deduplicação, compressão e compactação, além da taxa geral de eficiência de storage.

   Uma taxa de eficiência decrescente enquanto a capacidade física aumenta pode indicar que os dados recém-gravados não estão sendo desduplicados ou comprimidos tão bem quanto os dados existentes.

6. Para investigar o consumo de Snapshot, selecione **Snapshot View** no menu suspenso **View**.

   O gráfico mostra a reserva de Snapshot como uma linha de referência horizontal e a capacidade de Snapshot utilizada como uma área abaixo dela. Passe o cursor para ver o espaço de Snapshot utilizado e sua porcentagem em relação à reserva, a contagem total de Snapshot e a idade do Snapshot mais antigo.

   Quando o consumo de snapshots excede a reserva, os snapshots começam a consumir espaço da área de dados do volume, o que reduz o espaço disponível para novas gravações.

7. Se o volume faz tiering de dados para a nuvem, selecione **Visualização da Camada de Nuvem** no menu suspenso **Visualizar** para comparar quanto de capacidade está na camada de desempenho local em relação à camada de capacidade na nuvem.
8. Ative a opção **Mostrar Previsão** para projetar quando o volume atingirá um limite de alerta ou de capacidade crítica.

   A previsão de capacidade requer pelo menos 10 dias de dados históricos. Quando restam menos de 30 dias de capacidade antes que o volume esteja cheio, o analisador identifica o storage como quase cheio. A previsão exibe uma mensagem de insight com o tempo estimado para violação.

Depois que você terminar

Utilize as tendências de capacidade que você observar para decidir o que fazer a seguir:

- Se a capacidade disponível estiver se aproximando do limite, considere aumentar o tamanho do volume, ativar o autogrow ou mover os dados para fora do volume.
- Se a capacidade de Snapshot utilizada estiver excedendo a reserva, revise sua política de Snapshot e retenção para recuperar espaço.
- Se a razão de eficiência de storage estiver diminuindo, verifique se o tipo de dados da carga de trabalho ou as configurações de eficiência inline estão reduzindo a economia. Use "Saiba mais sobre as métricas do Workload Analyzer na implantação local do NetApp Console" para descrições detalhadas de capacidade, Snapshot e métricas de eficiência.

Métricas do Workload Analyzer na implantação local do NetApp Console

Na implantação local do NetApp Console, o Analisador de Carga de Trabalho exibe

métricas em seis seções. A descrição de cada métrica explica como o analisador renderiza a métrica no gráfico e o que ela indica sobre o comportamento do volume.

Linhas de referência de QoS em gráficos de latência

Se o volume selecionado usar uma política de QoS, você pode usar duas linhas de referência adicionais no seletor de métricas:

Linha de referência	Descrição
Limite máximo de QoS	O teto máximo de latência é definido pela política de QoS. Quando a linha de latência se aproxima ou toca esse limite, o ONTAP está limitando a carga de trabalho, e o limite de QoS — em vez de um recurso físico — é a principal fonte de latência.
Limite mínimo de QoS	O piso mínimo garantido de latência definido pela política de QoS. Esta linha indica o piso de tempo de resposta imposto à carga de trabalho. Quando outras cargas de trabalho utilizam mínimos de QoS para garantir sua taxa de transferência, o ONTAP pode limitar essa carga de trabalho, o que resulta em maior latência.

Essas linhas horizontais não aparecem na análise do centro de latência ao passar o cursor sobre o elemento. Elas servem como limites de referência, não como fatores que contribuem para a latência.

Análise da latência por tipo de I/O

Use a análise de tipo de E/S na seção **Análise de Latência** após selecionar **Análise por centro de atraso** no menu suspenso Exibir. O gráfico divide a latência total em três categorias com base na direção da operação de E/S. Use essas métricas para determinar se um problema de desempenho está afetando operações de leitura, gravação ou metadados.

Tipo de latência	Descrição	Causas comuns de valores elevados
Latência de leitura	Tempo médio para concluir uma solicitação de leitura do cliente no volume, desde o momento em que a solicitação é recebida até o retorno dos dados. As solicitações de leitura devem percorrer todo o caminho de E/S, desde a camada de protocolo de rede pela pilha de processamento de dados até o agregado onde os dados residem.	Contenção de agregados ou de disco; falhas de cache que promovem leituras para o disco físico; dados frios recuperados de uma camada de capacidade da nuvem via FabricPool; leituras entre nós quando os dados residem em um nó diferente daquele que está processando a solicitação.
Latência de gravação	Tempo médio para reconhecer uma solicitação de gravação do cliente no volume. O ONTAP reconhece uma gravação assim que ela é confirmada no log de gravação do NVRAM; os dados são posteriormente gravados no agregado.	Saturação da NIC ou alta latência de ida e volta entre o cliente e o nó de storage; SnapMirror síncrono aguardando o cluster de destino confirmar o recebimento antes que a gravação possa ser reconhecida; pressão na NVRAM sob cargas de gravação pesadas; sobrecarga de CPU devido à deduplicação, compressão ou compactação em execução no caminho de I/O de gravação.

Tipo de latência	Descrição	Causas comuns de valores elevados
Outra latência	Tempo médio para concluir operações que não sejam de leitura ou gravação no volume, incluindo abertura de arquivos, consulta de atributos, navegação em diretórios, criação de arquivos e bloqueios. Latência elevada em outras operações pode afetar a capacidade de resposta do aplicativo, mesmo quando a latência de leitura e gravação parece normal.	Pressão na CPU devido a operações de eficiência em linha que competem com o processamento de metadados; alta atividade no namespace proveniente de cargas de trabalho que geram um grande número de criações, exclusões ou varreduras de diretórios; limitação de QoS que restringe o total de IOPS, deixando menos IOPS disponíveis para operações de metadados; sobrecarga de ativação de volume quando muitos volumes estão ativos simultaneamente.

Componentes de throughput

Utilize os componentes de throughput na seção **Análise de Throughput** após você selecionar **Detalhamento (RWO)** no menu suspenso Exibir. O analisador exibe IOPS e MB/s simultaneamente.

Componente	Descrição	Renderizado como
Leitura IOPS	Operações de leitura por segundo.	Área empilhada no gráfico de IOPS.
IOPS de gravação	Operações de escrita por segundo.	Área empilhada no gráfico de IOPS.
Outros IOPS	Metadados e outras operações não relacionadas a dados por segundo.	Área empilhada no gráfico de IOPS.
Leitura MB/s	Taxa de transferência de leitura em megabytes por segundo.	Área empilhada no gráfico de MB/s.
Gravação MB/s	Taxa de transferência de escrita em megabytes por segundo.	Área empilhada no gráfico de MB/s.
Taxa de transferência da nuvem	Taxa de transferência em megabytes por segundo entre o volume e a camada de capacidade da nuvem. Essa métrica aparece apenas para cargas de trabalho que transferem capacidade para a nuvem por meio do FabricPool.	Área empilhada no gráfico de MB/s.

Os componentes de leitura, gravação e outros somam-se ao valor total de IOPS ou MB/s. Passe o cursor sobre o gráfico para ver o valor de cada componente, sua porcentagem do total e o tamanho médio de E/S (MB/s ÷ IOPS) por categoria.

Métricas de utilização de recursos

Use a seção **Utilização de Recursos** para revisar as métricas de utilização de recursos. O analisador mostra cada recurso que atende ao volume como uma linha independente. Os recursos não se acumulam.

Métricas do nó

Métrica	Descrição
Utilização de nós	Percentual de utilização composto para o nó. Passe o cursor sobre para ver a utilização de CPU, a utilização de rede e a margem disponível para cada nó.
Utilização de CPU	Porcentagem da capacidade de CPU do nó em uso. A dica de ferramenta exibida ao passar o cursor mostra esse valor.
Utilização de rede	Porcentagem da capacidade de rede do nó em uso. A dica de ferramenta exibida ao passar o cursor mostra esse valor.
Margem	Capacidade restante do nó disponível para carga de trabalho adicional. A dica de ferramenta ao passar o cursor mostra esse valor.

Métricas de agregado

Métrica	Descrição
Utilização de agregado	Percentual de ocupação do disco no agregado. Passe o cursor para ver o valor de ocupação do disco, o número de volumes no agregado e o espaço disponível.
Disco ocupado	Percentual do tempo em que os discos do agregado atendem ativamente solicitações de E/S. A dica de ferramenta exibida ao passar o cursor mostra esse valor.
Contagem de volumes	Número de volumes atualmente hospedados no agregado. A dica de ferramenta exibida ao passar o cursor mostra esse valor.
Margem	Capacidade agregada restante disponível para carga de trabalho adicional. A dica de ferramenta exibida ao passar o cursor mostra esse valor.

Quando uma linha de utilização de nó ou agregado cruza o limite de aviso de alta utilização, que o gráfico marca com uma linha de referência tracejada, outras cargas de trabalho nesse recurso podem estar competindo com o volume selecionado por capacidade de E/S.

Métricas de capacidade

Visão de capacidade

Use a seção **Análise de Capacidade** para revisar as métricas de Visualização de Capacidade após você selecionar **Visualização de Capacidade** no menu suspenso Exibir.

Métrica	Descrição
Capacidade física	Espaço consumido em disco após as operações de eficiência de storage. Esta é a área empilhada na parte inferior do gráfico. Físico + Disponível sempre é igual ao tamanho total do volume.
Capacidade disponível	Espaço livre restante no volume. Esta é a área empilhada superior no gráfico. Ela diminui à medida que a Capacidade Física aumenta.
Índice de Eficiência de Storage	Índice de eficiência geral (dados lógicos ÷ dados físicos). A dica de ferramenta exibida ao passar o cursor mostra esse valor. Ele reflete a economia combinada da desduplicação, compressão e compactação.
Economias com a desduplicação	Espaço economizado ao remover blocos de dados duplicados. A dica de ferramenta ao passar o cursor mostra esse valor.

Métrica	Descrição
Economia de compressão	Espaço economizado pela compactação de dados em linha. A dica de ferramenta exibida ao passar o cursor mostra esse valor.
Economia de compactação	O espaço é economizado ao compactar vários blocos pequenos em um único bloco físico. A dica de ferramenta ao passar o cursor exibe esse valor.

Visualização de Snapshot

Use a Visualização de Snapshot quando você quiser analisar métricas específicas de Snapshot.

Métrica	Descrição	Renderizado como
Snapshot disponível	Espaço pré-alocado reservado para snapshots, configurado como uma porcentagem do tamanho do volume.	Linha de referência horizontal.
Snapshot usado	Espaço real consumido pelas cópias de Snapshot.	Gráfico de área abaixo da linha de reserva.

Passe o cursor sobre o gráfico para ver o tamanho da reserva de Snapshot, o espaço usado pelo Snapshot e sua porcentagem da reserva, a contagem total de Snapshot e a idade do Snapshot mais antigo. Quando o consumo de Snapshot excede a reserva, os Snapshots começam a consumir espaço da área de dados do volume.

