



# Configurando clientes de auditoria para CIFS

StorageGRID

NetApp  
March 10, 2025

# Índice

- Configurando clientes de auditoria para CIFS ..... 1
  - Configurando clientes de auditoria para o Workgroup ..... 1
  - Configurando clientes de auditoria para o ativo Directory ..... 4
  - Adicionando um usuário ou grupo a um compartilhamento de auditoria CIFS ..... 7
  - Removendo um usuário ou grupo de um compartilhamento de auditoria CIFS ..... 9
  - Alterando um nome de usuário ou grupo de compartilhamento de auditoria CIFS ..... 11
  - Verificação da integração da auditoria CIFS ..... 11

# Configurando clientes de auditoria para CIFS

O procedimento usado para configurar um cliente de auditoria depende do método de autenticação: Windows Workgroup ou Windows active Directory (AD). Quando adicionado, o compartilhamento de auditoria é ativado automaticamente como um compartilhamento somente leitura.



A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

## Informações relacionadas

["Atualizar o software"](#)

## Configurando clientes de auditoria para o Workgroup

Execute este procedimento para cada nó de administrador em uma implantação do StorageGRID a partir da qual você deseja recuperar mensagens de auditoria.

### O que você vai precisar

- Você deve ter o `Passwords.txt` arquivo com a senha da conta root/admin (disponível no REFERIDO pacote).
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).

### Sobre esta tarefa

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

### Passos

1. Faça login no nó de administração principal:

- Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
- Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- Digite o seguinte comando para mudar para root: `su -`
- Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Confirme se todos os serviços têm estado em execução ou verificado: `storagegrid-status`

Se todos os serviços não estiverem em execução ou verificados, resolva os problemas antes de continuar.

3. Volte para a linha de comando, pressione **Ctrl \* C\***.

4. Inicie o utilitário de configuração CIFS: `config_cifs.rb`

Shares	Authentication	Config
add-audit-share	set-authentication	validate-config
enable-disable-share	set-netbios-name	help
add-user-to-share	join-domain	exit
remove-user-from-share	add-password-server	
modify-group	remove-password-server	
	add-wins-server	
	remove-wins-server	

## 5. Defina a autenticação para o grupo de trabalho do Windows:

Se a autenticação já tiver sido definida, é apresentada uma mensagem de aviso. Se a autenticação já tiver sido definida, vá para a próxima etapa.

- Introduza: `set-authentication`
- Quando solicitado para a instalação do Windows Workgroup ou do Active Directory, digite: `workgroup`
- Quando solicitado, insira um nome do grupo de trabalho: `workgroup_name`
- Quando solicitado, crie um nome NetBIOS significativo: `netbios_name`

ou

Pressione **Enter** para usar o nome do host do Admin Node como o nome NetBIOS.

O script reinicia o servidor Samba e as alterações são aplicadas. Isso deve levar menos de um minuto. Depois de definir a autenticação, adicione um cliente de auditoria.

- Quando solicitado, pressione **Enter**.

O utilitário de configuração CIFS é exibido.

## 6. Adicionar um cliente de auditoria:

- Introduza: `add-audit-share`



O compartilhamento é adicionado automaticamente como somente leitura.

- Quando solicitado, adicione um usuário ou grupo: `user`
- Quando solicitado, insira o nome de usuário da auditoria: `audit_user_name`
- Quando solicitado, insira uma senha para o usuário de auditoria: `password`
- Quando solicitado, digite novamente a mesma senha para confirmá-la: `password`
- Quando solicitado, pressione **Enter**.

O utilitário de configuração CIFS é exibido.



Não há necessidade de inserir um diretório. O nome do diretório de auditoria é predefinido.

7. Se mais de um usuário ou grupo tiver permissão para acessar o compartilhamento de auditoria, adicione os usuários adicionais:

a. Introduza: `add-user-to-share`

É apresentada uma lista numerada de partilhas ativadas.

b. Quando solicitado, insira o número do compartilhamento de auditoria-exportação: `share_number`

c. Quando solicitado, adicione um usuário ou grupo: `user`

ou `group`

d. Quando solicitado, insira o nome do usuário ou grupo de auditoria: `audit_user` or `audit_group`

e. Quando solicitado, pressione **Enter**.

