Monitorar e relatar

SnapCenter Plug-in for VMware vSphere

NetApp
January 31, 2025

Índice

Monitorar e relatar

Exibir informações de status

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

Passos

1. No painel Navegador esquerdo do cliente vSphere, clique em **Dashboard**, selecione um vCenter Server e clique na guia **Status** no painel do painel.
2. Veja informações de status da visão geral ou clique em um link para obter mais detalhes, conforme listado na tabela a seguir.

Este painel de instrumentos…	Exibe as seguintes informações…
Atividades de trabalho recentes	Os três a cinco trabalhos mais recentes de backup, restauração e montagem. • Clique em um ID de trabalho para ver mais detalhes sobre esse trabalho. • Clique em **See All** (Ver tudo) para aceder ao separador Job Monitor (Monitor de trabalhos) para obter mais detalhes sobre todos os trabalhos.
Trabalhos	Uma contagem de cada tipo de tarefa (backup, restauração e montagem) executada na janela de tempo selecionada. Passe o cursor sobre uma seção do gráfico para ver mais detalhes sobre essa categoria.

Este painel de instrumentos…	Exibe as seguintes informações…
Resumo de proteção mais recente	Resumos do status de proteção de dados de VMs primárias e secundárias ou armazenamentos de dados na janela de tempo selecionada. • Clique no 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-sucedida, o backup mais recente é listado para cada recurso. • Você pode alterar a janela de tempo editando o arquivo de configuração. O padrão é de 7 dias. Para obter mais informações, "Personalize sua configuração"consulte . • Os contadores internos são atualizados após cada backup primário ou secundário. O painel de instrumentos é atualizado a cada seis horas. O tempo de atualização não pode ser alterado. Observação: Se você usar uma política de proteção do mirror-Vault, os contadores do resumo de proteção serão exibidos no gráfico de resumo do SnapVault, não no gráfico SnapMirror.
Configuração	O número total de cada tipo de objeto gerenciado pelo plug-in SnapCenter para VMware vSphere.
Armazenamento	O número total de cópias Snapshot, SnapVault e SnapMirror Snapshot gerado e a quantidade de storage usada para cópias Snapshot primário e secundário. O gráfico de linha traça separadamente o consumo de storage primário e secundário diariamente durante um período contínuo de 90 dias. As informações de storage são atualizadas a cada 24 horas às 1:08:00. A economia de storage é a taxa de capacidade lógica (economia de cópia Snapshot e storage consumido) para a capacidade física do storage primário. O gráfico de barras ilustra a economia de armazenamento. Passe o cursor sobre uma linha no gráfico para ver os resultados detalhados do dia a dia.

Monitorizar trabalhos

Depois de executar qualquer operação de proteção de dados usando o cliente VMware vSphere, você pode monitorar o status da tarefa na guia Monitor de tarefas no Painel e exibir os detalhes da tarefa.

Passos

1. No painel Navegador esquerdo do cliente vSphere, clique em **Dashboard**, quando dois ou mais vCenters estiverem configurados no modo vinculado, selecione um vCenter Server e, em seguida, clique na guia **Job Monitor** no painel Painel. A guia Monitor de trabalhos lista cada tarefa e seu status, hora de início e hora de término. Se os nomes dos trabalhos forem longos, poderá ser necessário deslocar-se para a direita para visualizar os tempos de início e de fim. O visor é atualizado a cada 30 segundos.
    - Selecione o ícone Atualizar na barra de ferramentas para atualizar a exibição sob demanda.
    - Selecione o ícone de filtro para escolher o intervalo de tempo, o tipo, a etiqueta e o estado dos trabalhos que pretende visualizar. O filtro é sensível a maiúsculas e minúsculas.
    - Selecione o ícone Atualizar na janela Detalhes do trabalho para atualizar o visor enquanto o trabalho está em execução.

Se o Painel de instrumentos não apresentar informações sobre o trabalho, consulte "Artigo da KB: O painel do cliente do SnapCenter vSphere não exibe trabalhos" .