Comportamento de previsão

Use a opção **Mostrar Previsão** em qualquer seção de análise quando você quiser projetar valores futuros além do período atual com base na tendência observada. Os seguintes comportamentos se aplicam a todas as seções:

Aspecto	Comportamento
Janela de projeção	Projeta para frente com base no intervalo de tempo selecionado. Para uma visualização de 2 horas, a janela de projeção é de aproximadamente 1 hora. Para uma visualização de 7 dias, a janela de projeção se estende por vários dias.
Estilo visual	O analisador exibe os valores previstos como uma linha tracejada. Um separador vertical marca o limite entre os dados reais e os valores projetados.
Alertas de limite	O analisador exibe uma mensagem informativa quando a previsão indica que o volume ultrapassará um limite de alerta ou crítico, juntamente com uma estimativa do tempo para a violação.
Base de tendência	A projeção utiliza a taxa de alteração da porção mais recente do intervalo de tempo selecionado. Alta volatilidade nos dados recentes reduz a confiabilidade da previsão.
Dados mínimos necessários	A previsão de capacidade requer pelo menos 10 dias de dados históricos. Quando restam menos de 30 dias de capacidade antes que o volume esteja cheio, o analisador identifica o storage como quase cheio.

Informações relacionadas

- "Saiba mais sobre o NetApp Console local deployment Workload Analyzer"

- "Investigar alta latência em um volume"
- "Investigar a alta demanda de taxa de transferência em um volume"
- "Investigar o crescimento da capacidade em um volume"

Administrar e monitorar a implantação local do NetApp Console

Saiba mais sobre administração e monitoramento na implantação local do NetApp Console

Após implantar a implementação local do NetApp Console, use as ferramentas de administração e monitoramento para revisar a atividade, manter a VM e gerenciar o acesso dos membros.

Atividade de auditoria

Analise a atividade do usuário e da API, acompanhe o status das operações do Console, baixe os registros de auditoria e exporte os registros para ferramentas externas quando você precisar de maior retenção ou análise adicional.

- "Audite a atividade de implantação local do NetApp Console"
- "Configure os canais de entrega de notificações na implantação local do NetApp Console"

Licenses and subscriptions

Utilize as informações de licenciamento e assinaturas para entender os direitos de serviço e o status da assinatura do seu ambiente do Console.

"Saiba mais sobre Licenses and subscriptions".

Manter e solucionar problemas da VM de implantação local do Console

Realizar a manutenção da máquina virtual que hospeda a implantação local do Console, revisar as configurações de rede e do sistema, acessar ferramentas de diagnóstico e solucionar problemas quando o serviço ou o agente não se comportam como esperado.

"Mantenha seu vCenter ou host ESXi para implantação local do Console".

Gerenciar usuários e acessos

Analise o acesso de membros em toda a sua organização, ajuste o acesso no nível da frota e gerencie configurações de segurança, como recuperação de MFA e credenciais de contas de serviço.

- "Gerencie o acesso de membros no NetApp Console"
- "Visualize ou altere as atribuições de acesso à frota na NetApp Console implantação local"
- "Gerencie a segurança dos membros na implantação local do NetApp Console"

Audite a atividade de implantação local do NetApp Console

Você pode auditar a atividade do usuário iniciada tanto pela interface do usuário quanto pela API na página de auditoria, e pode monitorar o status das operações na implantação local do NetApp Console e o usuário que as iniciou.

Funções necessárias

Super admin, administrador da organização, administrador de pastas e frotas, analista de suporte operacional, super viewer, visualizador da organização ou visualizador de pastas e frotas. "Saiba mais sobre funções de acesso".

Você pode visualizar a atividade de auditoria na implantação local do Console, baixar um arquivo CSV do log de auditoria ou configurar o log de auditoria para ser enviado ao seu próprio servidor syslog usando um webhook.

Audite a atividade do usuário na página Audit.

Utilize a página de Auditoria para identificar quem realizou uma ação ou seu status.

A página de Auditoria mostra as ações que os usuários realizaram em sua organização. Por exemplo, você pode verificar quem adicionou um membro à organização ou se uma frota foi excluída com sucesso, além de ver outras ações de gerenciamento de storage realizadas pelos usuários em sua organização.

Os logs de auditoria mostram a atividade dos seguintes serviços:

- Tenancy: ações relacionadas ao gerenciamento da sua organização, como adicionar usuários, criar frotas e associar recursos.
- Gerenciamento de storage: ações relacionadas ao gerenciamento de seus recursos de storage.
- Federação: ações relacionadas ao gerenciamento de federações, como criar federações e adicionar ou remover organizações federadas.

Passos

1. Selecione **Administração > Auditoria**.
2. Use os filtros acima da tabela para alterar quais ações são exibidas na tabela.

   Por exemplo, você pode usar o filtro **Serviço** para exibir ações relacionadas a um serviço específico ou pode usar o filtro **Usuário** para exibir ações relacionadas a uma conta de usuário específica.

Filtre os logs de auditoria para ações de gerenciamento de identidade e acesso

Para visualizar apenas as ações relacionadas ao gerenciamento da sua organização, como adicionar membros, criar frotas ou excluir recursos, filtre o log de auditoria pelo serviço Tenancy.

Passos

1. Selecione **Administração > Auditoria**.
2. Use os filtros para refinar os resultados. Selecione **Serviço** e depois selecione **Locação**.
3. Utilize qualquer um dos outros filtros para refinar ainda mais os resultados.

   Por exemplo, use o filtro **Usuário** para exibir as ações do IAM realizadas por uma conta de usuário específica.

Faça o download dos logs de auditoria na página de Auditoria

Você pode baixar os logs de auditoria da página Auditoria para um arquivo CSV. Isso permite que você mantenha um registro das ações que os usuários realizam em sua organização. O arquivo CSV baixado inclui todas as colunas do log de auditoria, independentemente dos filtros ou colunas exibidas na página Auditoria.

Passos

1. Na página **Audit**, selecione o ícone de download no canto superior direito da tabela.

Manter o NetApp Console

Mantenha seu vCenter ou host ESXi para implantação local do NetApp Console

Na implantação local do NetApp Console, você pode fazer alterações no seu VCenter ou host ESXi existente após implantar o Console local deployment. Por exemplo, você pode aumentar a CPU ou a RAM da instância de VM que hospeda o Console local deployment.

Execute essas tarefas de manutenção usando o console web da VM:

- Aumentar o tamanho do disco
- Reinicie a implantação local do NetApp Console
- Atualizar rotas estáticas
- Atualizar domínios de pesquisa

Limitações

Você só pode visualizar (e não atualizar) informações sobre o endereço IP, DNS e gateways através do console de manutenção.

Acesse o console de manutenção da VM

Você pode acessar o console de manutenção a partir do cliente VSphere.

Passos

1. Abra o cliente VSphere e faça login no seu vCenter.
2. Selecione a instância de máquina virtual que hospeda a implantação local do Console.
3. Selecione **Launch Web Console**.
4. Faça login na instância da máquina virtual usando o nome de usuário e a senha que você especificou ao criar a instância da máquina virtual. O nome de usuário é `maint` e a senha é a que você especificou ao criar a instância da máquina virtual.

Alterar a senha do usuário de manutenção

Você pode alterar a senha do usuário `maint`.

Passos

1. Abra o cliente VSphere e faça login no seu vCenter.
2. Selecione a instância de máquina virtual que hospeda a implantação local do Console.
3. Selecione **Launch Web Console**.

4. Faça login na instância da máquina virtual usando o nome de usuário e a senha que você especificou ao criar a instância da máquina virtual. O nome de usuário é `maint` e a senha é a que você especificou ao criar a instância da máquina virtual.
5. Digite `1` para ver o `System Configuration` menu.
6. Digite `1` para alterar a senha do usuário de manutenção e siga as instruções na tela.

Aumente a CPU ou a RAM da instância da máquina virtual

Você pode aumentar a CPU ou a RAM da instância da máquina virtual que hospeda a implantação local do Console.

Edite as configurações da instância da máquina virtual no seu vCenter ou host ESXi e, em seguida, use o Console de manutenção para aplicar as alterações.

Etapas no cliente VSphere

1. Abra o cliente VSphere e faça login no seu vCenter.
2. Selecione a instância de máquina virtual que hospeda a implantação local do Console.
3. Clique com o botão direito do mouse na instância da máquina virtual e selecione **Editar configurações**.
4. Aumente o espaço em disco rígido usado para /opt ou para a partição /var.
   a. Selecione **Disco Rígido 2** para aumentar o espaço em disco rígido usado para /opt.
   b. Selecione **Disco Rígido 3** para aumentar o espaço em disco rígido usado para /var.
5. Salve suas alterações.

Etapas no console de manutenção

1. Abra o cliente VSphere e faça login no seu vCenter.
2. Selecione a instância de máquina virtual que hospeda a implantação local do Console.
3. Selecione **Launch Web Console**.
4. Faça login na instância da máquina virtual usando o nome de usuário e a senha que você especificou ao criar a instância da máquina virtual. O nome de usuário é `maint` e a senha é a que você especificou ao criar a instância da máquina virtual.
5. Digite `1 to view the `System Configuration`menu.
6. Digite `2` e siga as instruções na tela. O console verifica se há novas configurações e aumenta o tamanho das partições.

Visualize as configurações de rede da VM de implantação local do NetApp Console

Visualize as configurações de rede da VM de implantação local do Console no cliente VSphere para confirmar ou solucionar problemas de rede. Você só pode visualizar (e não atualizar) as seguintes configurações de rede: endereço IP e detalhes de DNS.

Passos

1. Abra o cliente VSphere e faça login no seu vCenter.
2. Selecione a instância de máquina virtual que hospeda a implantação local do Console.
3. Selecione **Launch Web Console**.
4. Faça login na instância da máquina virtual usando o nome de usuário e a senha que você especificou ao criar a instância da máquina virtual. O nome de usuário é `maint` e a senha é a que você especificou ao

criar a instância da máquina virtual.

5. Digite `2` para ver o `Network Configuration` menu.
6. Digite um número entre 1 e 6 para visualizar as configurações de rede correspondentes.

Atualize as rotas estáticas para a VM de implantação local do Console

Adicione, atualize ou remova rotas estáticas para a VM de implantação local do Console conforme necessário.

Passos

1. Abra o cliente VSphere e faça login no seu vCenter.
2. Selecione a instância de máquina virtual que hospeda a implantação local do Console.
3. Selecione **Launch Web Console**.
4. Faça login na instância da máquina virtual usando o nome de usuário e a senha que você especificou ao criar a instância da máquina virtual. O nome de usuário é `maint` e a senha é a que você especificou ao criar a instância da máquina virtual.
5. Digite `2` para ver o `Network Configuration` menu.
6. Digite `7` para atualizar as rotas estáticas e siga as instruções na tela.
7. Pressione Enter.
8. Opcionalmente, faça alterações adicionais.
9. Digite `9` para confirmar as suas alterações.

Atualize as configurações de pesquisa de domínio para a VM de implantação local do NetApp Console

Você pode atualizar as configurações do domínio de pesquisa para a VM de implantação local do Console.

Passos

1. Abra o cliente VSphere e faça login no seu vCenter.
2. Selecione a instância de máquina virtual que hospeda a implantação local do Console.
3. Selecione **Launch Web Console**.
4. Faça login na instância da máquina virtual usando o nome de usuário e a senha que você especificou ao criar a instância da máquina virtual. O nome de usuário é `maint` e a senha é a que você especificou ao criar a instância da máquina virtual.
5. Digite `2` ` para ver o `Network Configuration` menu.
6. Digite `8` para atualizar as configurações de pesquisa de domínio e siga as instruções na tela.
7. Pressione Enter.
8. Opcionalmente, faça alterações adicionais.
9. Digite `9` para confirmar as suas alterações.

Acesse as ferramentas de diagnóstico de implantação local do NetApp Console.

Acesse as ferramentas de diagnóstico para solucionar problemas com a implantação local do Console. NetApp Support pode pedir que você faça isso ao solucionar problemas.