O utilitário de configuração CIFS é exibido.

f. Repita essas subetapas para cada usuário ou grupo adicional que tenha acesso ao compartilhamento de auditoria.

8. Opcionalmente, verifique sua configuração: `validate-config`

Os serviços são verificados e exibidos. Você pode ignorar com segurança as seguintes mensagens:

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

a. Quando solicitado, pressione **Enter**.

A configuração do cliente de auditoria é exibida.

b. Quando solicitado, pressione **Enter**.

O utilitário de configuração CIFS é exibido.

9. Feche o utilitário de configuração CIFS: `exit`

10. Inicie o serviço Samba: `service smb start`

11. Se a implantação do StorageGRID for um único local, vá para a próxima etapa.

ou

Opcionalmente, se a implantação do StorageGRID incluir nós de administração em outros sites, habilite esse compartilhamento de auditoria conforme necessário:

- a. Faça login remotamente no Admin Node de um site:
  - i. Introduza o seguinte comando: `ssh admin@grid_node_IP`
  - ii. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
  - iii. Digite o seguinte comando para mudar para root: `su -`
  - iv. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- b. Repita as etapas para configurar o compartilhamento de auditoria para cada nó Admin adicional.
- c. Feche o login remoto do shell seguro para o Admin Node remoto: `exit`

12. Faça logout do shell de comando: `exit`

### Informações relacionadas

["Atualizar o software"](#)

## Configurando clientes de auditoria para o ativo Directory

Execute este procedimento para cada nó de administrador em uma implantação do StorageGRID a partir da qual você deseja recuperar mensagens de auditoria.

### O que você vai precisar

- Você deve ter o `Passwords.txt` arquivo com a senha da conta root/admin (disponível no REFERIDO pacote).
- Você deve ter o nome de usuário e a senha do CIFS ativo Directory.
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).



A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

### Passos

1. Faça login no nó de administração principal:
  - a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
  - b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
  - c. Digite o seguinte comando para mudar para root: `su -`
  - d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Confirme se todos os serviços têm estado em execução ou verificado: `storagegrid-status`

Se todos os serviços não estiverem em execução ou verificados, resolva os problemas antes de continuar.

3. Volte para a linha de comando, pressione **Ctrl \* C\***.
4. Inicie o utilitário de configuração CIFS: `config_cifs.rb`

Shares	Authentication	Config
add-audit-share	set-authentication	validate-config
enable-disable-share	set-netbios-name	help
add-user-to-share	join-domain	exit
remove-user-from-share	add-password-server	
modify-group	remove-password-server	
	add-wins-server	
	remove-wins-server	

##### 5. Defina a autenticação para o ativo Directory: `set-authentication`

Na maioria das implantações, você deve definir a autenticação antes de adicionar o cliente de auditoria. Se a autenticação já tiver sido definida, é apresentada uma mensagem de aviso. Se a autenticação já tiver sido definida, vá para a próxima etapa.

- Quando solicitado para a instalação do Workgroup ou do ativo Directory: `ad`
- Quando solicitado, insira o nome do domínio AD (nome de domínio curto).
- Quando solicitado, insira o endereço IP do controlador de domínio ou o nome de host DNS.
- Quando solicitado, insira o nome completo do domínio realm.

Use letras maiúsculas.

- Quando solicitado a ativar o suporte winbind, digite `y`.

O Winbind é usado para resolver informações de usuários e grupos de servidores AD.

- Quando solicitado, insira o nome NetBIOS.
- Quando solicitado, pressione **Enter**.

O utilitário de configuração CIFS é exibido.

