Gerenciar objetivos de segurança do cluster

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/pt-br/active-iq-unified-manager-918/health-checker/concept_manage_cluster_security_objectives.html on November 13, 2026. Always check docs.netapp.com for the latest.

Índice

Gerenciar objetivos de segurança do cluster . . . 1
Gerencie os objetivos de segurança do cluster no Active IQ Unified Manager . . . 1
Quais critérios de segurança estão sendo avaliados . . . 1
Entenda como o Active IQ Unified Manager avalia os critérios de segurança . . . 1
Compreenda as categorias de conformidade de cluster no Active IQ Unified Manager . . . 2
Entenda as categorias de conformidade de VMs de armazenamento no Active IQ Unified Manager . . . 5
Entenda as categorias de conformidade de volume no Active IQ Unified Manager . . . 6
Saiba mais sobre o status de conformidade do cluster e do SVM no Active IQ Unified Manager . . . 6
Visualize o status de segurança de clusters e VMs de armazenamento no Active IQ Unified Manager . . . 7
Veja o status da segurança em nível de objeto na página Segurança . . . 7
Veja os detalhes de segurança de todos os clusters na página Clusters . . . 8
Veja os detalhes de segurança de todos os clusters na página de VMs de storage . . . 8
Visualize eventos de segurança que podem exigir atualizações de software ou firmware no Active IQ Unified Manager . . . 9
Veja como os clusters gerenciam a autenticação em todos os clusters no Active IQ Unified Manager . . . 9
Veja o status de criptografia de todos os volumes no Active IQ Unified Manager . . . 10
Visualize o status de proteção contra ransomware de todos os volumes e máquinas virtuais de armazenamento no Active IQ Unified Manager . . . 10
Visualize os detalhes de segurança de todos os volumes com detecção anti-ransomware . . . 10
Visualize os detalhes de segurança de todas as VMs de armazenamento com detecção anti-ransomware . . . 11
Visualize todos os eventos de segurança ativos no Active IQ Unified Manager . . . 11
Adicione alertas para eventos de segurança no Active IQ Unified Manager . . . 11
Desative eventos de segurança específicos no Active IQ Unified Manager . . . 12
Visualize eventos de segurança no Active IQ Unified Manager . . . 13

Gerenciar objetivos de segurança do cluster

Gerencie os objetivos de segurança do cluster no Active IQ Unified Manager

O Unified Manager fornece um painel que identifica o nível de segurança dos seus clusters do ONTAP, máquinas virtuais de storage (SVMs) e volumes, com base nas recomendações definidas no *NetApp Security Hardening Guide for ONTAP 9*.

O objetivo do painel de segurança é mostrar quaisquer áreas em que seus clusters ONTAP não estejam em conformidade com as diretrizes recomendadas da NetApp, para que você possa corrigir esses possíveis problemas. Na maioria dos casos, você corrigirá os problemas usando o ONTAP System Manager ou a ONTAP CLI. Sua organização pode não seguir todas as recomendações, portanto, em alguns casos, você não precisará fazer nenhuma alteração.

Consulte o "NetApp Guia de Reforço de Segurança para o ONTAP 9" (TR-4569) para obter recomendações e resoluções detalhadas.

Além de reportar o status de segurança, o Unified Manager também gera eventos de segurança para qualquer cluster ou SVM que apresente violações de segurança. Você pode acompanhar esses problemas na página de inventário do Event Management e configurar alertas para que o seu administrador de storage seja notificado quando novos eventos de segurança ocorrerem.

Para obter mais informações, consulte "Quais critérios de segurança estão sendo avaliados".

Quais critérios de segurança estão sendo avaliados

Entenda como o Active IQ Unified Manager avalia os critérios de segurança

Em geral, os critérios de segurança para seus clusters do ONTAP, máquinas virtuais de storage (SVMs) e volumes são avaliados em relação às recomendações definidas no *NetApp Security Hardening Guide for ONTAP 9*.

Algumas das verificações de segurança incluem:

- se um cluster está usando um método de autenticação seguro, como SAML
- se os clusters interligados têm sua comunicação criptografada
- se uma máquina virtual de storage tem seu log de auditoria ativado
- se seus volumes têm criptografia de software ou de hardware ativada

Consulte os tópicos sobre categorias de conformidade e o "NetApp Guia de Reforço de Segurança para o ONTAP 9" para obter informações detalhadas.