Transferir registos de trabalhos

Você pode fazer o download dos logs de tarefas na guia Monitor de tarefas no Painel do cliente VMware vSphere do SnapCenter.

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 predefinido para reter registos de trabalhos é de 30 dias; o valor predefinido para trabalhos de retenção é de 90 dias. Os registos de trabalhos e os trabalhos que são mais antigos do que a retenção configurada são purgados a cada seis horas. Você pode usar as APIs REST de configuração `jobs/cleanup` para modificar por quanto tempo as tarefas e os logs de tarefas são retidos. Não é possível modificar o agendamento de purga.

Passos

1. No painel Navegador esquerdo do cliente vSphere, clique em **Dashboard**, selecione um vCenter Server e, em seguida, clique na guia **Job Monitor** no painel Dashboard.
2. Selecione o ícone de transferência na barra de título do Monitor de trabalhos.

    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 clicar em **Download de logs de trabalho**.

Resultado

Os logs de tarefa estão localizados no host de VM Linux onde o plug-in SnapCenter VMware é implantado. A localização predefinida do registo de trabalhos é `/var/log/netapp`.

Se você tentou fazer o download de logs de trabalho, mas o arquivo de log nomeado na mensagem de erro foi excluído, você pode 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.

Acesse relatórios

Pode solicitar relatórios para um ou mais trabalhos a partir do painel de instrumentos.

O separador relatórios contém informações sobre os trabalhos selecionados na página trabalhos no Painel de instrumentos. Se não forem selecionados trabalhos, o separador relatórios fica em branco.

Passos

1. No painel Navegador esquerdo do cliente vSphere, clique em **Dashboard**, selecione um vCenter Server e clique na guia **Reports**.
2. Para relatórios de backup, você pode fazer o seguinte:
   a. Modifique o relatório

      Selecione o ícone de filtro para modificar o intervalo de tempo, o tipo de estado da tarefa, os grupos de recursos e as políticas a serem incluídas no relatório.

   b. Gerar um relatório detalhado

      Clique duas vezes em qualquer tarefa para gerar um relatório detalhado para esse trabalho.
3. Opcional: Na guia relatórios, clique em **Download** e selecione o formato (HTML ou CSV).

   Também pode clicar no ícone de transferência para transferir registos de plug-in.

Tipos de relatórios do cliente VMware vSphere

O cliente VMware vSphere para SnapCenter oferece opções de relatório personalizáveis que fornecem detalhes sobre suas tarefas de proteção de dados e status do recurso de plug-in. Você pode gerar relatórios apenas para proteção primária.

> As programações de backup são executadas no fuso horário em que o plug-in SnapCenter VMware é implantado. O vCenter relata dados no fuso horário em que o vCenter está localizado. Portanto, se o plug-in do VMware SnapCenter e o vCenter estiverem em fusos horários diferentes, os dados no Dashboard do cliente do VMware vSphere podem não ser os mesmos que os dados nos relatórios.

O Dashboard exibe informações sobre backups migrados somente após a realização dos backups após a migração.