Passos

1. Abra o cliente VSphere e faça login no seu vCenter.
2. Selecione a instância de máquina virtual que hospeda a implantação local do Console.
3. Selecione **Launch Web Console**.
4. Faça login na instância da máquina virtual usando o nome de usuário e a senha que você especificou ao criar a instância da máquina virtual. O nome de usuário é `maint` e a senha é a que você especificou ao criar a instância da máquina virtual.
5. Digite `3` para visualizar o menu Suporte e Diagnóstico.
6. Digite `1` para acessar as ferramentas de diagnóstico e siga as instruções na tela.

Acesse remotamente as ferramentas de diagnóstico de implantação local do Console.

Você pode acessar ferramentas de diagnóstico remotamente com uma ferramenta como o PuTTY. Habilite o acesso SSH à VM de implantação local do Console atribuindo uma senha de uso único.

O acesso SSH permite funcionalidades avançadas do terminal, como copiar e colar.

Passos

1. Abra o cliente VSphere e faça login no seu vCenter.
2. Selecione a instância de máquina virtual que hospeda a implantação local do Console.
3. Selecione **Launch Web Console**.
4. Faça login na instância da máquina virtual usando o nome de usuário e a senha que você especificou ao criar a instância da máquina virtual. O nome de usuário é `maint` e a senha é a que você especificou ao criar a instância da máquina virtual.
5. Digite `3` para ver o `Support and Diagnostics` menu.
6. Digite `2` para acessar as ferramentas de diagnóstico e siga as instruções na tela para configurar uma senha de uso único que expira em 24 horas.
7. Utilize uma ferramenta SSH como o Putty para se conectar à VM de implantação local do Console usando o nome de usuário `diag` e a senha de uso único que você configurou.

Gerenciar usuários e acessos

Gerencie o acesso de membros na implantação local do NetApp Console

Na implantação local do NetApp Console, revise ou altere as funções de um usuário em várias pastas ou frotas, como verificar tudo o que um engenheiro de armazenamento pode acessar, adicionar uma nova função em outra região ou remover o acesso desse usuário quando as responsabilidades mudarem.

Funções de acesso necessárias

Superadministrador, administrador da organização ou administrador de pastas ou frotas (para pastas e frotas que estão administrando). "Saiba mais sobre funções de acesso".

Você pode visualizar e gerenciar o acesso de duas maneiras, dependendo das suas necessidades. Se você quiser visualizar as funções que um determinado usuário possui em toda a frota da sua organização, use a página **Membros**.

Se você deseja confirmar quem pode acessar uma frota específica, verifique os membros atribuídos a essa

frota. "Gerencie as atribuições de acesso à frota".

Para adicionar um novo membro, conta de serviço ou usuário do diretório e atribuir sua primeira função, use a tarefa de integração em vez disso. "Adicione membros e atribua funções".

Entenda como o acesso é concedido no NetApp Console

O NetApp Console utiliza controle de acesso baseado em funções (RBAC) para gerenciar as permissões dos membros. Você pode atribuir funções predefinidas no nível da organização, da pasta ou da frota, dependendo do escopo de acesso que um membro precisa.

Utilizando a herança de funções

Uma função que você atribui no nível da organização ou da pasta é herdada pelos escopos filhos abaixo dela, portanto, altere uma atribuição herdada no escopo superior onde você a concedeu originalmente.

"Saiba mais sobre herança de funções na implantação local do NetApp Console".

Veja as funções atribuídas a um membro

Confirme exatamente quais funções um membro possui e em qual âmbito antes de fazer qualquer alteração. Por exemplo, verifique se um colega de equipe já tem a função de administrador de armazenamento na `Production-EU-West` frota.

Se você tiver a função de *Administrador de pasta ou frota*, a página exibirá todos os membros da organização. No entanto, você só pode visualizar e gerenciar permissões apenas para as pastas e frotas que administra. "Saiba mais sobre as ações de administração de pastas ou frotas no NetApp Console implantação local".

1. Na página **Membros**, navegue até um membro na tabela, selecione ••• e, em seguida, selecione **Ver detalhes**.
2. Na tabela, expanda a linha correspondente à organização, pasta ou frota onde você deseja visualizar a função atribuída ao membro e selecione **Visualizar** na coluna **Função**.

Atribuir ou modificar o acesso de membro

Você pode ajustar o acesso de um membro sempre que as responsabilidades mudarem. Por exemplo, quando um colega de equipe assume as funções de backup para uma segunda região, adicione a função de administrador de Backup e Recovery à frota dessa região sem alterar suas funções de armazenamento existentes.

Se você precisar adicionar um novo membro e atribuir sua primeira função, consulte "Adicione membros e atribua funções".

Adicionar uma função de acesso a um membro existente

Atribua a um membro uma função adicional no nível da organização, pasta ou frota quando suas responsabilidades aumentarem. Por exemplo, atribua a um Storage admin a função de Backup and recovery admin no nível da organização para que ele possa gerenciar tarefas de backup e recuperação em todas as frotas sem perder suas permissões de armazenamento existentes.

Você pode atribuir a um membro uma função de acesso para sua organização, pasta ou frota.

Os membros podem ter várias funções dentro da mesma frota e em frotas diferentes. Por exemplo, organizações menores podem atribuir todas as funções de acesso disponíveis ao mesmo usuário, enquanto organizações maiores podem ter usuários que executam tarefas mais especializadas. Alternativamente, você

também pode atribuir a um usuário a função de administrador de resiliência a ransomware no nível da organização. Nesse exemplo, o usuário poderá executar tarefas de resiliência a ransomware em todas as frotas da sua organização.

Sua estratégia de funções de acesso deve estar alinhada com a forma como você organizou seus recursos da NetApp.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Members**.
3. Selecione uma das abas de membros: **Usuários**, **Usuários do diretório** ou **Contas de serviço**.
4. Selecione o menu de ações ••• ao lado do membro ao qual você deseja atribuir uma função e selecione **Adicionar uma função**.
5. Para adicionar uma função, siga os passos indicados na caixa de diálogo:
   - **Selecione uma organização, pasta ou frota**: escolha o nível da sua hierarquia de recursos para o qual o membro deve ter permissões.

     Se você selecionar a organização ou uma pasta, o membro terá permissões para tudo o que estiver dentro da organização ou pasta.

   - **Selecione uma categoria**: escolha uma categoria de função. "Saiba mais sobre funções de acesso".
   - Selecione uma **função**: escolha uma função que conceda ao membro permissões para os recursos associados à organização, pasta ou frota que você selecionou.
   - **Adicionar função**: se você deseja conceder acesso a pastas ou frotas adicionais dentro da sua organização, selecione **Adicionar função**, especifique outra pasta, frota ou categoria de função e, em seguida, selecione uma categoria de função e a função correspondente.
6. Selecione **Adicionar novas funções**.

Alterar a função atribuída a um membro

Substitua a função atual de um membro por uma diferente quando suas responsabilidades mudarem. Por exemplo, quando um visualizador de armazenamento na `Production-US-East` frota precisar da função de administrador de armazenamento.

Cada usuário deve ter pelo menos uma função. Você não pode remover todas as funções de um usuário. Se precisar remover todas as funções, exclua o usuário da sua organização.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Members**.
3. Selecione uma das abas de membros: **Usuários**, **Usuários do diretório** ou **Contas de serviço**.
4. Na página **Membros**, navegue até um membro na tabela, selecione ••• e, em seguida, selecione **Ver detalhes**.
5. Na tabela, expanda a linha correspondente à organização, pasta ou frota onde você deseja alterar a função atribuída ao membro e selecione **Exibir** na coluna **Função** para visualizar as funções atribuídas a esse membro.
6. Você pode alterar uma função existente para um membro ou remover uma função.

a. Para alterar a função de um membro, selecione **Alterar** ao lado da função que você deseja alterar. Você só pode alterar uma função para outra dentro da mesma categoria de função. Por exemplo, você pode alterar de uma função de serviço de dados para outra. Confirme a alteração.

b. Para remover a função de um membro, selecione ao lado da função para remover a respectiva função do membro. Você será solicitado a confirmar a remoção.

Remover um membro da sua organização

Remova um membro quando ele deixar a organização ou mudar de função de forma que não precise mais de acesso ao Console. Por exemplo, quando o contrato de um prestador de serviços terminar ou quando um funcionário for transferido para uma equipe fora da sua organização do Console.

Usuários do diretório

Remover um usuário do seu diretório impede que ele se autentique. Você também deve remover o usuário da sua organização do Console para manter a lista de membros precisa e remover quaisquer funções atribuídas na implantação local do Console.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Members**.
3. Selecione uma das abas de membros: **Usuários**, **Usuários do diretório** ou **Contas de serviço**.
4. Na página **Membros**, navegue até um membro na tabela, selecione ••• e depois selecione **Excluir usuário**.
5. Confirme que você deseja remover o membro da sua organização.

Visualize ou altere as atribuições de acesso à frota na NetApp Console implantação local

Audite ou altere as atribuições de acesso de membros para pastas e frotas de armazenamento na implantação local do NetApp Console. Os administradores de pastas e frotas geralmente trabalham a partir dessa visualização, pois ela mostra apenas os escopos que eles administram.

Funções de acesso necessárias

Superadministrador, administrador da organização ou administrador de pasta ou frota. "Saiba mais sobre funções de acesso".

Alternativamente, você pode gerenciar todas as funções de um membro específico em várias pastas ou frotas. "Gerencie o acesso de membros".

Como funciona o acesso a pastas e frotas

A implantação local do console usa controle de acesso baseado em funções (RBAC). Uma função que você atribui no nível da pasta se aplica a todas as frotas e subpastas dentro dessa pasta; uma função que você atribui no nível da frota se aplica somente aos recursos dessa frota. "Saiba mais sobre herança de funções na implantação local do NetApp Console".

Não é possível alterar uma função no nível da frota se um membro a herdar de uma pasta ou da organização. Para alterar o acesso herdado, altere a função no escopo superior.

Veja os membros atribuídos a uma pasta ou frota

Verifique exatamente quem pode gerenciar uma pasta ou frota específica. Por exemplo, antes de associar um novo cluster ONTAP de produção à `Production-US-East`frota, abra a guia Acesso da frota para confirmar quem tem acesso.

Passos

1. Selecione **Administração** > **Identidade e acesso**.
2. Selecione **Organization**.
3. Na página Organização, navegue até uma pasta ou frota na tabela, selecione ••• e, em seguida, selecione **Editar pasta** ou **Editar frota**.
4. Selecione **Acesso** para visualizar os membros que têm acesso à pasta ou à frota.

Modificar o acesso de membros a partir de uma pasta ou frota

Ajuste as funções dos membros que já pertencem à sua organização, restringindo-as a uma única pasta ou frota. Por exemplo, quando um membro da equipe migrar de uma frota de desenvolvimento para uma frota de produção, promova-o de Storage viewer para Storage admin na frota de produção, sem afetar o acesso dele em outros locais.

Para adicionar um novo membro e atribuir sua primeira função, use a tarefa de integração. "Adicione membros e atribua funções".

Passos

1. Na página Organização, navegue até uma pasta ou frota na tabela, selecione ••• e, em seguida, selecione **Editar pasta** ou **Editar frota**.
2. Selecione **Acesso** para visualizar a lista de membros que têm acesso.
3. Modificar o acesso de membros:
   - **Alterar a função de um membro**: Para qualquer membro com uma função diferente de Organization admin, selecione a função atual e escolha uma nova função. A alteração se aplica somente a este escopo; funções herdadas de um escopo superior não aparecem aqui.
   - **Remover acesso de membro neste escopo**: Para um membro que tenha uma função definida diretamente nesta pasta ou frota, remova a função para revogar o acesso dele neste escopo. Isso não remove o membro da sua organização nem afeta as funções que ele possui em outros escopos.

