



Monitorar e relatar

SnapCenter Plug-in for VMware vSphere

NetApp

December 09, 2025

This PDF was generated from https://docs.netapp.com/pt-br/sc-plugin-vmware-vsphere-61/scpivs44_view_status_information.html on December 09, 2025. Always check docs.netapp.com for the latest.

Índice

Monitorar e relatar	1
Ver informações de status	1
Monitorar trabalhos	3
Baixar registros de tarefas	3
Relatórios de acesso	4
Tipos de relatórios do cliente VMware vSphere	4
Gerar um pacote de suporte a partir do SnapCenter Plug-in for VMware vSphere GUI	6
Gerar um pacote de suporte a partir do console de manutenção	7
Registros de auditoria	8
Eventos de Proteção de Dados	9
Eventos do Console de Manutenção	10
Eventos do Console de Administração	10
Configurar servidores syslog	11
Alterar configurações do log de auditoria	11

Monitorar e relatar

Ver informações de status

Você pode visualizar informações de status no Painel do cliente vSphere. As informações de status são atualizadas uma vez por hora.

Passos

1. Na página de atalho do cliente vCenter, selecione SnapCenter Plug-in for VMware vSphere (SCV).
2. No painel de navegação esquerdo do SCV, selecione **Painel > Status**.
3. Veja informações gerais sobre o status ou selecione um link para obter mais detalhes, conforme listado na tabela a seguir.

Este bloco do painel...	Exibe as seguintes informações...
Atividades de trabalho recentes	<p>Os três a cinco trabalhos de backup, restauração e montagem mais recentes.</p> <ul style="list-style-type: none">• Selecione um ID de trabalho para ver mais detalhes sobre ele.• Selecione Ver tudo para ir para a aba Monitor de Tarefas e obter mais detalhes sobre todas as tarefas.
Empregos	<p>Uma contagem de cada tipo de trabalho (backup, restauração e montagem) executado dentro da janela de tempo selecionada. Passe o cursor sobre uma seção do gráfico para ver mais detalhes dessa categoria.</p>

Este bloco do painel...	Exibe as seguintes informações...
Resumo da proteção mais recente	<p>Resumos do status de proteção de dados de VMs primárias e secundárias ou armazenamentos de dados dentro da janela de tempo selecionada.</p> <ul style="list-style-type: none"> Selecione o menu suspenso para selecionar VMs ou Datastores. Para armazenamento secundário, selecione * SnapVault* ou * SnapMirror*. Passe o cursor sobre uma seção de um gráfico para ver a contagem de VMs ou Datastores nessa categoria. Na categoria Bem-sucedido, o backup mais recente é listado para cada recurso. Você pode alterar a janela de tempo editando o arquivo de configuração. O padrão é 7 dias. Para mais informações, consulte "Personalize sua configuração". Os contadores internos são atualizados após cada backup primário ou secundário. O painel é atualizado a cada seis horas. O tempo de atualização não pode ser alterado. Observação: se você usar uma política de proteção de mirror-vault, os contadores do resumo de proteção serão exibidos no gráfico de resumo do SnapVault , não no gráfico do SnapMirror .
Configuração	O número total de cada tipo de objeto gerenciado pelo SnapCenter Plug-in for VMware vSphere.
Armazenar	<p>O número total de snapshots, SnapVault e SnapMirror gerados e a quantidade de armazenamento usada para snapshots primários e secundários. O gráfico de linhas representa separadamente o consumo de armazenamento primário e secundário, dia a dia, durante um período contínuo de 90 dias. As informações de armazenamento são atualizadas uma vez a cada 24 horas à 1h08. A economia de armazenamento é a proporção entre a capacidade lógica (economia de instantâneo mais armazenamento consumido) e a capacidade física do armazenamento primário. O gráfico de barras ilustra a economia de armazenamento.</p> <p>Passe o cursor sobre uma linha no gráfico para ver resultados detalhados dia a dia.</p>

Monitorar trabalhos

Depois de executar qualquer operação de proteção de dados usando o cliente VMware vSphere, você pode monitorar o status do trabalho na guia Monitor de Trabalho no Painel e visualizar os detalhes do trabalho.