> Os eventos de upgrade relatados pela plataforma do Active IQ também são considerados eventos de segurança. Esses eventos identificam problemas cuja resolução exige que você atualize o software ONTAP, o firmware do nó ou o software do sistema operacional (para avisos de segurança). Esses eventos não são exibidos no painel Segurança, mas estão disponíveis na página de inventário do Gerenciamento de Eventos.

Para obter mais informações, consulte "Gerenciar os objetivos de segurança do cluster".

Compreenda as categorias de conformidade de cluster no Active IQ Unified Manager

Esta tabela descreve os parâmetros de conformidade de segurança do cluster que o Unified Manager avalia, a recomendação da NetApp e se o parâmetro afeta a determinação geral de se o cluster está em conformidade ou não.

Ter SVMs não conformes em um cluster afetará o valor de conformidade do cluster. Portanto, em alguns casos, pode ser necessário corrigir um problema de segurança em uma SVM antes que a segurança do cluster seja considerada em conformidade.

Observe que nem todos os parâmetros listados abaixo aparecem em todas as instalações. Por exemplo, se você não tiver clusters emparelhados ou se tiver desativado o AutoSupport em um cluster, não verá os itens "Emparelhamento de Cluster" ou "AutoSupport HTTPS Transport" na página da interface de usuário.

Parâmetro	Descrição	Recomendação	Afeta a conformidade do cluster
FIPS global	Indica se o modo de conformidade Global FIPS (Federal Information Processing Standard) 140-2 está ativado ou desativado. Quando o FIPS está ativado, o TLSv1 e o SSLv3 são desativados, e somente o TLSv1.1 e o TLSv1.2 são permitidos.	Habilitado	Sim
Telnet	Indica se o acesso Telnet ao sistema está habilitado ou desabilitado. NetApp recomenda o Secure Shell (SSH) para acesso remoto seguro.	Desabilitado	Sim
Configurações SSH inseguras	Indica se o SSH usa cifras inseguras, por exemplo cifras que começam com *cbc.	Não	Sim
Banner de login	Indica se o banner de login está habilitado ou desabilitado para os usuários que acessam o sistema.	Habilitado	Sim

Parâmetro	Descrição	Recomendação	Afeta a conformidade do cluster
Interconexão de clusters	Indica se a comunicação entre clusters emparelhados é criptografada ou não criptografada. A criptografia deve estar configurada nos clusters de origem e de destino para que este parâmetro seja considerado em conformidade.	Criptografado	Sim
Protocolo de Tempo de Rede	Indica se o cluster possui um ou mais servidores NTP configurados. Para redundância e melhor serviço, a NetApp recomenda que você associe pelo menos três servidores NTP ao cluster.	Configurado	Sim
OCSP	A partir da versão 9.14.1, o Active IQ Unified Manager fornece informações de status do Online Certificate Status Protocol (OCSP) no nível da máquina virtual de armazenamento (SVM, anteriormente conhecida como Vserver). Isso significa que a validação de OCSP é aplicada a todas as conexões SSL/TLS feitas com a SVM e garante a integridade e a validade dos certificados usados nessas conexões.	Habilitado	Não
Log de auditoria remoto	Indica se o encaminhamento de logs (Syslog) está criptografado ou não criptografado.	Criptografado	Sim
AutoSupport Transporte HTTPS	Indica se o HTTPS é usado como protocolo de transporte padrão para enviar mensagens do AutoSupport ao suporte da NetApp.	Habilitado	Sim

Parâmetro	Descrição	Recomendação	Afeta a conformidade do cluster
Usuário administrador padrão	Indica se o usuário administrador padrão (incorporado) está ativado ou desativado. NetApp recomenda bloquear (desativar) todas as contas incorporadas desnecessárias.	Desabilitado	Sim
Usuários SAML	Indica se o SAML está configurado. O SAML permite que você configure a autenticação multifator (MFA) como método de login para single sign-on.	Não	Não
Usuários do Active Directory	Indica se o Active Directory está configurado. O Active Directory e o LDAP são os mecanismos de autenticação preferenciais para usuários que acessam clusters.	Não	Não
Usuários LDAP	Indica se o LDAP está configurado. O Active Directory e o LDAP são os mecanismos de autenticação preferenciais para usuários que gerenciam clusters, em comparação com usuários locais.	Não	Não
Usuários de certificado	Indica se um usuário com certificado está configurado para fazer login no cluster.	Não	Não
Usuários locais	Indica se os usuários locais estão configurados para fazer login no cluster.	Não	Não
Shell remoto	Indica se o RSH está habilitado. Por motivos de segurança, o RSH deve ser desabilitado. O Secure Shell (SSH) para acesso remoto seguro é o método preferencial.	Desabilitado	Sim