     "Remover um membro da sua organização".
4. Selecione **Aplicar**.

Gerencie a segurança dos membros na implantação local do NetApp Console

Proteja o acesso dos usuários à sua organização de implantação local do NetApp Console gerenciando as configurações de segurança dos membros. Você pode orientar os usuários locais a alterarem suas próprias senhas, gerenciar a autenticação multifator (MFA) dos usuários locais e recriar as credenciais da conta de serviço.

Funções de acesso necessárias

Superadministrador, administrador da organização ou administrador de pasta ou frota. "Saiba mais sobre funções de acesso".

Redefinir senhas de usuários (somente usuários locais)

Os administradores não podem redefinir as senhas de usuários locais diretamente.

Oriente os usuários locais a redefinirem suas senhas na página de login da implantação local do Console, selecionando **Esqueceu sua senha?**.

Esta opção não está disponível para usuários do diretório.

Gerencie a autenticação multifator (MFA) de um usuário local

Se um usuário local perder o acesso ao seu dispositivo MFA, você pode remover ou desativar a configuração de MFA dele.

A autenticação multifator está disponível apenas para usuários locais. Usuários do diretório não podem habilitar a autenticação multifator por meio da implantação local do Console.

Use estas orientações para escolher a ação correta:

- Selecione **Desativar** quando o usuário perder temporariamente o acesso ao seu dispositivo MFA. Desativar o MFA permite um login sem MFA por oito horas e, em seguida, o MFA é reativado automaticamente.
- Selecione **Remover** quando o usuário precisar redefinir completamente a MFA. Após remover a MFA, o usuário faz login sem MFA até configurar a MFA novamente.

Se um usuário tiver um código de recuperação salvo, ele pode entrar com esse código. Se um usuário não tiver um código de recuperação, desative a autenticação multifator (MFA) para que o usuário possa entrar e recuperar o acesso.

Para gerenciar a autenticação multifator de um usuário local, você deve ter um endereço de e-mail no mesmo domínio que o usuário afetado.

Passos

1. Selecione **Administração** > **Identidade e acesso**.
2. Selecione **Members**.
3. Na página de Membros, navegue até um membro na tabela, selecione ••• e depois selecione **Gerenciar autenticação multifator**.
4. Escolha se deseja remover ou desativar a configuração de MFA do usuário.

Depois que você terminar

Analise o log de auditoria para confirmar quem alterou o acesso MFA, quando a alteração foi feita e se a ação foi bem-sucedida. "Saiba como auditar a atividade de implantação local do NetApp Console".

Recrie as credenciais para uma conta de serviço

Você pode criar novas credenciais para uma conta de serviço caso as perca ou precise atualizá-las.

A criação de novas credenciais exclui as antigas. Você não pode usar as credenciais antigas.

Passos

1. Selecione **Administração** > **Identidade e acesso**.

2. Selecione **Members**.
3. Na tabela Membros, navegue até uma conta de serviço, selecione ••• e depois selecione **Recriar segredos**.
4. Selecione **Recriar**.
5. Baixe ou copie o client ID e o client secret.

   A implantação local do Console exibe o segredo do cliente apenas uma vez. Certifique-se de copiá-lo ou baixá-lo e armazená-lo em local seguro.

Referência

NetApp Console API de implantação local

Gerencie a organização de implantação local do seu NetApp Console e os IDs da frota

Na implantação local do NetApp Console, sua organização do NetApp Console tem um nome e um ID. Você pode escolher um nome para sua organização para ajudar a identificá-la. Você também pode precisar recuperar o ID da organização para certas integrações.

Funções de acesso necessárias

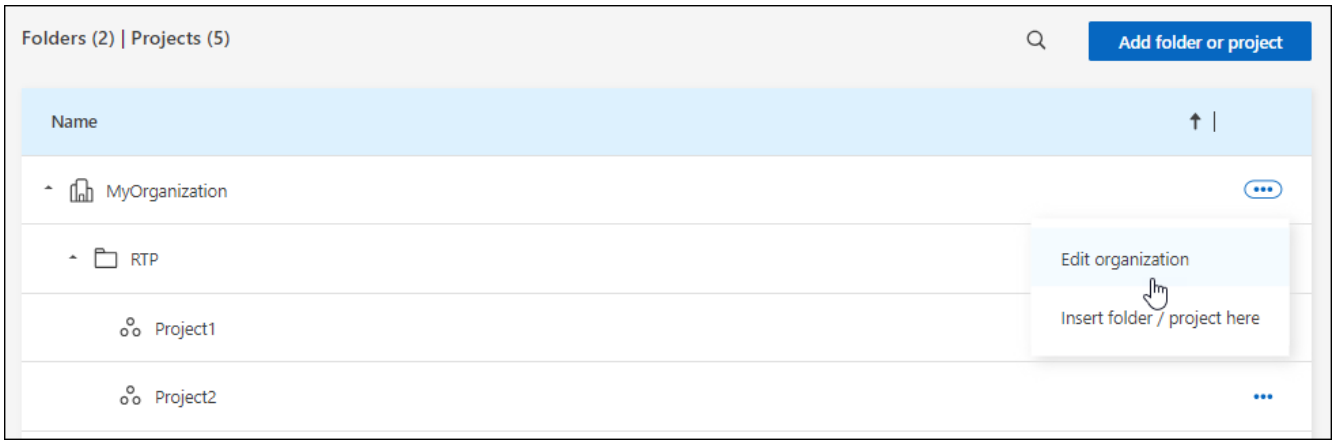
Superadministrador ou administrador da organização. "Saiba mais sobre funções de acesso".

Renomeie sua organização

Você pode renomear sua organização.

Passos

1. Selecione **Administração > Identidade e acesso**.
2. Selecione **Organization**.
3. Na página **Organização**, navegue até a primeira linha da tabela, selecione ••• e, em seguida, selecione **Editar organização**.



4. Insira o nome da nova organização e selecione **Aplicar**.

Obtenha o ID da organização

O ID da organização é usado para determinadas integrações com o Console.

Você pode visualizar o ID da organização na página Organizações e copiá-lo para a área de transferência conforme sua necessidade.

Passos

1. Selecione **Administração > Identidade e acesso** > **Organização**.
2. Na página **Organização**, procure o ID da sua organização na barra de resumo e copie-o para a área de transferência. Você pode salvá-lo para usar mais tarde ou copiá-lo diretamente para onde precisar usá-lo.

Obtenha o ID de uma frota

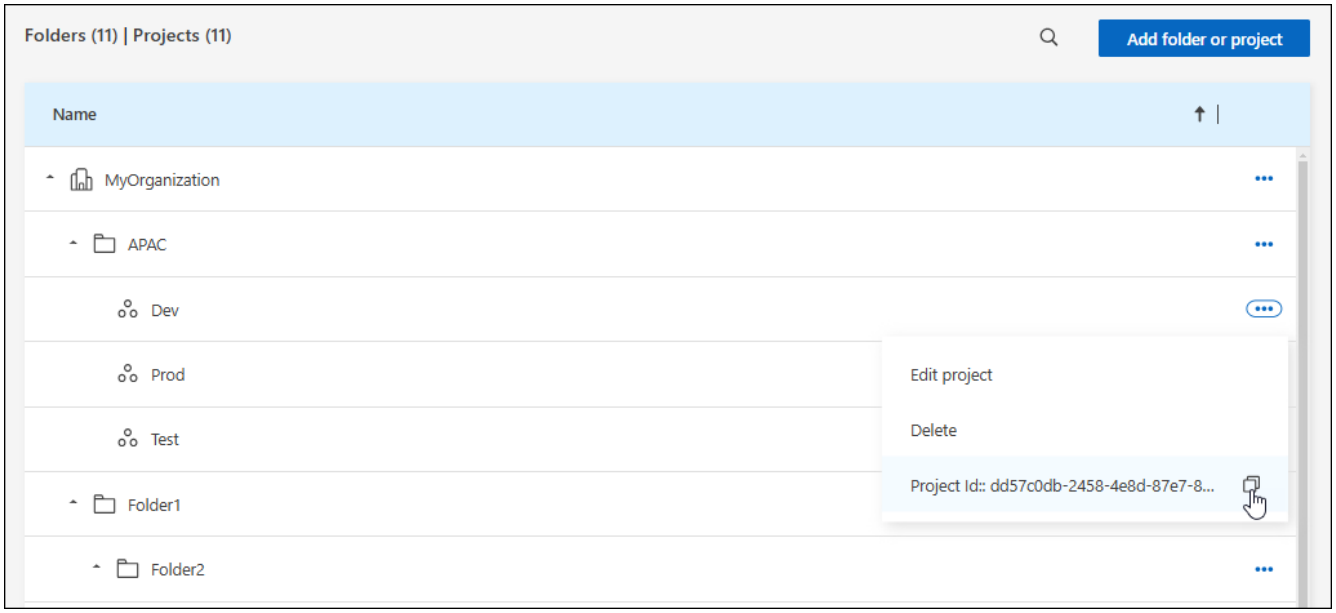
Você precisará obter o ID de uma fleet se estiver usando a API.

Passos

1. Na página **Organização**, navegue até uma frota na tabela e selecione •••

   O ID da frota é exibido.

2. Para copiar o ID, selecione o botão copiar.



Informações relacionadas

- "Saiba mais sobre gerenciamento de identidade e acesso"
- "Comece a usar identidade e acesso no NetApp Console"
- "Saiba mais sobre a API de identidade e acesso"

Fornecedores e modelos LLM suportados na implantação local do NetApp Console

NetApp Console local deployment oferece suporte aos tipos de provedor OpenAI, compatíveis com OpenAI e Anthropic LLM. Os modelos que você pode selecionar dependem do tipo de provedor e do endpoint que você configurar.

Esta documentação sobre como conectar um LLM ao assistente do Console para habilitar recursos de IA é fornecida como uma prévia da tecnologia. Com esta oferta de prévia, NetApp reserva-se o direito de modificar os detalhes, o conteúdo e o cronograma da oferta antes da Disponibilidade Geral.

Escolha um modelo que corresponda aos seus requisitos de desempenho, custo e governança.

Veja como o tipo de provedor afeta a disponibilidade do modelo

O tipo de provedor que você escolher determina quais modelos aparecem na lista de modelos de implantação local do NetApp Console:

- **OpenAI** — fornece modelos para integração direta com o OpenAI.
- **Compatível com OpenAI** — fornece modelos que o endpoint compatível da sua organização expõe.
- **Anthropic** — fornece modelos para integração direta com o Anthropic.

Os modelos que você vê podem variar de acordo com a configuração do endpoint, o comportamento do proxy ou gateway e a política organizacional. Os tipos de provedor diferem pelo endpoint ao qual você se conecta e pelos modelos que esse endpoint expõe, não pelo protocolo de transporte.

Modelos OpenAI suportados

- GPT-5.4
- GPT-5.5

Modelos Anthropic suportados

- Claude Sonnet 4.6
- Claude Opus 4.6, 4.7 e 4.8

Informações relacionadas

- "Conecte seu LLM e ative o assistente do NetApp Console".
- "Saiba mais sobre a integração do LLM na implantação local do NetApp Console".

Referência de alertas do ONTAP na implantação local do NetApp Console

Esta referência lista os alertas do ONTAP que a implantação local do NetApp Console pode monitorar, organizados por categoria de impacto.