Passos

1. Na página de atalho do cliente vCenter, selecione SnapCenter Plug-in for VMware vSphere (SCV).
2. No painel de navegação esquerdo do SCV, selecione **Painel**.
3. Quando dois ou mais vCenters estiverem configurados no modo vinculado, selecione a instância do plug-in SCV e selecione a guia **Job Monitor**. A guia Monitor de tarefas lista cada tarefa e seu status, hora de início e hora de término. Se os nomes dos trabalhos forem longos, talvez seja necessário rolar para a direita para ver os horários de início e término. A exibição é atualizada a cada 30 segundos.
 - Selecione o ícone de atualização na barra de ferramentas para atualizar a exibição sob demanda.
 - Selecione o ícone de filtro para escolher o intervalo de tempo, o tipo, a tag e o status dos trabalhos que você deseja exibir. O filtro diferencia maiúsculas de minúsculas.
 - Selecione o ícone de atualização na janela Detalhes do trabalho para atualizar a exibição enquanto o trabalho estiver em execução.

Se o Painel não exibir informações do trabalho, consulte "[Artigo da KB: O painel do cliente SnapCenter vSphere não exibe trabalhos](#)" .

Baixar registros de tarefas

Você pode baixar os logs de trabalho na guia Monitor de trabalho no Painel do cliente SnapCenter VMware vSphere.

Se você encontrar um comportamento inesperado ao usar o cliente VMware vSphere, poderá usar os arquivos de log para identificar a causa e resolver o problema.

 O valor padrão para retenção de logs de trabalhos é 30 dias; o valor padrão para retenção de trabalhos é 90 dias. Os logs de trabalho e os trabalhos mais antigos que a retenção configurada são limpos a cada seis horas. Você pode usar a Configuração jobs/cleanup APIs REST para modificar por quanto tempo os trabalhos e logs de trabalhos são retidos. Você não pode modificar o cronograma de limpeza.

Passos

1. Na página de atalho do cliente vCenter, selecione SnapCenter Plug-in for VMware vSphere (SCV).
2. No painel de navegação esquerdo do SCV, selecione **Painel > Monitor de tarefas**.
3. Selecione o ícone de download na barra de título do Job Monitor.

Talvez seja necessário rolar para a direita para ver o ícone.

Você também pode clicar duas vezes em um trabalho para acessar a janela Detalhes do trabalho e selecionar **Baixar registros de trabalho**.

Resultado

Os logs de trabalho estão localizados no host da VM Linux onde o SnapCenter Plug-in for VMware vSphere

está implantado. O local padrão do log de trabalho é `/var/log/netapp`.

Se você tentou baixar os logs de trabalho, mas o arquivo de log mencionado na mensagem de erro foi excluído, você poderá encontrar o seguinte erro: `HTTP ERROR 500 Problem accessing /export-scv-logs`. Para corrigir esse erro, verifique o status de acesso ao arquivo e as permissões para o arquivo nomeado na mensagem de erro e corrija o problema de acesso.

Relatórios de acesso

Você pode solicitar relatórios para um ou mais trabalhos no painel.

A guia Relatórios contém informações sobre os trabalhos selecionados na página Trabalhos no Painel. Se nenhuma tarefa for selecionada, a guia Relatórios ficará em branco.

Passos

1. Na página de atalho do cliente vCenter, selecione SnapCenter Plug-in for VMware vSphere (SCV).
2. No painel de navegação esquerdo do SCV, selecione **Painel** > guia **Relatórios**.
3. Para relatórios de backup, você pode fazer o seguinte:

- a. Modificar o relatório

Selezione o ícone de filtro para modificar o intervalo de tempo, o tipo de status do trabalho, os grupos de recursos e as políticas a serem incluídos no relatório.