Tipo de relatório	Descrição
Relatório de cópia de segurança	Apresenta dados gerais sobre trabalhos de cópia de segurança. Clique em uma seção/status no gráfico para ver uma lista de tarefas com esse status na guia **relatórios**. Para cada tarefa, o relatório lista o ID do trabalho, o grupo de recursos correspondente, a política de backup, a hora e a duração do início, o status e os detalhes do trabalho, que incluem o nome do trabalho (nome da cópia instantânea) se o trabalho for concluído e quaisquer mensagens de aviso ou erro. Você pode fazer o download da tabela Relatório em formato HTML ou CSV. Também pode transferir os registos de trabalhos do Monitor de trabalhos para todos os trabalhos (não apenas os trabalhos do relatório). Os backups excluídos não estão incluídos no relatório.
Relatório de montagem	Apresenta dados de visão geral sobre trabalhos de montagem. Clique numa secção/estado no gráfico para ver uma lista de trabalhos com esse estado no separador relatórios. Para cada trabalho, o relatório lista a ID do trabalho, o estado do trabalho, o nome do trabalho e as horas de início e fim do trabalho. O nome do trabalho inclui o nome da cópia Snapshot. Por exemplo: `Mount Backup <snapshot-copy-name>` Você pode baixar a tabela Relatório em formato HTML ou CSV. Também pode transferir os registos de trabalhos do Monitor de trabalhos para todos os trabalhos (não apenas os trabalhos do relatório).
Restaurar relatório	Apresenta informações de estado geral sobre os trabalhos de restauro. Clique numa secção/estado no gráfico para ver uma lista de trabalhos com esse estado no separador relatórios. Para cada trabalho, o relatório lista a ID do trabalho, o estado do trabalho, o nome do trabalho e as horas de início e fim do trabalho. O nome do trabalho inclui o nome da cópia Snapshot. Por exemplo: `Restore Backup <snapshot-copy-name>` Você pode baixar a tabela Relatório em formato HTML ou CSV. Também pode transferir os registos de trabalhos do Monitor de trabalhos para todos os trabalhos (não apenas os trabalhos do relatório).

Tipo de relatório	Descrição
Último Status de proteção de VMs ou relatórios de datastores	Exibe informações gerais sobre o status de proteção, durante o número de dias configurado, para VMs e datastores gerenciados pelo plug-in SnapCenter VMware. O padrão é 7 dias. Para modificar o valor no arquivo de propriedades, "Modifique os valores padrão de configuração"consulte . Clique em uma seção/status no gráfico de proteção primária para ver uma lista de VMs ou datastores com esse status na guia **relatórios**. O Relatório de Status da proteção de VM ou datastores para VMs e datastores protegidos exibe os nomes das VMs ou datastores que foram copiados durante o número de dias configurado, o nome da cópia Snapshot mais recente e os horários de início e término da execução mais recente do backup. O Relatório de Status de proteção de VM ou datastores para VMs ou datastores desprotegidos exibe os nomes de VMs ou datastores que não têm backups bem-sucedidos durante o número de dias configurado. Você pode fazer o download da tabela Relatório em formato HTML ou CSV. Também pode transferir os registos de trabalhos do Monitor de trabalhos para todos os trabalhos (não apenas os trabalhos do 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 recentemente copiados.

Gere um pacote de suporte a partir do plug-in do SnapCenter para a GUI do VMware vSphere

Antes de começar

Para fazer logon na GUI de gerenciamento do plug-in do SnapCenter para VMware vSphere, você deve saber o endereço IP e as credenciais de login. Você também deve anotar o token MFA gerado a partir do console de manutenção.