Mapeamento de gravidade

O mesmo alerta do EMS pode aparecer como Crítico, Aviso ou Informação, dependendo do evento do ONTAP que o causou:

- **Crítico**: Mapas das gravidades do ONTAP `alert`, `emergency`
- **Aviso**: Mapas da gravidade do ONTAP `error`
- **Informação**: Mapas das gravidades do ONTAP `notice`, `informational`
- **Outros**: Passado como está

O mapeamento dinâmico permite que uma única regra de alerta emita diferentes níveis de severidade dependendo do contexto de execução do evento do EMS.

As seções abaixo agrupam os alertas por categoria de impacto e classificam cada tabela em ordem alfabética pelo nome do alerta.

Alertas de disponibilidade

Esses alertas podem afetar a disponibilidade do sistema, do serviço ou a disponibilidade de dados.

Nome do alerta	Gravidade	Tipo	Descrição
Conexão com o servidor Active Directory inativa	Crítico	EMS	Todos os servidores AD/LDAP configurados para esta SVM estão inacessíveis.
O Aggregate não está online	Crítico	Métrica	Alguns agregados estão offline. A criação de volumes pode causar FSIDs duplicados.
Servidor antivírus ocupado	Crítico, Aviso, Informação	EMS	O servidor antivírus está sobrecarregado e não pode aceitar solicitações de verificação adicionais.
Credenciais da AWS não inicializadas	Crítico, Aviso, Informação	EMS	Um módulo tentou acessar credenciais baseadas em funções do AWS IAM antes que elas fossem inicializadas.
Nível de nuvem inacessível	Crítico, Aviso, Informação	EMS	Um nó de storage não consegue se conectar à API de armazenamento de objetos do Cloud Tier. Alguns dados ficarão inacessíveis.
Falha no disco	Crítico	Métrica	Um disco apresentou falha, está sendo sanitizado ou está em modo de manutenção.
Disco fora de serviço	Crítico, Aviso, Informação	EMS	Um disco foi retirado de serviço devido a falha, sanitização ou manutenção.
Fonte de alimentação do shelf de disco removida	Crítico, Aviso, Informação	EMS	Uma fonte de alimentação foi removida da gaveta de discos.
Comandos da porta de destino FC excedidos	Crítico, Aviso, Informação	EMS	O número de comandos pendentes na porta de destino FC física excede o limite suportado.
Falha no giveback do pool de storage	Crítico, Aviso, Informação	EMS	Este evento ocorre durante a realocação de um pool de storage (agregado) como parte de um giveback de storage failover (SFO), quando o nó de destino não consegue alcançar os armazenamentos de objetos.
Interconexão HA desativada	Crítico, Aviso, Informação	EMS	A interconexão HA está inativa. Risco de interrupção de serviço quando o failover não está disponível.
InstanceDown	Crítico	Métrica	A instância monitorada está inacessível e pode estar inativa ou apresentando problemas de rede.

Nome do alerta	Gravidade	Tipo	Descrição
LUN destruído	Crítico, Aviso, Informação	EMS	Um LUN foi destruído e não está mais acessível.
LUN off-line	Crítico, Aviso, Informação	EMS	Um LUN foi desativado manualmente.
A ventoinha da unidade principal falhou	Crítico, Aviso, Informação	EMS	Uma ou mais ventoinhas da unidade principal falharam. O sistema permanece operacional.
Ventilador da unidade principal em estado de alerta	Crítico, Aviso, Informação	EMS	Uma ou mais ventoinhas de refrigeração da unidade principal estão em estado de alerta.
Número máximo de sessões por usuário excedido	Crítico, Aviso, Informação	EMS	Você excedeu o número máximo de sessões permitidas por usuário em uma conexão TCP.
Número máximo de vezes que um arquivo pode ficar aberto foi excedido	Crítico, Aviso, Informação	EMS	Você excedeu o número máximo de vezes que pode abrir o arquivo por meio de uma conexão TCP.
MetroCluster switchover automática não planejada desativada	Crítico, Aviso, Informação	EMS	A capacidade de switchover automática não planejada foi desativada neste cluster.
MetroCluster monitoramento	Crítico, Aviso, Informação	EMS	O alerta do monitor de integridade do sistema foi detectado.
Pool de storage NFSv4 esgotado	Crítico, Aviso, Informação	EMS	Um pool de storage NFSv4 foi esgotado.
Conflito de nome NetBIOS	Crítico, Aviso, Informação	EMS	O serviço de nomes NetBIOS recebeu uma resposta negativa a uma solicitação de registro de nome, proveniente de uma máquina remota.
Nenhum mecanismo de digitalização registrado	Crítico, Aviso, Informação	EMS	O conector de antivírus notificou o ONTAP de que não possui um mecanismo de varredura registrado.
Sem conexão Vscan	Crítico, Aviso, Informação	EMS	O ONTAP não possui conexão com o Vscan para atender às solicitações de verificação de vírus. Isso pode causar indisponibilidade de dados se a opção de verificação obrigatória estiver ativada.
Servidor antivírus não responsivo	Crítico, Aviso, Informação	EMS	O ONTAP detectou um servidor antivírus que não respondia e encerrou à força sua conexão com o Vscan.
Compartilhamento de administrador inexistente	Crítico, Aviso, Informação	EMS	Problema com o Vscan: um cliente tentou se conectar a um compartilhamento ONTAP_ADMIN$ inexistente.

Nome do alerta	Gravidade	Tipo	Descrição
Bateria NVRAM fraca	Crítico, Aviso, Informação	EMS	A capacidade da bateria da NVRAM está criticamente baixa. Pode haver perda de dados se a bateria se esgotar.
Namespace NVMe destruído	Crítico, Aviso, Informação	EMS	Um namespace NVMe foi destruído e não está mais acessível.
Namespace NVMe offline	Crítico, Aviso, Informação	EMS	Um namespace NVMe foi desativado manualmente.
Namespace NVMe online	Crítico, Aviso, Informação	EMS	Um namespace NVMe foi reativado.
Período de carência da licença NVMe-oF ativo	Crítico, Aviso, Informação	EMS	Esse evento ocorre diariamente quando o protocolo NVMe over Fabrics (NVMe-oF) está em uso e o período de carência da licença está ativo.
O período de carência da licença NVMe-oF expirou	Crítico, Aviso, Informação	EMS	O período de carência da licença NVMe over Fabrics (NVMe-oF) terminou e a funcionalidade NVMe-oF está desativada.
Início do período de carência da licença NVMe-oF	Crítico, Aviso, Informação	EMS	A configuração NVMe over Fabrics (NVMe-oF) foi detectada durante a atualização para o software ONTAP 9.5.
Host de armazenamento de objetos não resolvido	Crítico, Aviso, Informação	EMS	O nome do host do servidor de armazenamento de objetos não pode ser resolvido para um endereço IP.
Armazenamento de objetos LIF entre clusters inativo	Crítico, Aviso, Informação	EMS	O cliente de armazenamento de objetos não consegue encontrar uma LIF operacional para se comunicar com o servidor de armazenamento de objetos.
Incompatibilidade na assinatura do armazenamento de objetos	Crítico, Aviso, Informação	EMS	A assinatura da solicitação enviada ao servidor de armazenamento de objetos não corresponde à assinatura calculada pelo cliente.
Status da porta inativo	Crítico	EMS	Esta porta Ethernet está inativa. O tráfego nessa conexão pode ser afetado.
Tempo limite de READDIR	Crítico, Aviso, Informação	EMS	Uma operação de arquivo READDIR excedeu o tempo limite permitido para sua execução no WAFL.
A realocação do pool de storage falhou	Crítico, Aviso, Informação	EMS	Esse evento ocorre durante a realocação de um pool de storage (agregado), quando o nó de destino não consegue alcançar os armazenamentos de objetos.
O estado "ativo-ativo" da SAN foi alterado	Crítico, Aviso, Informação	EMS	O roteamento SAN não é mais simétrico.

Nome do alerta	Gravidade	Tipo	Descrição
Pulsação do Service Processor perdida	Crítico, Aviso, Informação	EMS	O ONTAP não está recebendo o sinal de pulsação esperado do Service Processor (SP).
O Service Processor parou de funcionar.	Crítico, Aviso, Informação	EMS	O ONTAP não está mais recebendo sinais de atividade do Service Processor (SP).
Processador de serviço não configurado	Crítico, Aviso, Informação	EMS	Este evento ocorre semanalmente para lembrar você de configurar o Service Processor (SP).
Service Processor offline	Crítico, Aviso, Informação	EMS	O Service Processor (SP) está offline.
SFP no adaptador de destino FC recebendo baixa potência	Crítico, Aviso, Informação	EMS	Este alerta ocorre quando a potência recebida (RX) por um transceptor plugável de pequeno formato (SFP em FC target) está em um nível abaixo do limite definido.
SFP em adaptador de destino FC transmitindo baixa potência	Crítico, Aviso, Informação	EMS	Este alerta ocorre quando a potência transmitida (TX) por um transceptor plugável de pequeno formato (SFP em FC target) está em um nível abaixo do limite definido.
A cópia de sombra falhou	Crítico, Aviso, Informação	EMS	Uma operação de backup e restauração do Serviço de Cópias de Sombra de Volume (VSS), um serviço de backup e restauração do Microsoft Server, falhou.
O ventilador de prateleira apresentou defeito	Crítico, Aviso, Informação	EMS	O ventilador ou módulo de ventilação indicado da prateleira apresentou defeito.
SnapMirror o tempo de atraso é alto	Crítico	Métrica	A relação do SnapMirror está com mais de uma hora de atraso em relação ao cronograma de atualização previsto.
Interconexão de failover de armazenamento um ou mais links inativos	Aviso	EMS	Um ou mais links de interconexão HA com o nó parceiro estão inativos. A redundância de failover está reduzida.
Falha nas fontes de alimentação do switch de storage	Crítico, Aviso, Informação	EMS	Há uma fonte de alimentação ausente no switch de cluster. A redundância está reduzida.
A parada da VM de armazenamento foi concluída com êxito	Crítico, Aviso, Informação	EMS	A máquina virtual de armazenamento foi interrompida com sucesso.
Licença de replicação de configuração SVM inválida	Aviso	EMS	A licença de replicação de configuração do SVM-DR está ausente, expirada ou não aplicada

Nome do alerta	Gravidade	Tipo	Descrição
O sistema não pode funcionar devido a uma falha na ventoinha da unidade principal	Crítico, Aviso, Informação	EMS	Uma ou mais ventoinhas da unidade principal falharam, interrompendo o funcionamento do sistema. Isso pode levar a uma potencial perda de dados.
Muitas autenticações CIFS	Crítico, Aviso, Informação	EMS	Muitas negociações de autenticação ocorreram simultaneamente. Há 256 solicitações incompletas de novas sessões deste cliente.
Discos não atribuídos	Crítico, Aviso, Informação	EMS	O sistema possui discos não atribuídos; a capacidade está sendo desperdiçada.
Estado do volume offline	Informativo	Métrica	O volume foi colocado offline.
Volume restrito	Crítico, Aviso, Informação	EMS	Este evento indica que um volume flexível foi restringido.
Vírus detectado	Crítico, Aviso, Informação	EMS	Um servidor Vscan relatou que um arquivo pode estar infectado com um vírus.

Alertas de capacidade

Esses alertas indicam consumo de armazenamento ou pressão de capacidade.