- b. Gerar um relatório detalhado

Clique duas vezes em qualquer trabalho para gerar um relatório detalhado para esse trabalho.

4. Opcional: Na guia Relatórios, selecione **Download** e selecione o formato (HTML ou CSV).

Você também pode selecionar o ícone de download para baixar os logs do plug-in.

Tipos de relatórios do cliente VMware vSphere

O cliente VMware vSphere para SnapCenter fornece opções de relatórios personalizáveis que fornecem detalhes sobre seus trabalhos de proteção de dados e status de recursos de plug-in. Você pode gerar relatórios somente para proteção primária.

 Os agendamentos de backup são executados no fuso horário em que o SnapCenter Plug-in for VMware vSphere está implantado. O vCenter relata dados no fuso horário em que o vCenter está localizado. Portanto, se o SnapCenter Plug-in for VMware vSphere e o vCenter estiverem em fusos horários diferentes, os dados no painel do cliente VMware vSphere podem não ser os mesmos que os dados nos relatórios.

O Painel exibe informações sobre backups migrados somente após os backups pós-migração serem realizados.

Tipo de relatório	Descrição
Relatório de backup	<p>Exibe dados gerais sobre tarefas de backup. Selecione uma seção/status no gráfico para ver uma lista de trabalhos com esse status na guia Relatórios. Para cada trabalho, o relatório lista o ID do trabalho, o grupo de recursos correspondente, a política de backup, a hora de início e a duração, o status e os detalhes do trabalho, que incluem o nome do trabalho (nome do instantâneo), se o trabalho foi concluído, e quaisquer mensagens de aviso ou erro. Você pode baixar a tabela do Relatório em formato HTML ou CSV. Você também pode baixar os logs de tarefas do Job Monitor para todas as tarefas (não apenas as tarefas no relatório). Backups excluídos não são incluídos no relatório.</p>
Relatório de montagem	<p>Exibe dados gerais sobre trabalhos de montagem. Selecione uma seção/status no gráfico para ver uma lista de trabalhos com esse status na guia Relatórios. Para cada trabalho, o relatório lista o ID do trabalho, o status do trabalho, o nome do trabalho e os horários de início e término do trabalho. O nome do trabalho inclui o nome do instantâneo. Por exemplo: Mount Backup <snapshot-copy-name> Você pode baixar a tabela do Relatório em formato HTML ou CSV. Você também pode baixar os logs de tarefas do Job Monitor para todas as tarefas (não apenas as tarefas no relatório).</p>
Relatório de restauração	<p>Exibe informações gerais sobre o status dos trabalhos de restauração. Selecione uma seção/status no gráfico para ver uma lista de trabalhos com esse status na guia Relatórios. Para cada trabalho, o relatório lista o ID do trabalho, o status do trabalho, o nome do trabalho e os horários de início e término do trabalho. O nome do trabalho inclui o nome do instantâneo. Por exemplo: Restore Backup <snapshot-copy-name> Você pode baixar a tabela do Relatório em formato HTML ou CSV. Você também pode baixar os logs de tarefas do Job Monitor para todas as tarefas (não apenas as tarefas no relatório).</p>

Tipo de relatório	Descrição
Último relatório de status de proteção de VMs ou datastores	<p>Exibe informações gerais sobre o status de proteção, durante o número configurado de dias, para VMs e armazenamentos de dados gerenciados pelo SnapCenter Plug-in for VMware vSphere. O padrão é 7 dias. Para modificar o valor no arquivo de propriedades, consulte "Modificar valores padrão de configuração". Selecione uma seção/status no gráfico de proteção primária para ver uma lista de VMs ou armazenamentos de dados com esse status na guia Relatórios. O Relatório de status de proteção de VM ou datastors para VMs e datastors protegidos exibe os nomes das VMs ou datastors dos quais foi feito backup durante o número de dias configurado, o nome do snapshot mais recente e os horários de início e término da última execução de backup. O Relatório de status de proteção de VMs ou datastors para VMs ou datastors desprotegidos exibe os nomes das VMs ou datastors que não têm backups bem-sucedidos durante o número de dias configurado. Você pode baixar a tabela do Relatório em formato HTML ou CSV. Você também pode baixar os logs de tarefas do Job Monitor para todas as tarefas (não apenas as tarefas no relatório). Este relatório é atualizado a cada hora quando o cache do plug-in é atualizado. Portanto, o relatório pode não exibir VMs ou armazenamentos de dados que foram submetidos a backup recentemente.</p>