Parâmetro	Descrição	Recomendação	Afeta a conformidade do cluster
MD5 em uso	Indica se as contas de usuário do ONTAP usam a função de hash MD5, menos segura. A migração das contas de usuário com hash MD5 para uma função de hash criptográfica mais segura, como SHA-512, é recomendada.	Não	Sim
Tipo de emissor do certificado	Indica o tipo de certificado digital utilizado.	Assinado pela CA	Não

Entenda as categorias de conformidade de VMs de armazenamento no Active IQ Unified Manager

Esta tabela descreve os critérios de conformidade de segurança da máquina virtual de armazenamento (SVM) que o Unified Manager avalia, a recomendação da NetApp e se o parâmetro afeta a determinação geral de a SVM estar em conformidade ou não.

Parâmetro	Descrição	Recomendação	Afeta o SVM Compliance
Registro de auditoria	Indica se o registro de auditoria está ativado ou desativado.	Habilitado	Sim
Configurações SSH inseguras	Indica se o SSH usa cifras inseguras, por exemplo cifras que começam com `cbc*`.	Não	Sim
Banner de login	Indica se o banner de login está habilitado ou desabilitado para usuários que acessam SVMs no sistema.	Habilitado	Sim
Criptografia LDAP	Indica se a criptografia LDAP está ativada ou desativada.	Habilitado	Não
Autenticação NTLM	Indica se a autenticação NTLM está ativada ou desativada.	Habilitado	Não
Assinatura de carga útil LDAP	Indica se a assinatura de payload LDAP está ativada ou desativada.	Habilitado	Não
Configurações CHAP	Indica se o CHAP está ativado ou desativado.	Habilitado	Não

Parâmetro	Descrição	Recomendação	Afeta o SVM Compliance
Kerberos V5	Indica se a autenticação Kerberos V5 está ativada ou desativada.	Habilitado	Não
Autenticação NIS	Indica se o uso da autenticação NIS está configurado.	Desabilitado	Não
Status ativo do FPolicy	Indica se a FPolicy foi criada ou não.	Sim	Não
Criptografia SMB ativada	Indica se o SMB -Signing & Sealing não está ativado.	Sim	Não
Assinatura SMB ativada	Indica se o SMB -Signing não está habilitado.	Sim	Não

Entenda as categorias de conformidade de volume no Active IQ Unified Manager

Esta tabela descreve os parâmetros de criptografia de volume que o Unified Manager avalia para determinar se os dados em seus volumes estão adequadamente protegidos contra o acesso de usuários não autorizados.

Observe que os parâmetros de criptografia do volume não afetam se o cluster ou a máquina virtual de armazenamento é considerado compatível.

Parâmetro	Descrição
Criptografado por software	Exibe o número de volumes protegidos usando as soluções de criptografia por software NetApp Volume Encryption (NVE) ou NetApp Aggregate Encryption (NAE).
Criptografado por hardware	Exibe o número de volumes protegidos usando a criptografia de hardware NetApp Storage Encryption (NSE).
Criptografia de software e hardware	Exibe o número de volumes protegidos por criptografia de software e de hardware.
Não criptografado	Exibe o número de volumes que não estão criptografados.

Saiba mais sobre o status de conformidade do cluster e do SVM no Active IQ Unified Manager

Clusters e máquinas virtuais de armazenamento (SVMs) são considerados não conformes quando qualquer um dos critérios de segurança avaliados em relação às recomendações definidas no *Guia de Reforço de Segurança da NetApp para ONTAP 9* não for atendido. Além disso, um cluster é considerado não conforme quando qualquer SVM for sinalizada como não conforme.

Os ícones de status nos cartões de segurança têm os seguintes significados em relação à sua conformidade:

- - O parâmetro está configurado conforme recomendado.
- - O parâmetro não está configurado conforme recomendado.
- - Ou a funcionalidade não está habilitada no cluster, ou o parâmetro não está configurado conforme recomendado, mas esse parâmetro não contribui para a conformidade do objeto.