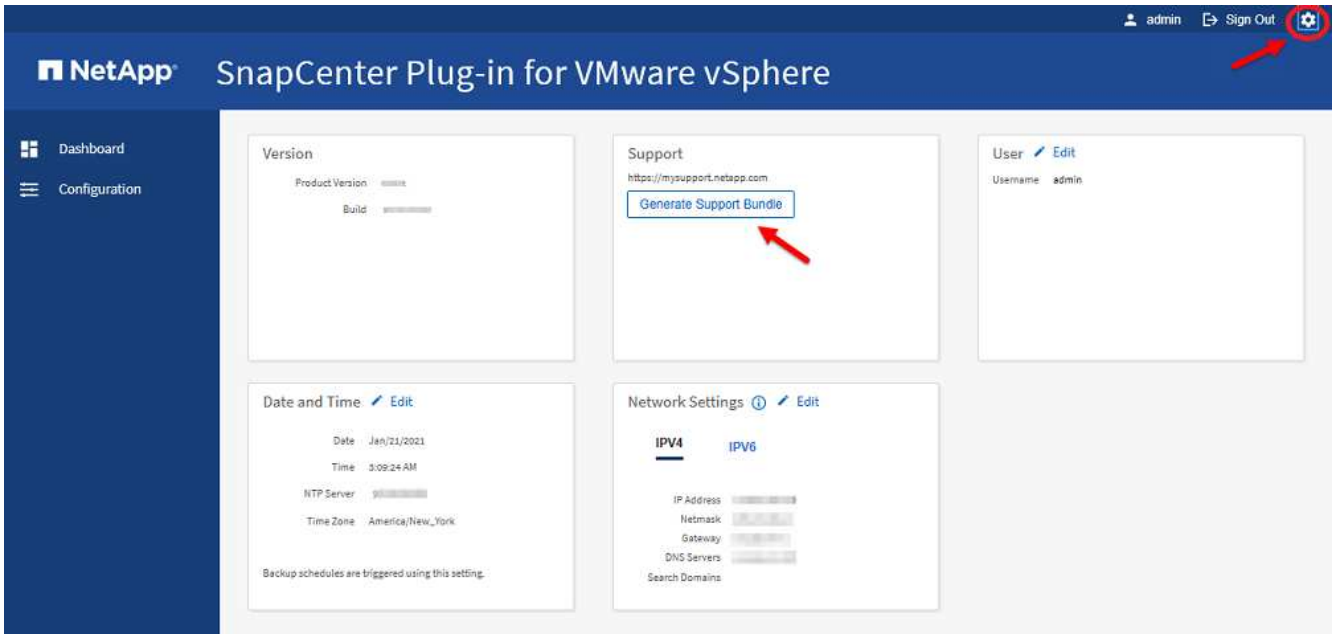
- O endereço IP foi exibido quando o plug-in SnapCenter VMware foi implantado.
- Use as credenciais de login fornecidas durante a implantação do plug-in SnapCenter VMware ou conforme modificado posteriormente.
- Gere um token MFA de 6 dígitos usando as opções de configuração do sistema do console de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