Gerar um pacote de suporte a partir do SnapCenter Plug-in for VMware vSphere GUI

Antes de começar

Para fazer logon na GUI de gerenciamento do SnapCenter Plug-in for VMware vSphere , você precisa saber o endereço IP e as credenciais de logon. Você também deve anotar o token MFA gerado pelo console de manutenção.

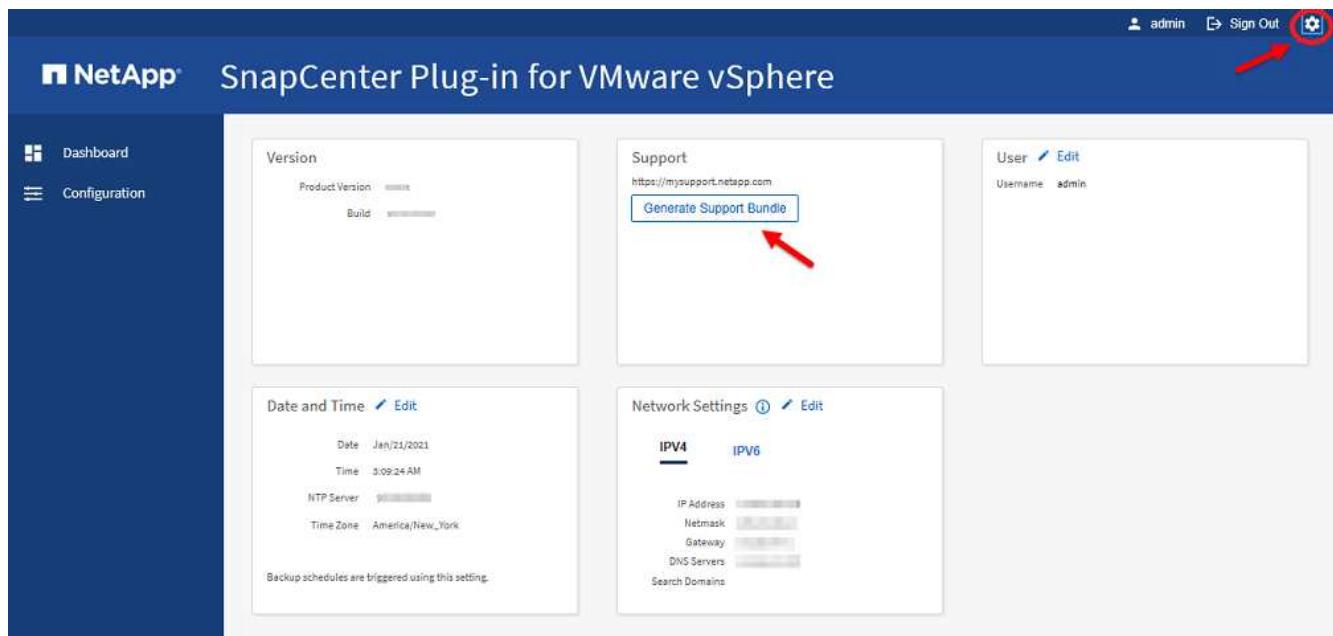
- O endereço IP foi exibido quando o SnapCenter Plug-in for VMware vSphere foi implantado.
- Use as credenciais de login fornecidas durante a implantação do SnapCenter Plug-in for VMware vSphere ou conforme modificado posteriormente.
- Gere um token MFA de 6 dígitos usando as opções de configuração do sistema do console de manutenção.