Observe que o status de criptografia do volume não contribui para determinar se o cluster ou a SVM são considerados em conformidade.

Visualize o status de segurança de clusters e VMs de armazenamento no Active IQ Unified Manager

O Active IQ Unified Manager permite visualizar o status de segurança dos objetos de armazenamento no seu ambiente a partir de diferentes pontos da interface. Você pode coletar e analisar informações e relatórios com base em parâmetros definidos e detectar comportamentos suspeitos ou alterações não autorizadas no sistema em clusters e máquinas virtuais de storage monitorados.

Para obter recomendações de segurança, consulte o "NetApp Guia de Reforço de Segurança para o ONTAP 9"

Veja o status da segurança em nível de objeto na página Segurança

Como administrador do sistema, você pode usar a página **Segurança** para ter visibilidade da robustez da segurança dos seus clusters do ONTAP e VMs de storage nos níveis de data center e site. Os objetos suportados são cluster, VMs de storage e volumes. Siga estes passos:

Passos

1. No painel de navegação esquerdo, clique em **Dashboard**.
2. Dependendo de você querer visualizar o status de segurança de todos os clusters monitorados ou de um único cluster, selecione **Todos os Clusters** ou selecione um único cluster no menu suspenso.
3. Clique na seta para a direita no painel **Security**. A página Security é exibida.

Clicar nos gráficos de barras, contagens e `View Reports` links leva você à página de Volumes, Clusters ou Storage VMs, onde você pode visualizar os detalhes correspondentes ou gerar relatórios, conforme necessário.

A página de Segurança exibe os seguintes painéis:

- **Conformidade do cluster**: o status de segurança (número de clusters que estão em conformidade ou fora de conformidade) de todos os clusters em um data center
- **Conformidade de VMs de armazenamento**: o status de segurança (número de VMs de armazenamento que estão em conformidade ou não estão em conformidade) para todas as VMs de armazenamento no seu data center
- **Criptografia de volume**: o status da criptografia de todos os volumes no seu ambiente (número de volumes criptografados ou não criptografados)
- **Status de anti-ransomware do volume**: o status de segurança (número de volumes com anti-ransomware ativado ou desativado) de todos os volumes em seu ambiente

- **Autenticação e certificados de cluster**: o número de clusters que usam cada tipo de método de autenticação, como SAML, Active Directory ou por meio de certificados e autenticação local. O painel também exibe o número de clusters cujos certificados expiraram ou estão prestes a expirar em 60 dias.

Veja os detalhes de segurança de todos os clusters na página Clusters

A página de detalhes **Clusters / Segurança** permite que você visualize o status de conformidade de segurança no nível do cluster.

Passos

1. No painel de navegação esquerdo, clique em **Storage > Clusters**.
2. Selecione **Exibir > Segurança > Todos os clusters**.

São exibidos os parâmetros de segurança padrão, como FIPS global, Telnet, configurações inseguras de SSH, banner de login, protocolo de tempo de rede, transporte HTTPS do AutoSupport e o status de expiração do certificado do cluster.

Você pode clicar no botão "mais opções" e escolher visualizar os detalhes de segurança na página **Security** do Unified Manager ou no System Manager. Você precisa ter credenciais válidas para visualizar os detalhes no System Manager.

Se um cluster tiver um certificado expirado, você pode clicar `expired` em **Validade do Certificado do Cluster** e renová-lo no System Manager (9.10.1 e posterior). Não é possível clicar `expired` se a instância do System Manager for de uma versão anterior à 9.10.1.

Veja os detalhes de segurança de todos os clusters na página de VMs de storage

A página de detalhes **VMs de armazenamento / Segurança** permite que você visualize o status de conformidade de segurança no nível de uma VM de armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > VMs de storage**.
2. Selecione **Exibir > Segurança > Todas as VMs de armazenamento**. Uma lista de clusters com os parâmetros de segurança é exibida.

Você pode ter uma visão padrão da conformidade de segurança das VMs de storage verificando os parâmetros de segurança, como VMs de storage, cluster, banner de login, log de auditoria e configurações de SSH inseguras.

Você pode clicar no botão "mais opções" e escolher visualizar os detalhes de segurança na página **Security** do Unified Manager ou no System Manager. Você precisa ter credenciais válidas para visualizar os detalhes no System Manager.