##### 6. Junte-se ao domínio:

- Se ainda não tiver sido iniciado, inicie o utilitário de configuração CIFS: `config_cifs.rb`
- Junte-se ao domínio: `join-domain`
- Você será solicitado a testar se o nó Admin é atualmente um membro válido do domínio. Se este nó Admin não tiver aderido anteriormente ao domínio, introduza: `no`
- Quando solicitado, forneça o nome de usuário do Administrador: `administrator_username`

```
`_administrator_username_`Onde está o nome de usuário do CIFS ativo
Directory, não o nome de usuário do StorageGRID.
```

- Quando solicitado, forneça a senha do administrador: `administrator_password`

Was `administrator_password` é o nome de usuário do CIFS ativo Directory, não a senha do StorageGRID.

f. Quando solicitado, pressione **Enter**.

O utilitário de configuração CIFS é exibido.

7. Verifique se você entrou corretamente no domínio:

a. Junte-se ao domínio: `join-domain`

b. Quando solicitado a testar se o servidor é atualmente um membro válido do domínio, digite: `y`

Se você receber a mensagem ""Join is OK"", você se juntou com sucesso ao domínio. Se você não receber essa resposta, tente configurar a autenticação e ingressar no domínio novamente.

c. Quando solicitado, pressione **Enter**.

O utilitário de configuração CIFS é exibido.

8. Adicionar um cliente de auditoria: `add-audit-share`

a. Quando solicitado a adicionar um usuário ou grupo, digite: `user`

b. Quando solicitado a inserir o nome de usuário da auditoria, insira o nome de usuário da auditoria.

c. Quando solicitado, pressione **Enter**.

O utilitário de configuração CIFS é exibido.

9. Se mais de um usuário ou grupo tiver permissão para acessar o compartilhamento de auditoria, adicione usuários adicionais: `add-user-to-share`

É apresentada uma lista numerada de partilhas ativadas.

a. Introduza o número da partilha de auditoria-exportação.

b. Quando solicitado a adicionar um usuário ou grupo, digite: `group`

Você será solicitado a fornecer o nome do grupo de auditoria.

c. Quando solicitado o nome do grupo de auditoria, insira o nome do grupo de usuários de auditoria.

d. Quando solicitado, pressione **Enter**.

O utilitário de configuração CIFS é exibido.

e. Repita esta etapa para cada usuário ou grupo adicional que tenha acesso ao compartilhamento de auditoria.

10. Opcionalmente, verifique sua configuração: `validate-config`

Os serviços são verificados e exibidos. Você pode ignorar com segurança as seguintes mensagens:

- Não foi possível encontrar o arquivo incluir `/etc/samba/includes/cifs-interfaces.inc`
- Não foi possível encontrar o arquivo incluir `/etc/samba/includes/cifs-filesystem.inc`
- Não foi possível encontrar o arquivo incluir `/etc/samba/includes/cifs-interfaces.inc`



- Não foi possível encontrar o arquivo incluir `/etc/samba/includes/cifs-custom-config.inc`
- Não foi possível encontrar o arquivo incluir `/etc/samba/includes/cifs-shares.inc`
- `Rlimit_Max`: Aumentando `rlimit_Max` (1024) para o limite mínimo de Windows (16384)



Não combine a configuração 'anúncios' com o parâmetro 'servidor de senha'. (Por padrão, o Samba irá descobrir o DC correto para entrar em Contato automaticamente).

- Quando solicitado, pressione **Enter** para exibir a configuração do cliente de auditoria.
- Quando solicitado, pressione **Enter**.

O utilitário de configuração CIFS é exibido.

11. Feche o utilitário de configuração CIFS: `exit`

12. Se a implantação do StorageGRID for um único local, vá para a próxima etapa.

ou

Opcionalmente, se a implantação do StorageGRID incluir nós de administração em outros sites, habilite esses compartilhamentos de auditoria conforme necessário:

a. Faça login remotamente no Admin Node de um site:

- Introduza o seguinte comando: `ssh admin@grid_node_IP`
- Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- Digite o seguinte comando para mudar para root: `su -`
- Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

b. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó de administração.

c. Feche o login remoto do shell seguro para o Admin Node: `exit`

13. Faça logout do shell de comando: `exit`

#### Informações relacionadas

["Atualizar o software"](#)

## Adicionando um usuário ou grupo a um compartilhamento de auditoria CIFS

Você pode adicionar um usuário ou grupo a um compartilhamento de auditoria CIFS integrado à autenticação AD.