Passos

1. Efetue login na interface gráfica do usuário do SnapCenter Plug-in for VMware vSphere .

Use o formato `https://<OVA-IP-address>:8080` .

2. Selecione o ícone Configurações na barra de ferramentas superior.



3. Na página **Configurações**, na seção **Supor te**, selecione **Gerar pacote de suporte**.
4. Depois que o pacote de suporte for gerado, selecione o link fornecido para baixar o pacote para o NetApp.

Gerar um pacote de suporte a partir do console de manutenção

Passos

1. No cliente VMware vSphere, selecione a VM onde o SnapCenter Plug-in for VMware vSphere está localizado.
2. Na guia **Resumo** do dispositivo virtual, selecione **Iniciar console remoto ou Iniciar console da Web** para abrir uma janela do console de manutenção e, em seguida, faça logon.

Para obter informações sobre como acessar e fazer logon no console de manutenção, consulte "[Acesse o Console de Manutenção](#)" .

```
Maintenance Console : "SnapCenter Plug-in for VMware vSphere"
Discovered interfaces: eth0 (ENABLED)

Main Menu:
-----
1 ) Application Configuration
2 ) System Configuration
3 ) Network Configuration
4 ) Support and Diagnostics

x ) Exit

Enter your choice: _
```

3. No Menu Principal, acesse a opção **4) Suporte e Diagnóstico**.
4. No menu Suporte e Diagnóstico, insira a opção **1) Gerar pacote de suporte**.

Para acessar o pacote de suporte, no menu Suporte e Diagnóstico, insira a opção **2) Acessar Shell de Diagnóstico**. No console, navegue até `/support/support/<bundle_name>.tar.gz`.

Registros de auditoria

Um log de auditoria é uma coleção de eventos em ordem cronológica, que é gravada em um arquivo dentro do dispositivo. Os arquivos de log de auditoria são gerados em `/var/log/netapp/audit` localização e os nomes dos arquivos seguem uma das convenções de nomenclatura abaixo:

- `audit.log`: arquivo de log de auditoria ativo que está em uso.
- `audit-%d{aaaa-MM-dd-HH-mm-ss}.log.gz`: Arquivo de log de auditoria substituído. A data e a hora no nome do arquivo indicam quando o arquivo foi criado, por exemplo: `audit-2022-12-15-16-28-01.log.gz`.

Na interface do usuário do plug-in SCV, você pode visualizar e exportar os detalhes do log de auditoria em **Painel > Configurações > Guia Logs de auditoria**. Você pode visualizar a auditoria de operação nos logs de auditoria. Os logs de auditoria são baixados com o pacote de suporte.

Se as configurações de e-mail estiverem definidas, o SCV enviará uma notificação por e-mail no caso de uma falha na verificação de integridade do log de auditoria. Uma falha na verificação de integridade do log de auditoria pode ocorrer quando um dos arquivos é adulterado ou excluído.

As configurações padrão dos arquivos de auditoria são:

- O arquivo de log de auditoria em uso pode crescer até um máximo de 10 MB

- São retidos no máximo 10 arquivos de log de auditoria

Os logs de auditoria transferidos são verificados periodicamente quanto à integridade. O SCV fornece APIs REST para visualizar logs e verificar sua integridade. Um agendamento integrado aciona e atribui um dos seguintes status de integridade.