Para obter detalhes de segurança anti-ransomware para volumes e VMs de storage, consulte "Visualizando o status do anti-ransomware de todos os volumes e VMs de storage".

Visualize eventos de segurança que podem exigir atualizações de software ou firmware no Active IQ Unified Manager

Existem determinados eventos de segurança que têm como área de impacto “Atualização”. Esses eventos são relatados pela plataforma Active IQ e identificam problemas cuja resolução exige que você atualize o software ONTAP, o firmware do nó ou o software do sistema operacional (para avisos de segurança).

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Você pode querer tomar medidas corretivas imediatas para alguns desses problemas, enquanto outros podem esperar até a próxima manutenção programada. Você pode visualizar todos esses eventos e atribuí-los aos usuários que podem resolver os problemas. Além disso, se houver determinados eventos de atualização de segurança sobre os quais você não deseja ser notificado, esta lista pode ajudar você a identificá-los para que você possa desativá-los.

Passos

1. No painel de navegação à esquerda, clique em **Event Management**.

   Por padrão, todos os eventos ativos (novos e confirmados) são exibidos na página de inventário do Gerenciamento de Eventos.

2. No menu Exibir, selecione **Eventos de atualização**.

   A página exibe todos os eventos de segurança de atualização ativos.

Veja como os clusters gerenciam a autenticação em todos os clusters no Active IQ Unified Manager

A página Security exibe os tipos de autenticação usados para autenticar usuários em cada cluster e o número de usuários que acessam o cluster usando cada tipo. Isso permite que você verifique se a autenticação está sendo realizada de forma segura, conforme definido pela sua organização.

Passos

1. No painel de navegação esquerdo, clique em **Dashboard**.
2. Na parte superior do painel de controle, selecione **Todos os Clusters** no menu suspenso.
3. Clique na seta para a direita no painel **Segurança** e a página **Segurança** é exibida.
4. Consulte o cartão **Cluster Authentication** para ver o número de usuários que acessam o sistema usando cada tipo de autenticação.
5. Consulte o cartão **Segurança do Cluster** para ver os mecanismos de autenticação usados para autenticar usuários em cada cluster.

Se houver usuários acessando o sistema por meio de um método inseguro ou de um método não recomendado pela NetApp, você pode desativar esse método.

Veja o status de criptografia de todos os volumes no Active IQ Unified Manager

Você pode visualizar uma lista de todos os volumes e seus respectivos status atuais de criptografia para determinar se os dados em seus volumes estão adequadamente protegidos contra o acesso por usuários não autorizados.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Os tipos de criptografia que podem ser aplicados a um volume são:

- Software: volumes protegidos usando as soluções de criptografia de software NetApp Volume Encryption (NVE) ou NetApp Aggregate Encryption (NAE).
- Hardware: volumes protegidos usando criptografia de hardware do NetApp Storage Encryption (NSE).
- Software e hardware: volumes protegidos por criptografia de software e de hardware.
- Nenhum: volumes que não estão criptografados.

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. No menu Exibir, selecione **Saúde** > **Criptografia de volumes**
3. Na visualização **Health: Volumes Encryption**, classifique pelo campo **Encryption Type** ou use o filtro para exibir volumes que tenham um tipo de criptografia específico ou que não estejam criptografados (**Encryption Type** de “None”).

Visualize o status de proteção contra ransomware de todos os volumes e máquinas virtuais de armazenamento no Active IQ Unified Manager

Você pode visualizar uma lista de todos os volumes e máquinas virtuais de storage (SVMs) e seu status atual contra ransomware, para determinar se os dados em seus volumes e SVMs estão adequadamente protegidos contra ataques de ransomware.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Para obter mais informações sobre os diferentes status de anti-ransomware, consulte "O ONTAP: ativar a proteção contra ransomware".

Visualize os detalhes de segurança de todos os volumes com detecção anti-ransomware

Passos

1. No painel de navegação à esquerda, clique em **Armazenamento** > **Volumes**.
2. No menu Exibir, selecione **Integridade** > **Segurança** > **Anti-ransomware**
3. Na visualização **Segurança: anti-ransomware**, você pode ordenar pelos vários campos ou usar o filtro.