Nome do alerta	Gravidade	Tipo	Descrição
FabricPool a resincronização da replicação do espelho foi concluída	Crítico, Aviso, Informação	EMS	O processo de ressincronização do espelhamento do FabricPool foi concluído com sucesso do armazenamento de objetos primário para o armazenamento de objetos de espelho.
O limite de uso de espaço do FabricPool está quase no fim	Crítico, Aviso, Informação	EMS	O uso total de espaço do FabricPool em armazenamento de objetos em todo o cluster, proveniente de provedores com licenças de capacidade, está quase atingindo o limite da licença.
FabricPool limite de utilização do espaço atingido	Crítico, Aviso, Informação	EMS	O uso total de espaço do FabricPool em armazenamento de objetos em todo o cluster, proveniente de provedores com licenças de capacidade, atingiu o limite da licença.
Espaço do volume raiz do nó baixo	Crítico, Aviso, Informação	EMS	O sistema detectou que o volume raiz está perigosamente baixo em espaço.
Memória do monitor de QoS no limite	Crítico, Aviso, Informação	EMS	A memória dinâmica do subsistema QoS atingiu seu limite para o hardware da plataforma atual.

Nome do alerta	Gravidade	Tipo	Descrição
Redimensionamento automático de volume concluído com sucesso	Crítico, Aviso, Informação	EMS	O volume foi redimensionado automaticamente porque o crescimento automático de volume está ativado.
Volume cheio	Crítico	Métrica	O volume está mais de 90% cheio. Libere espaço ou adicione capacidade para evitar falhas de gravação.

Alertas de configuração

Esses alertas indicam alterações de configuração ou atualizações de inventário.

Nome do alerta	Gravidade	Tipo	Descrição
Fonte de alimentação do shelf de disco descoberta	Crítico, Aviso, Informação	EMS	Uma fonte de alimentação foi adicionada à gaveta de discos.
Volume criado	Informação	Métrica	Um volume foi criado.
Volume excluído	Aviso	Métrica	Um volume foi excluído.
Volume modificado	Informação	Métrica	Um volume foi modificado.
Verificação de consistência WAFL vencida	Aviso	EMS	As verificações de consistência do WAFL neste agregado excederam o limite horário.

Alertas de desempenho

Esses alertas indicam problemas de latência ou de desempenho do nó.

Nome do alerta	Gravidade	Tipo	Descrição
A latência do NFS do nó está alta	Crítico	Métrica	As operações NFS neste nó estão apresentando alta latência (>5000 us).
Pânico no nó	Crítico, Aviso, Informação	EMS	O nó entrou em pânico e foi reiniciado.

Alertas de proteção

Esses alertas afetam a replicação, o failover ou a recuperação.

Nome do alerta	Gravidade	Tipo	Descrição
O snapshot comum da relação de fanout do SnapMirror foi excluído	Crítico, Aviso, Informação	EMS	Uma cópia Snapshot mais antiga é excluída como parte de uma operação de ressincronização ou atualização síncrona do SnapMirror.
ONTAP Mediator adicionado	Crítico, Aviso, Informação	EMS	O ONTAP Mediator foi adicionado com sucesso a este cluster.

Nome do alerta	Gravidade	Tipo	Descrição
O certificado CA do mediador ONTAP expirou	Crítico, Aviso, Informação	EMS	O certificado da autoridade certificadora (CA) do ONTAP Mediator expirou.
Certificado CA do ONTAP Mediator expirando	Crítico, Aviso, Informação	EMS	O certificado da autoridade certificadora (CA) do ONTAP Mediator expirará nos próximos 30 dias.
Certificado de cliente do ONTAP Mediator expirado	Crítico, Aviso, Informação	EMS	O certificado de cliente do ONTAP Mediator expirou.
Certificado de cliente do ONTAP Mediator expirando	Crítico, Aviso, Informação	EMS	O certificado de cliente do ONTAP Mediator está prestes a expirar nos próximos 30 dias.
O ONTAP Mediator não está acessível	Crítico, Aviso, Informação	EMS	O ONTAP Mediator não está acessível, seja porque foi reaproveitado ou porque o pacote do Mediator não está mais instalado.
ONTAP Mediator removido	Crítico, Aviso, Informação	EMS	O ONTAP Mediator foi removido com sucesso deste cluster.
ONTAP Mediator inacessível	Crítico, Aviso, Informação	EMS	O ONTAP Mediator está inacessível, o que significa que o SnapMirror failover não é possível até que a conectividade seja restaurada.
O certificado do servidor ONTAP Mediator expirou	Crítico, Aviso, Informação	EMS	O certificado do servidor ONTAP Mediator expirou.
Certificado do servidor ONTAP Mediator expirando	Crítico, Aviso, Informação	EMS	O certificado do servidor ONTAP Mediator expirará nos próximos 30 dias.
SnapMirror relação de sincronização ativa fora de sincronia	Crítico, Aviso, Informação	EMS	A relação síncrona do SnapMirror passou de sincronizada para dessincronizada. A proteção de dados é afetada.
SnapMirror active sync failover automático não planejado concluído	Crítico, Aviso, Informação	EMS	A operação automática de failover não planejado do SnapMirror Business Continuity (SMBC) foi concluída.
SnapMirror active sync falha na transição automática não planejada	Crítico, Aviso, Informação	EMS	A operação automática de failover não planejada do SnapMirror Business Continuity (SMBC) falhou.
SnapMirror a sincronização ativa com failover planejado foi concluída	Crítico, Aviso, Informação	EMS	A operação de failover planejada do SnapMirror Business Continuity (SMBC) foi concluída.
SnapMirror active sync com failover planejado falhou	Crítico, Aviso, Informação	EMS	A operação de failover planejada do SnapMirror Business Continuity (SMBC) falhou.

Nome do alerta	Gravidade	Tipo	Descrição
SnapMirror falha na cópia Snapshot comum da relação do SnapMirror	Crítico, Aviso, Informação	EMS	Há uma falha na criação de uma cópia Snapshot comum.
SnapMirror relação do SnapMirror falhou na inicialização	Crítico, Aviso, Informação	EMS	O comando de inicialização do SnapMirror falhou e nenhuma outra tentativa será feita.
SnapMirror relação fora de sincronia	Crítico, Aviso, Informação	EMS	A relação síncrona do SnapMirror passou de sincronizada para dessincronizada. A proteção de dados é afetada.
SnapMirror A tentativa de ressincronização da relação do SnapMirror falhou	Crítico, Aviso, Informação	EMS	A SnapMirror tentativa de sincronização entre os volumes de origem e destino falhou.
A cópia Snapshot da relação do SnapMirror não foi replicada	Crítico, Aviso, Informação	EMS	A cópia Snapshot da relação do SnapMirror Synchronous não foi replicada com sucesso.

Alertas de segurança

Esses alertas indicam ameaças ou acessos não autorizados.

Nome do alerta	Gravidade	Tipo	Descrição
Atividade de ransomware detectada	Crítico, Aviso, Informação	EMS	Para proteger os dados contra o ransomware detectado, uma cópia Snapshot foi criada e pode ser usada para restaurar os dados originais.
Monitoramento anti-ransomware de Storage VM	Crítico, Aviso, Informação	EMS	O estado de proteção contra ransomware da Storage VM foi alterado.
Acesso não autorizado do usuário ao compartilhamento administrativo	Crítico, Aviso, Informação	EMS	Um cliente tentou se conectar ao compartilhamento privilegiado ONTAP_ADMIN$, mas o usuário conectado não faz parte de nenhum pool de scanners Vscan ativo nesta SVM.
Monitoramento de volume anti-ransomware	Crítico, Aviso, Informação	EMS	O estado de proteção contra ransomware de um volume foi alterado.

Categorias de conformidade de segurança de cluster na implantação local do NetApp Console

Use esta referência para analisar as categorias de conformidade de segurança do cluster exibidas na implantação local do NetApp Console, incluindo o valor recomendado e se cada categoria afeta o status geral de conformidade.

Essas categorias são baseadas nas verificações de postura de segurança do ONTAP.

Categoria	O que a categoria verifica	Valor recomendado	Afeta a conformidade geral
FIPS global	Indica se o modo FIPS 140-2 está ativado. Quando ativado, TLSv1 e SSLv3 são desativados e apenas TLSv1.1 e TLSv1.2 são permitidos.	Habilitado	Sim
Telnet	Se o acesso Telnet está habilitado. O SSH é o método de acesso remoto seguro recomendado.	Desabilitado	Sim
Configurações SSH inseguras	Se o SSH estiver configurado com cifras inseguras, como cifras que começam com `cbc`.	Não	Sim
Banner de login	Indica se um banner de login está configurado para acesso ao sistema.	Habilitado	Sim
Peer de cluster	Indica se a comunicação entre clusters emparelhados é criptografada. A criptografia deve estar habilitada tanto no cluster de origem quanto no de destino.	Criptografado	Sim
Protocolo de Tempo de Rede	Se um ou mais servidores NTP estão configurados para o cluster. NetApp recomenda pelo menos três servidores NTP para maior resiliência.	Configurado	Sim
OCSP	Indica se a validação do Online Certificate Status Protocol está habilitada para validação de certificados SSL/TLS.	Habilitado	Não
Registro de auditoria remota	Se o encaminhamento de logs (syslog) é criptografado.	Criptografado	Sim
AutoSupport transporte HTTPS	Indica se o HTTPS é usado como protocolo de transporte padrão para AutoSupport mensagens.	Habilitado	Sim
Usuário administrador padrão	Indica se a conta de administrador padrão incorporada está desativada.	Desabilitado	Sim
Usuários SAML	Se o SAML está configurado para single sign-on e autenticação compatível com MFA.	Não	Não
Usuários do Active Directory	Se a autenticação do Active Directory está configurada para acesso ao cluster.	Não	Não
Usuários LDAP	Se a autenticação LDAP está configurada para acesso ao cluster.	Não	Não
Usuários de certificado	Se os usuários baseados em certificado estão configurados para login no cluster.	Não	Não
Usuários locais	Se os usuários locais estão configurados para login no cluster.	Não	Não
Shell remoto	Se o RSH está habilitado. O SSH é preferido para acesso remoto seguro.	Desabilitado	Sim

Categoria	O que a categoria verifica	Valor recomendado	Afeta a conformidade geral
MD5 em uso	Se as contas de usuário do ONTAP ainda utilizam hash MD5 em vez de hashes mais robustos, como SHA-512.	Não	Sim
Tipo de emissor de certificado	O tipo de emissor de certificado usado pelo cluster.	Assinado pela CA	Não

Categorias de conformidade de segurança de VMs de armazenamento na implantação local do NetApp Console

Use esta referência para analisar as categorias de conformidade de segurança da máquina virtual de armazenamento (SVM) exibidas na implantação local do NetApp Console, incluindo o valor recomendado e se cada categoria afeta o status geral de conformidade.

Essas categorias são baseadas nas verificações de postura de segurança do ONTAP.