Passos

1. Faça login no plug-in do SnapCenter para a GUI do VMware vSphere.

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

2. Clique no ícone Configurações na barra de ferramentas superior.



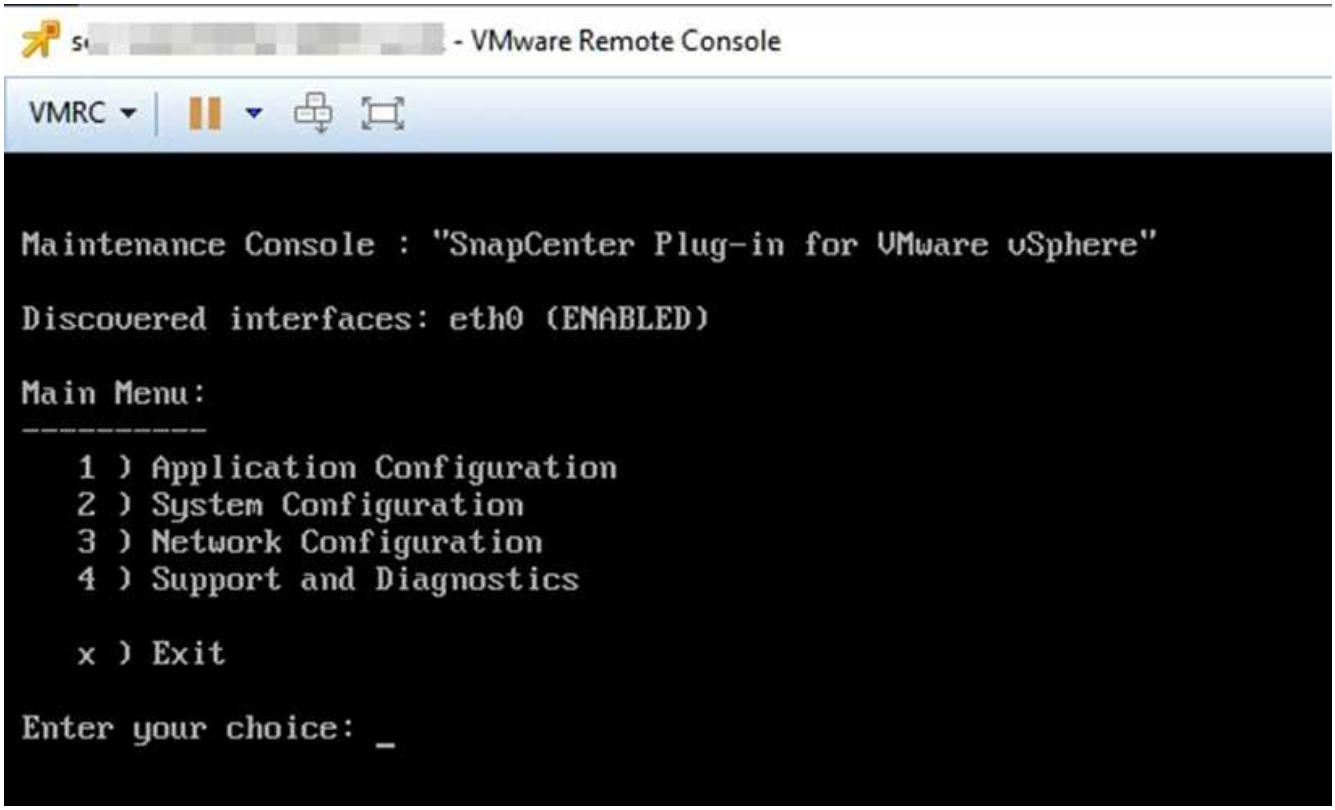
3. Na página **Configurações**, na seção **suporte**, clique em **gerar suporte** Bundle.
4. Depois que o pacote de suporte for gerado, clique no link fornecido para fazer o download do pacote para o NetApp.

Gere um pacote de suporte a partir do console de manutenção

Passos

1. No cliente VMware vSphere, selecione a VM onde o plug-in SnapCenter VMware está localizado.
2. Clique com o botão direito do Mouse na VM e, em seguida, na guia **Summary** do dispositivo virtual clique em **Launch Remote Console ou Launch Web Console** 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, "Acesse o console de manutenção"consulte .



3. No menu principal, insira 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) Acesso ao Shell de Diagnóstico**. No console, navegue até `/support/support/<bundle_name>.tar.gz`.

Logs de auditoria

Log de auditoria é uma coleção de eventos em uma ordem cronológica, que é gravada em um arquivo dentro do dispositivo. Os arquivos de log de auditoria são gerados no `/var/log/netapp/audit` local e os nomes de arquivo seguem uma das convenções de nomenclatura abaixo:

- Audit.log: Arquivo de log de auditoria ativo que está em uso.
- Audit-%d.log.gz: Rolado sobre o arquivo de log de auditoria. 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 exibir e exportar os detalhes do log de auditoria de **Painel** > **Configurações** > **Logs de auditoria** guia você pode exibir a auditoria de operação nos logs de auditoria. Os logs de auditoria são baixados com o pacote suporte.

Se as configurações de e-mail estiverem configuradas, a SCV enviará uma notificação por e-mail no caso de uma falha na Verificação de integridade do Registro 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

- Um máximo de 10 arquivos de log de auditoria são mantidos

Para modificar as configurações padrão, adicione um par de valores de chave no /opt/NetApp/scvservice/standalone_Aegis/etc/scbr/scbr.properties e reinicie o scvservice.

As configurações para arquivos de log de auditoria são:

- <xx>, onde xx é o número máximo de arquivos de log de auditoria rolados, por exemplo: AuditMaxROFiles.15.
- <XX>, onde xx é o tamanho do arquivo em MB, por exemplo: AuditLogSize 15MB.

Os logs de auditoria rolados são verificados periodicamente quanto à integridade. O SCV fornece APIs REST para visualizar logs e verificar sua integridade. Uma programação integrada aciona e atribui um dos seguintes Estados de integridade.