#### O que você vai precisar

- Você deve ter o `Passwords.txt` arquivo com a senha da conta root/admin (disponível no REFERIDO pacote).
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).

#### Sobre esta tarefa

O procedimento a seguir é para um compartilhamento de auditoria integrado com autenticação AD.



A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

## Passos

1. Faça login no nó de administração principal:

- Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
- Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- Digite o seguinte comando para mudar para root: `su -`
- Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Confirme se todos os serviços têm estado em execução ou verificado. Introduza: `storagegrid-status`

Se todos os serviços não estiverem em execução ou verificados, resolva os problemas antes de continuar.

3. Volte para a linha de comando, pressione **Ctrl \* C**.

4. Inicie o utilitário de configuração CIFS: `config_cifs.rb`

```
-----  
| Shares                | Authentication          | Config                  |  
-----  
| add-audit-share       | set-authentication      | validate-config        |  
| enable-disable-share  | set-netbios-name       | help                   |  
| add-user-to-share     | join-domain            | exit                   |  
| remove-user-from-share | add-password-server    |                        |  
| modify-group          | remove-password-server |                        |  
|                       | add-wins-server        |                        |  
|                       | remove-wins-server     |                        |  
-----
```

5. Comece a adicionar um usuário ou grupo: `add-user-to-share`

Uma lista numerada de compartilhamentos de auditoria que foram configurados é exibida.

6. Quando solicitado, insira o número para o compartilhamento de auditoria (auditoria-exportação):

`audit_share_number`

Você será perguntado se deseja dar a um usuário ou a um grupo acesso a esse compartilhamento de auditoria.

7. Quando solicitado, adicione um usuário ou grupo: `user` Ou `group`

8. Quando for solicitado o nome do usuário ou grupo para este compartilhamento de auditoria do AD, digite o nome.

O usuário ou grupo é adicionado como somente leitura para o compartilhamento de auditoria tanto no

sistema operacional do servidor quanto no serviço CIFS. A configuração do Samba é recarregada para permitir que o usuário ou grupo acesse o compartilhamento de cliente de auditoria.

9. Quando solicitado, pressione **Enter**.

O utilitário de configuração CIFS é exibido.

10. Repita estas etapas para cada usuário ou grupo que tenha acesso ao compartilhamento de auditoria.

11. Opcionalmente, verifique sua configuração: `validate-config`

Os serviços são verificados e exibidos. Você pode ignorar com segurança as seguintes mensagens:

- Não foi possível encontrar include file `/etc/samba/includes/cifs-interfaces.inc`
- Não foi possível encontrar include file `/etc/samba/includes/cifs-filesystem.inc`
- Não foi possível encontrar include file `/etc/samba/includes/cifs-custom-config.inc`
- Não foi possível encontrar include file `/etc/samba/includes/cifs-shares.inc`
  - i. Quando solicitado, pressione **Enter** para exibir a configuração do cliente de auditoria.
  - ii. Quando solicitado, pressione **Enter**.

12. Feche o utilitário de configuração CIFS: `exit`

13. Determine se você precisa habilitar compartilhamentos de auditoria adicionais, como a seguir:

- Se a implantação do StorageGRID for um único local, vá para a próxima etapa.
- Se a implantação do StorageGRID incluir nós de administração em outros sites, habilite esses compartilhamentos de auditoria conforme necessário:
  - i. Faça login remotamente no Admin Node de um site:
    - A. Introduza o seguinte comando: `ssh admin@grid_node_IP`
    - B. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
    - C. Digite o seguinte comando para mudar para root: `su -`
    - D. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
  - ii. Repita estas etapas para configurar os compartilhamentos de auditoria para cada nó de administração.
  - iii. Feche o login remoto do shell seguro para o Admin Node remoto: `exit`

14. Faça logout do shell de comando: `exit`

## Removendo um usuário ou grupo de um compartilhamento de auditoria CIFS

Não é possível remover o último usuário ou grupo permitido para acessar o compartilhamento de auditoria.