Categoria	O que a categoria verifica	Valor recomendado	Afeta a conformidade geral
Registro de auditoria	Indica se o registro de auditoria do SVM está ativado.	Habilitado	Sim
Configurações SSH inseguras	Se o SSH estiver configurado com cifras inseguras, como cifras que começam com `cbc`.	Não	Sim
Banner de login	Indica se um banner de login está configurado para usuários que acessam as SVMs.	Habilitado	Sim
LDAP criptografia	Se a criptografia LDAP está ativada.	Habilitado	Não
Autenticação NTLM	Indica se a autenticação NTLM está ativada.	Habilitado	Não
Assinatura de carga LDAP	Indica se a assinatura de carga LDAP está habilitada.	Habilitado	Não
Configurações de CHAP	Indica se o CHAP está ativado.	Habilitado	Não
Kerberos V5	Indica se a autenticação Kerberos V5 está ativada.	Habilitado	Não
Autenticação NIS	Se a autenticação NIS está configurada.	Desabilitado	Não
Status do FPolicy: ativo	Se a FPolicy foi criada e está ativa.	Sim	Não
Criptografia SMB ativada	Se a assinatura e a selagem SMB estão ativadas.	Sim	Não
Assinatura SMB ativada	Se a assinatura SMB está ativada.	Sim	Não

Conhecimento e suporte

Registre-se para obter suporte na implantação local do NetApp Console

NetApp Console informações sobre a implantação local para esta tarefa. O registro de suporte é necessário para receber suporte técnico específico para o NetApp Console e suas soluções de storage e serviços de dados. O registro de suporte também é necessário para habilitar fluxos de trabalho essenciais para os sistemas Cloud Volumes ONTAP.

O cadastro para suporte não habilita o suporte da NetApp para um serviço de arquivos do provedor de nuvem. Para suporte técnico relacionado a um serviço de arquivos do provedor de nuvem, sua infraestrutura ou qualquer solução que utilize o serviço, consulte "Obtendo ajuda" na documentação desse produto.

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Visão geral do registro de suporte

Existem duas formas de registro para ativar o direito ao suporte:

- Registrando o número de série da sua conta do NetApp Console (seu número de série de 20 dígitos 960xxxxxxxxx localizado na página de Recursos de Suporte no Console).

  Este ID serve como sua única identificação de assinatura de suporte para qualquer serviço dentro do Console. Cada conta do Console deve ser registrada.

- Registrar os números de série do Cloud Volumes ONTAP associados a uma assinatura no marketplace do seu provedor de nuvem (esses são números de série de 20 dígitos 909201xxxxxxxx).

  Esses números de série são comumente chamados de *números de série PAYGO* e são gerados pelo NetApp Console no momento da implantação do Cloud Volumes ONTAP.

O registro de ambos os tipos de números de série habilita funcionalidades como a abertura de chamados de suporte e a geração automática de casos. O registro é concluído ao adicionar contas do NetApp Support Site (NSS) ao Console, conforme descrito abaixo.

Registre o Console NetApp para suporte da NetApp

Para se cadastrar no suporte e ativar o direito ao suporte, um usuário na sua conta do NetApp Console deve associar uma conta do NetApp Support Site ao login do Console. Como você se cadastra no suporte da NetApp depende de já ter ou não uma conta do NetApp Support Site (NSS).

Cliente existente com conta NSS

Se você for um NetApp cliente com uma conta NSS, basta se cadastrar para receber suporte através do Console.

Passos

1. Selecione **Administração** > **Credenciais**.

2. Selecione **Credenciais do Usuário**.
3. Selecione **Adicionar credenciais NSS** e siga o prompt de autenticação do site de suporte da NetApp (NSS).
4. Para confirmar se o processo de registro foi bem-sucedido, selecione o ícone Ajuda e selecione **Suporte**.

   A página **Recursos** deve mostrar que sua conta do Console está registrada para suporte.

   Observe que outros usuários do Console não verão o mesmo status de registro de suporte se não tiverem associado uma conta do NetApp Support Site ao seu login. No entanto, isso não significa que sua conta não esteja registrada para suporte. Contanto que um usuário da organização tenha seguido estas etapas, sua conta estará registrada.

Cliente existente, mas sem conta NSS

Se você já é cliente NetApp e possui licenças e números de série existentes, mas não tem uma conta NSS, você precisa criar uma conta NSS e associá-la ao seu login do Console.

Passos

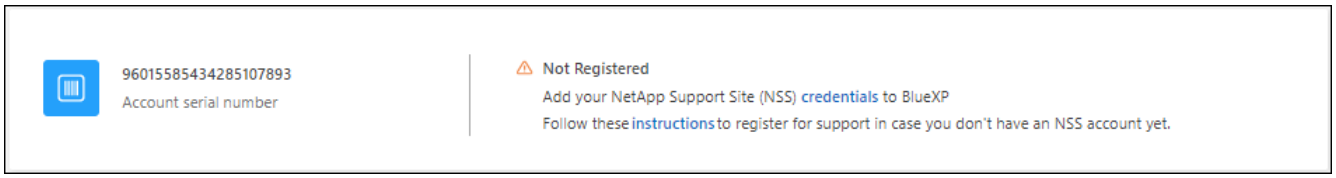
1. Crie uma conta no site de suporte da NetApp preenchendo o "NetApp Formulário de registro de usuário do site de suporte"
   a. Certifique-se de selecionar o Nível de Usuário apropriado, que normalmente é **NetApp Customer/End User**.
   b. Certifique-se de copiar o número de série da conta do Console (960xxxx) usado acima para o campo de número de série. Isso agilizará o processamento da conta.
2. Associe sua nova conta NSS ao seu login do Console concluindo as etapas em Cliente existente com conta NSS.

Totalmente novo na NetApp

Se você é completamente novo na NetApp e não possui uma conta NSS, siga cada passo abaixo.

Passos

1. No canto superior direito do Console, selecione o ícone de Ajuda e selecione **Suporte**.
2. Localize o número de série do seu ID de conta na página de Support Registration.



3. Navegue até "NetApp's site de registro de suporte" e selecione **Não sou um cliente NetApp registrado**.
4. Preencha os campos obrigatórios (aqueles com asteriscos vermelhos).
5. No campo **Linha de Produtos**, selecione **Cloud Manager** e, em seguida, selecione seu provedor de faturamento aplicável.
6. Copie o número de série da sua conta da etapa 2 acima, conclua a verificação de segurança e confirme que leu a Política Global de Privacidade de Dados da NetApp.

   Um e-mail é enviado imediatamente para a caixa de entrada fornecida para finalizar esta transação segura. Certifique-se de verificar suas pastas de spam caso o e-mail de validação não chegue em poucos

minutos.

7. Confirme a ação diretamente no e-mail.

   Ao confirmar, você envia sua solicitação para a NetApp e recomenda-se que você crie uma conta no site de suporte da NetApp.

8. Crie uma conta no site de suporte da NetApp preenchendo o "NetApp Formulário de registro de usuário do site de suporte"
   a. Certifique-se de selecionar o Nível de Usuário apropriado, que normalmente é **NetApp Customer/End User**.
   b. Certifique-se de copiar o número de série da conta (960xxxx) usado acima para o campo de número de série. Isso agilizará o processamento.

Depois que você terminar

NetApp deve entrar em contato com você durante este processo. Este é um exercício de integração único para novos usuários.

Depois que você tiver sua conta no site de suporte da NetApp, associe a conta ao seu login no Console seguindo as etapas em Cliente existente com conta NSS.

Associar credenciais NSS para suporte ao Cloud Volumes ONTAP

Associar as credenciais do site de suporte da NetApp à sua conta do Console é necessário para habilitar os seguintes fluxos de trabalho principais para o Cloud Volumes ONTAP:

- Registrando sistemas Cloud Volumes ONTAP com pagamento conforme o uso para suporte

  É necessário fornecer sua conta NSS para ativar o suporte ao seu sistema e obter acesso aos recursos de suporte técnico da NetApp.

- Implantando Cloud Volumes ONTAP quando você traz sua própria licença (BYOL)

  É necessário fornecer sua conta NSS para que o Console possa carregar sua chave da licença e ativar a assinatura pelo período adquirido. Isso inclui atualizações automáticas para renovações de período.

- Atualizando o software Cloud Volumes ONTAP para a versão mais recente

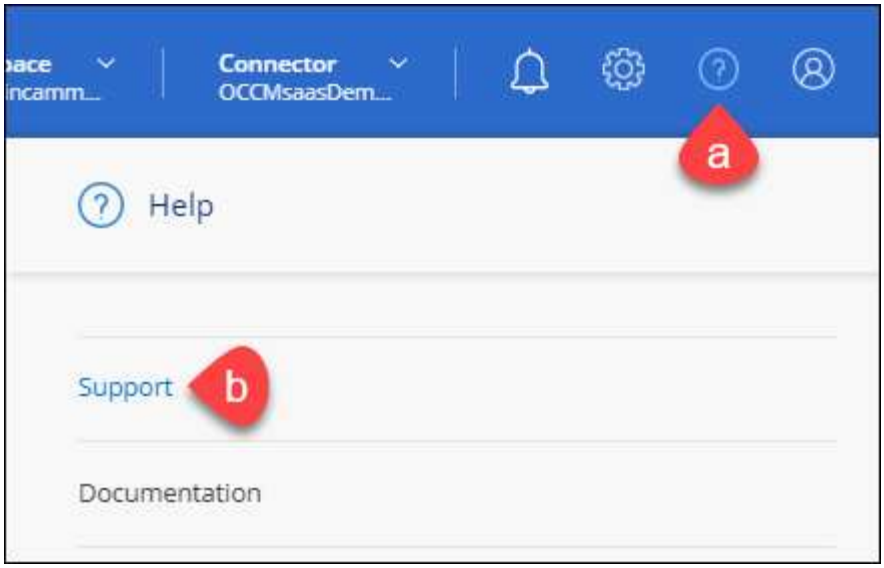
Associar as credenciais do NSS à sua conta do NetApp Console é diferente da conta do NSS associada ao login de um usuário do Console.

Essas credenciais do NSS estão associadas ao seu ID de conta específico do Console. Usuários que pertencem à organização do Console podem acessar essas credenciais em **Suporte > Gerenciamento do NSS**.

- Se você possui uma conta de cliente, pode adicionar uma ou mais contas NSS.
- Se você possui uma conta de parceiro ou revendedor, pode adicionar uma ou mais contas NSS, mas elas não podem ser adicionadas juntamente com contas de nível de cliente.

Passos

1. No canto superior direito do Console, selecione o ícone de Ajuda e selecione **Suporte**.



2. Selecione **NSS Management > Adicionar NSS Account**.
3. Quando solicitado, selecione **Continuar** para ser redirecionado para uma página de login da Microsoft.

   NetApp usa o Microsoft Entra ID como provedor de identidade para serviços de autenticação específicos de suporte e licenciamento.

4. Na página de login, forneça seu endereço de e-mail registrado no site de suporte da NetApp e sua senha para realizar o processo de autenticação.

   Essas ações permitem que o Console utilize sua conta NSS para atividades como downloads de licença, verificação de atualização de software e registros de suporte futuro.

   Observe o seguinte:

   - A conta NSS deve ser uma conta de cliente (não uma conta de convidado ou temporária). Você pode ter várias contas NSS de cliente.
   - Só pode haver uma conta NSS se essa conta for de nível de parceiro. Se você tentar adicionar contas NSS de nível de cliente e já existir uma conta de nível de parceiro, você receberá a seguinte mensagem de erro:

     "O tipo de cliente NSS não é permitido para esta conta, pois já existem usuários NSS de tipo diferente."

   O mesmo se aplica se você já tiver contas NSS de nível de cliente e tentar adicionar uma conta de nível de parceiro.

   - Após o login bem-sucedido, NetApp armazenará o nome de usuário do NSS.

     Este é um ID gerado pelo sistema que corresponde ao seu e-mail. Na página **Gerenciamento de NSS**, você pode visualizar seu e-mail no ••• menu.

   - Se você precisar atualizar seus tokens de credencial de login, também há a opção **Atualizar Credenciais** no ••• menu.

     Ao usar esta opção, você será solicitado a fazer login novamente. Observe que o token dessas contas expira após 90 dias. Uma notificação será exibida para alertar você sobre isso.