Estado	Descrição
ADULTERADO	O conteúdo do arquivo de log de auditoria foi modificado
NORMAL	O arquivo de log de auditoria não foi modificado
ELIMINAÇÃO DE CAPOTAMENTO	- O arquivo de log de auditoria é excluído com base na retenção - por padrão, apenas 10 arquivos são retidos
ELIMINAÇÃO INESPERADA	O arquivo de log de auditoria é excluído
ATIVO	- Arquivo de log de auditoria está em uso - apenas aplicável a audit.log

Os eventos são categorizados em três categorias principais:

- Eventos de proteção de dados
- Eventos da consola de manutenção
- Eventos do Admin Console

Eventos de proteção de dados

Os recursos na SCV são:

- Sistema de storage
- Grupo recursos
- Política
- Backup

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

Recursos	Operações
Sistema de storage	Criado, modificado, excluído
Grupo recursos	Criado, modificado, excluído, suspenso, retomado

Política	Criado, modificado, excluído
Backup	Criado, renomeado, excluído, montado, desmontado, restaurado VMDK, restaurado VM, anexar VMDK, desanexar VMDK, Guest File Restore

Eventos da consola de manutenção

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

1. Iniciar / Parar serviços
2. Alterar nome de utilizador e palavra-passe
3. Altere a senha do MySQL
4. Configure o MySQL Backup
5. Restaure o MySQL Backup
6. Altere a palavra-passe do utilizador 'não'
7. Alterar fuso horário
8. Altere o servidor NTP
9. Desativar o acesso SSH
10. Aumente o tamanho do disco de cadeia
11. Atualização
12. Instalar o VMware Tools (estamos trabalhando para substituir isso por ferramentas Open-vm)
13. Altere as definições do endereço IP
14. Altere as configurações de pesquisa de nome de domínio
15. Alterar rotas estáticas
16. Aceder ao shell de diagnóstico
17. Ative o acesso de diagnóstico remoto

Eventos do Admin Console

As seguintes operações na IU do Admin Console são auditadas:

- Definições
  - Alterar credenciais de administrador
  - Altere o fuso horário
  - Altere o servidor NTP
  - Altere as definições IPv4 / IPv6
- Configuração
  - Altere as credenciais do vCenter
  - Ativação/desativação do plug-in

Configurar servidores syslog

Os logs de auditoria são armazenados no dispositivo e são verificados periodicamente quanto à integridade. O encaminhamento de eventos permite que você obtenha eventos do computador de origem ou encaminhamento e armazene-os 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 Privileges administrador.

Sobre esta tarefa

Esta tarefa ajuda você a configurar o servidor syslog.

Passos

1. Faça login no plug-in do SnapCenter para VMware vSphere.
2. No painel de navegação esquerdo, selecione **Settings** > **Audit Logs** > **Settings**.
3. No painel **Configurações do Registro de auditoria**, selecione **Enviar logs de auditoria para o servidor Syslog**
4. Introduza os seguintes detalhes:
   - IP do servidor syslog
   - Porta do servidor syslog
   - Formato de RFC
   - Certificado do servidor syslog
5. Clique em **SAVE** para salvar as configurações do servidor Syslog.

Alterar as definições do registo de auditoria

Pode alterar as configurações predefinidas das definições de registo.

Antes de começar

Você deve ter Privileges administrador.

Sobre esta tarefa

Esta tarefa ajuda-o a alterar as definições de registo de auditoria predefinidas.

Passos

1. Faça login no plug-in do SnapCenter para VMware vSphere.
2. No painel de navegação esquerdo, selecione **Settings** > **Audit Logs** > **Settings**.
3. No painel **Configurações do Registro de auditoria**, insira o **número de entradas de auditoria** e o **limite de tamanho do log de auditoria** de acordo com suas necessidades.

Informações sobre direitos autorais

Informações sobre marcas comerciais