### O que você vai precisar

- Você deve ter o `Passwords.txt` arquivo com as senhas da conta root (disponível no REFERIDO pacote).
- Você deve ter o `Configuration.txt` arquivo (disponível no REFERIDO pacote).

## Sobre esta tarefa

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

## Passos

1. Faça login no nó de administração principal:

- a. Introduza o seguinte comando: `ssh admin@primary_Admin_Node_IP`
- b. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.
- c. Digite o seguinte comando para mudar para root: `su -`
- d. Introduza a palavra-passe listada no `Passwords.txt` ficheiro.

Quando você estiver conetado como root, o prompt mudará de `$` para `#`.

2. Inicie o utilitário de configuração CIFS: `config_cifs.rb`

```
-----  
| Shares                | Authentication          | Config                  |  
-----  
| add-audit-share       | set-authentication      | validate-config        |  
| enable-disable-share  | set-netbios-name       | help                   |  
| add-user-to-share     | join-domain            | exit                   |  
| remove-user-from-share| add-password-server    |                        |  
| modify-group          | remove-password-server |                        |  
|                       | add-wins-server        |                        |  
|                       | remove-wins-server     |                        |  
-----
```

3. Comece a remover um usuário ou grupo: `remove-user-from-share`

Uma lista numerada de compartilhamentos de auditoria disponíveis para o nó Admin é exibida. O compartilhamento de auditoria é rotulado `auditoria-exportação`.

4. Introduza o número da partilha de auditoria: `audit_share_number`

5. Quando solicitado a remover um usuário ou um grupo: `user` Ou `group`

É apresentada uma lista numerada de utilizadores ou grupos para a partilha de auditoria.

6. Introduza o número correspondente ao utilizador ou grupo que pretende remover: `number`

O compartilhamento de auditoria é atualizado e o usuário ou grupo não tem mais permissão para acessar o compartilhamento de auditoria. Por exemplo:

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
 1. audituser
 2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Feche o utilitário de configuração CIFS: `exit`
8. Se a implantação do StorageGRID incluir nós de administração em outros sites, desative o compartilhamento de auditoria em cada site, conforme necessário.
9. Faça logout de cada shell de comando quando a configuração estiver concluída: `exit`

#### Informações relacionadas

["Atualizar o software"](#)

## Alterando um nome de usuário ou grupo de compartilhamento de auditoria CIFS

Você pode alterar o nome de um usuário ou grupo para um compartilhamento de auditoria CIFS adicionando um novo usuário ou grupo e excluindo o antigo.

#### Sobre esta tarefa

A exportação de auditoria por meio do CIFS/Samba foi obsoleta e será removida em uma futura versão do StorageGRID.

#### Passos

1. Adicione um novo usuário ou grupo com o nome atualizado ao compartilhamento de auditoria.
2. Exclua o nome de usuário ou grupo antigo.

#### Informações relacionadas

["Atualizar o software"](#)

["Adicionando um usuário ou grupo a um compartilhamento de auditoria CIFS"](#)

["Removendo um usuário ou grupo de um compartilhamento de auditoria CIFS"](#)

## Verificação da integração da auditoria CIFS

O compartilhamento de auditoria é somente leitura. Os ficheiros de registo destinam-se a ser lidos por aplicações de computador e a verificação não inclui a abertura de um

ficheiro. Considera-se verificação suficiente que os arquivos de log de auditoria apareçam em uma janela do Windows Explorer. Após a verificação de conexão, feche todas as janelas.

## **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 DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

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

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

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

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

## **Informações sobre marcas comerciais**

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