Obtenha ajuda com a implantação local do NetApp Console

Informações sobre a implantação local do NetApp Console para esta tarefa. A NetApp oferece suporte para o NetApp Console e seus serviços em nuvem de diversas maneiras. Opções extensas e gratuitas de autoatendimento estão disponíveis 24 horas por dia, 7 dias por semana, como artigos da base de conhecimento (KB) e um fórum da comunidade. Seu registro de suporte inclui suporte técnico remoto por meio de sistema de tickets online.

Obtenha suporte para um serviço de arquivos de provedor de nuvem

Para suporte técnico relacionado a um serviço de arquivos de um provedor de nuvem, sua infraestrutura ou qualquer solução que utilize o serviço, consulte a documentação do produto.

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Para receber suporte técnico específico para NetApp e suas soluções de armazenamento e serviços de dados, utilize as opções de suporte descritas abaixo.

Utilize opções de autoatendimento

Essas opções estão disponíveis gratuitamente, 24 horas por dia, 7 dias por semana:

- Documentação

  A documentação do NetApp Console que você está visualizando no momento.

- "Base de conhecimento"

  Pesquise na base de conhecimento da NetApp para encontrar artigos úteis que o ajudarão a solucionar problemas.

- "Comunidades"

  Participe da comunidade NetApp Console para acompanhar discussões em andamento ou criar novas.

Crie um caso com o suporte da NetApp

Além das opções de autoatendimento acima, você pode trabalhar com um especialista de suporte da NetApp para resolver quaisquer problemas após ativar o suporte.

Antes de começar

- Para usar a funcionalidade **Criar um Caso**, primeiro você precisa associar suas credenciais do NetApp Support Site ao seu login do Console. "Aprenda a gerenciar as credenciais associadas ao seu login no Console"
- Se você estiver abrindo um chamado para um sistema ONTAP que possui um número de série, sua conta NSS deve estar associada ao número de série desse sistema.

Passos

1. No NetApp Console, selecione **Ajuda > Suporte**.
2. Na página **Recursos**, escolha uma das opções disponíveis em suporte técnico:

   a. Selecione **Ligue para nós** se você quiser falar com alguém por telefone. Você será direcionado para uma página no netapp.com/br/ que lista os números de telefone para os quais você pode ligar.

   b. Selecione **Criar um caso** para abrir um chamado com um especialista de suporte da NetApp:

      - **Serviço**: Selecione o serviço ao qual o problema está associado. Por exemplo, **NetApp Console** quando se tratar de um problema específico de suporte técnico relacionado a fluxos de trabalho ou funcionalidades do Console.
      - **Sistema**: Se aplicável ao armazenamento, selecione **Cloud Volumes ONTAP** ou **On-Prem** e, em seguida, o ambiente de trabalho associado.

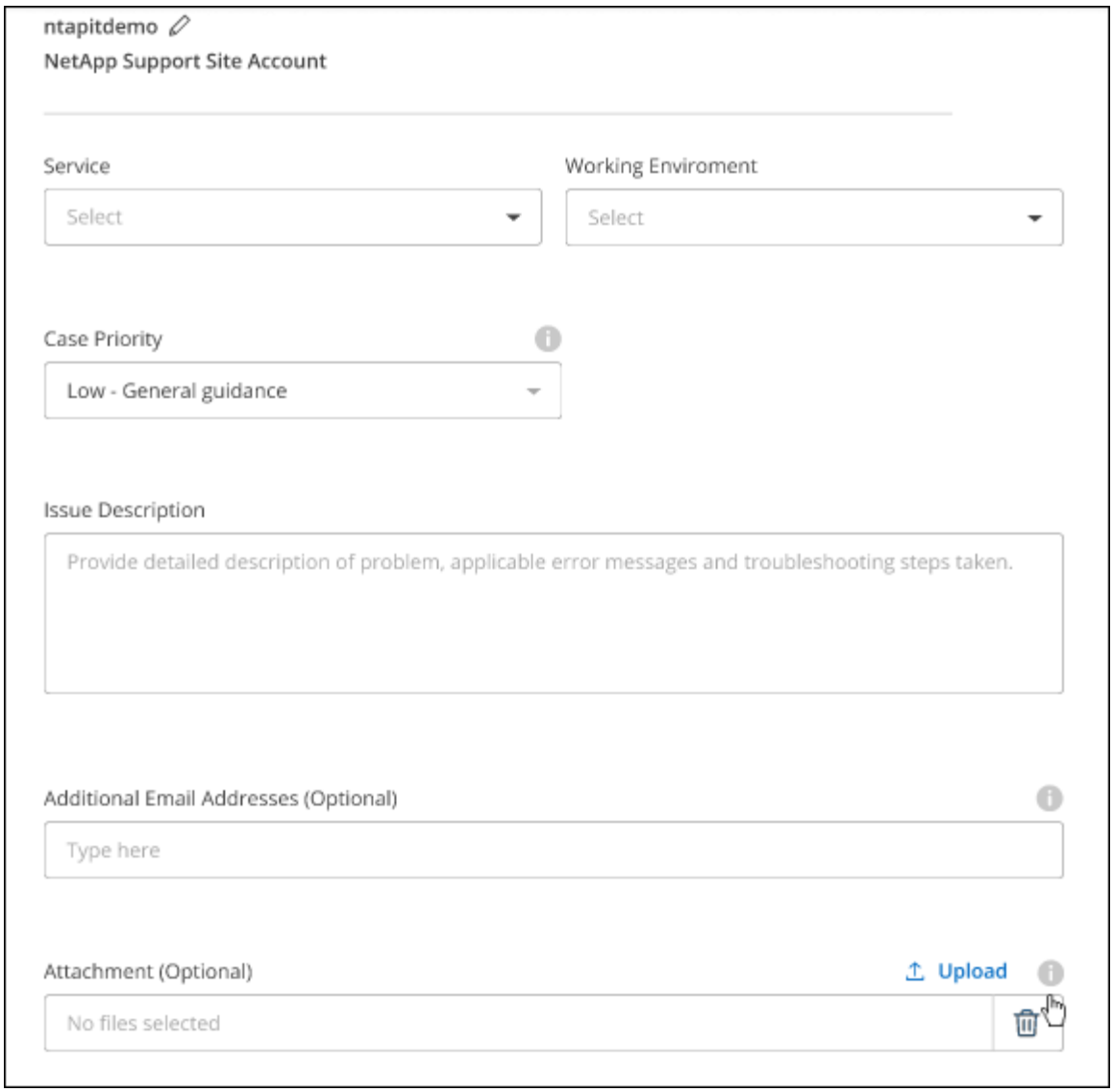
        A lista de sistemas está dentro do escopo da organização do Console e do agente do Console que você selecionou no banner superior.

      - **Prioridade do caso**: escolha a prioridade do caso, que pode ser Baixa, Média, Alta ou Crítica.

        Para obter mais detalhes sobre essas prioridades, passe o cursor do mouse sobre o ícone de informações ao lado do nome do campo.

      - **Descrição do problema**: Forneça uma descrição detalhada do seu problema, incluindo quaisquer mensagens de erro aplicáveis ou etapas de solução de problemas que você executou.
      - **Endereços de e-mail adicionais**: Insira endereços de e-mail adicionais se você quiser informar outras pessoas sobre este problema.
      - **Anexo (Opcional)**: Faça o upload de até cinco anexos, um de cada vez.

        Os anexos estão limitados a 25 MB por arquivo. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.



Depois que você terminar

Uma janela pop-up aparecerá com o número do seu caso de suporte. Um especialista de suporte da NetApp analisará seu caso e entrará em contato com você em breve.

Para consultar o histórico dos seus chamados de suporte, você pode selecionar **Configurações > Linha do tempo** e procurar por ações com o nome "criar chamado de suporte". Um botão no canto direito permite que você expanda a ação para ver os detalhes.

É possível que você encontre a seguinte mensagem de erro ao tentar criar um caso:

Você não tem autorização para criar um caso contra o serviço selecionado.

Esse erro pode significar que a conta NSS e a empresa registrada a ela associada não são as mesmas empresas registradas para o número de série da conta do NetApp Console (ou seja, 960xxxx) ou para o número de série do ambiente de trabalho. Você pode buscar ajuda usando uma das seguintes opções:

- Envie um caso não técnico em https://mysupport.netapp.com/site/help

Gerencie seus casos de suporte

Você pode visualizar e gerenciar casos de suporte ativos e resolvidos diretamente do Console. Você pode gerenciar os casos associados à sua conta NSS e à sua empresa.

Observe o seguinte:

- O painel de gestão de casos, localizado na parte superior da página, oferece duas visualizações:
  - A visualização à esquerda mostra o total de casos abertos nos últimos 3 meses pela conta de usuário NSS que você forneceu.
  - A visualização à direita mostra o total de casos abertos nos últimos 3 meses no nível da sua empresa com base na sua conta de usuário NSS.

  Os resultados na tabela refletem os casos relacionados à visualização que você selecionou.
- Você pode adicionar ou remover colunas de seu interesse e filtrar o conteúdo de colunas como Prioridade e Status. Outras colunas oferecem apenas opções de classificação.

  Veja os passos abaixo para mais detalhes.
- Em nível de caso individual, oferecemos a possibilidade de atualizar as anotações do caso ou encerrar um caso que ainda não esteja com o status "Encerrado" ou "Pendente de Encerramento".

Passos

1. No NetApp Console, selecione **Ajuda > Suporte**.
2. Selecione **Gestão de Casos** e, se solicitado, adicione sua conta NSS ao Console.

   A página **Gerenciamento de casos** exibe os casos abertos relacionados à conta NSS associada à sua conta de usuário do Console. Essa é a mesma conta NSS que aparece na parte superior da página **Gerenciamento de NSS**.
3. Opcionalmente, modifique as informações exibidas na tabela:
   - Em **Casos da organização**, selecione **Visualizar** para ver todos os casos associados à sua empresa.
   - Modifique o intervalo de datas escolhendo um intervalo exato de datas ou escolhendo um período diferente.
   - Filtre o conteúdo das colunas.
   - Altere as colunas que aparecem na tabela selecionando e escolhendo as colunas que deseja exibir.
4. Gerencie um caso existente selecionando e selecionando uma das opções disponíveis:
   - **Ver caso**: Veja todos os detalhes sobre um caso específico.
   - **Atualizar notas do caso**: Forneça detalhes adicionais sobre seu problema ou selecione **Carregar arquivos** para anexar até no máximo cinco arquivos.

     Os anexos estão limitados a 25 MB por arquivo. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.
   - **Fechar caso**: Forneça detalhes sobre por que você está fechando o caso e selecione **Fechar caso**.

Avisos legais para NetApp Console implantação local

NetApp Console documentação de implantação local para esta página.

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e mais.

Direitos autorais

"https://www.netapp.com/company/legal/copyright/"

Marcas registradas

NETAPP, o logotipo da NETAPP e as marcas listadas na página de Marcas Registradas da NetApp são marcas registradas da NetApp, Inc. Outros nomes de empresas e produtos podem ser marcas registradas de seus respectivos proprietários.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

A lista atual de patentes detidas pela NetApp pode ser encontrada em:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidade

"https://www.netapp.com/company/legal/privacy-policy/"

Código aberto

Os arquivos de notificação fornecem informações sobre direitos autorais e licenças de terceiro usados no software NetApp.

"Aviso para o NetApp Console".

Informações sobre direitos autorais

Informações sobre marcas comerciais