Status	Descrição
VIOLADO	O conteúdo do arquivo de log de auditoria foi modificado
NORMAL	O arquivo de log de auditoria não foi modificado
ROLLOVER EXCLUIR	- O arquivo de log de auditoria é excluído com base na retenção - Por padrão, apenas 10 arquivos são retidos
EXCLUSÃO INESPERADA	O arquivo de log de auditoria foi excluído
ATIVO	- O arquivo de log de auditoria está em uso - Aplicável somente a audit.log

Os eventos são categorizados em três categorias principais:

- Eventos de Proteção de Dados
- Eventos do Console de Manutenção
- Eventos do Console de Administração

Eventos de Proteção de Dados

Os recursos no SCV são:

- Sistema de armazenamento
- Grupo de Recursos
- Política
- Backup
- Subscrição
- Conta

A tabela a seguir lista as operações que podem ser executadas em cada recurso:

Recursos	Operações
Sistema de armazenamento	Criado, Modificado, Excluído
Subscrição	Criado, Modificado, Excluído
Conta	Criado, Modificado, Excluído
Grupo de Recursos	Criado, modificado, excluído, suspenso, retomado
Política	Criado, Modificado, Excluído

Backup	Criado, renomeado, excluído, montado, desmontado, VMDK restaurado, VM restaurada, anexar VMDK, desanexar VMDK, restauração de arquivo convidado
--------	---

Eventos do Console de Manutenção

As operações administrativas no console de manutenção são auditadas. As opções de console de manutenção disponíveis são:

1. Iniciar/Parar serviços
2. Alterar nome de usuário e senha
3. Alterar senha do MySQL
4. Configurar backup do MySQL
5. Restaurar backup do MySQL
6. Alterar senha do usuário 'maint'
7. Alterar fuso horário
8. Alterar servidor NTP
9. Desabilitar acesso SSH
10. Aumentar o tamanho do disco de prisão
11. Atualizar
12. Instalar o VMware Tools (estamos trabalhando para substituí-lo pelo Open-VM Tools)
13. Alterar configurações de endereço IP
14. Alterar configurações de pesquisa de nome de domínio
15. Alterar rotas estáticas
16. Acessar shell de diagnóstico
17. Habilitar acesso de diagnóstico remoto

Eventos do Console de Administração

As seguintes operações na interface do usuário do Admin Console são auditadas:

- Configurações
 - Alterar credenciais de administrador
 - Alterar fuso horário
 - Alterar servidor NTP
 - Alterar configurações de endereço IPv4/IPv6
- Configuração
 - Alterar credenciais do vCenter
 - Habilitar/Desabilitar Plug-in

Configurar servidores syslog

Os logs de auditoria são armazenados no dispositivo e sua integridade é verificada periodicamente. O encaminhamento de eventos permite que você obtenha eventos do computador de origem ou de encaminhamento e os armazene em um computador centralizado, que é o servidor Syslog. Os dados são criptografados em trânsito entre a origem e o destino.

Antes de começar

Você deve ter privilégios de administrador.

Sobre esta tarefa

Esta tarefa ajuda você a configurar o servidor syslog.

Passos

1. Efetue login no SnapCenter Plug-in for VMware vSphere.
2. No painel de navegação esquerdo, selecione **Configurações > Registros de auditoria > Configurações**.
3. No painel **Configurações do Log de Auditoria**, selecione **Enviar logs de auditoria para o servidor Syslog**
4. Insira os seguintes detalhes:
 - IP do servidor Syslog
 - Porta do servidor Syslog
 - Formato RFC
 - Certificado do Servidor Syslog
5. Selecione **SALVAR** para salvar as configurações do servidor Syslog.

Alterar configurações do log de auditoria

Você pode alterar as configurações padrão das definições de log.

Antes de começar

Você deve ter privilégios de administrador.

Sobre esta tarefa

Esta tarefa ajuda você a alterar as configurações padrão do log de auditoria.

Passos

1. Efetue login no SnapCenter Plug-in for VMware vSphere.
2. No painel de navegação esquerdo, selecione **Configurações > Registros de auditoria > Configurações**.
3. No painel **Configurações do Log de Auditoria**, insira o Número máximo de arquivos de log de auditoria e o Limite de tamanho do arquivo de log de auditoria.
4. Selecione a opção **Enviar logs de auditoria para o servidor Syslog** se você optar por enviar os logs para o servidor Syslog. Insira os detalhes do servidor.
5. Salve as configurações.

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

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

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

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

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

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

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

Informações sobre marcas comerciais

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