A proteção contra ransomware não é compatível com volumes offline, volumes restritos, volumes SnapLock, volumes FlexGroup, volumes FlexCache, volumes somente SAN, volumes de VMs de storage interrompidas, volumes raiz de VMs de storage ou volumes de proteção de dados.

Visualize os detalhes de segurança de todas as VMs de armazenamento com detecção anti-ransomware

Passos

1. No painel de navegação esquerdo, clique em **Armazenamento > VMs de storage**.
2. Selecione **Exibir > Segurança > Antiransomware**. Uma lista de SVMs com o status de antiransomware é exibida.

O monitoramento anti-ransomware não é suportado em máquinas virtuais de storage que não têm o protocolo NAS ativado.

Visualize todos os eventos de segurança ativos no Active IQ Unified Manager

Você pode visualizar todos os eventos de segurança ativos e, em seguida, atribuir cada um deles a um usuário que possa resolver o problema. Além disso, se houver determinados eventos de segurança que você não deseja receber, esta lista pode ajudar você a identificar os eventos que deseja desativar.

Antes de começar

Você precisa ter a função de Operador, Administrador de Aplicativos ou administrador de storage.

Passos

1. No painel de navegação à esquerda, clique em **Event Management**.

   Por padrão, os eventos Novos e Reconhecidos são exibidos na página de inventário de gerenciamento de eventos.

2. No menu Exibir, selecione **eventos de segurança ativos**.

   A página exibe todos os eventos de segurança novos e reconhecidos gerados nos últimos 7 dias.

Adicione alertas para eventos de segurança no Active IQ Unified Manager

Você pode configurar alertas para eventos de segurança individuais, assim como para qualquer outro evento recebido pelo Unified Manager. Além disso, se desejar tratar todos os eventos de segurança da mesma forma e enviar e-mails para a mesma pessoa, você pode criar um único alerta para que você seja notificado quando qualquer evento de segurança for acionado.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

O exemplo abaixo mostra como criar um alerta para o evento de segurança “Telnet Protocol Enabled”. Isso enviará um alerta se o acesso Telnet estiver configurado para acesso administrativo remoto no cluster. Você pode usar essa mesma metodologia para criar alertas para todos os eventos de segurança.

Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento** > **Configuração de alertas**.
2. Na página **Alert Setup**, clique em **Add**.
3. Na caixa de diálogo **Adicionar Alerta**, clique em **Nome** e insira um nome e uma descrição para o alerta.
4. Clique em **Recursos** e selecione o cluster ou o cluster no qual você deseja ativar este alerta.
5. Clique em **Eventos** e execute as seguintes ações:
   a. Na lista de gravidade do evento, selecione **Aviso**.
   b. Na lista de eventos correspondentes, selecione **Telnet Protocol Enabled**.
6. Clique em **Ações** e selecione o nome do usuário que receberá o e-mail de alerta no campo **Alertar estes usuários**.
7. Configure outras opções nesta página para a frequência de notificação, a emissão de traps SNMP e a execução de um script.
8. Clique em **Salvar**.

Desative eventos de segurança específicos no Active IQ Unified Manager

Todos os eventos estão ativados por padrão. Você pode desativar eventos específicos para impedir a geração de notificações para aqueles que não são importantes no seu ambiente. Você pode ativar eventos desativados se desejar voltar a receber notificações para eles.

Antes de começar

Você precisa ter a função de Application Administrator ou Storage Administrator.

Ao desativar eventos, os eventos gerados anteriormente no sistema são marcados como obsoletos e os alertas configurados para esses eventos não são acionados. Ao ativar eventos desativados, as notificações para esses eventos são geradas a partir do próximo ciclo de monitoramento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração de eventos**.
2. Na página **Event** Setup, desative ou ative eventos escolhendo uma das seguintes opções:

Se você quiser…	Então faça isso…
Desativar eventos	a. Clique em **Desativar**. b. Na caixa de diálogo Disable Events, selecione a gravidade **Warning**. Esta é a categoria para todos os eventos de segurança. c. Na coluna Eventos correspondentes, selecione os eventos de segurança que deseja desativar e clique na seta para a direita para movê-los para a coluna Desativar eventos. d. Clique em **Salvar e fechar**. e. Verifique se os eventos que você desativou são exibidos na exibição em lista da página Configuração de Eventos.
Ativar eventos	a. Na lista de eventos desativados, selecione a caixa de seleção do evento, ou dos eventos, que você deseja reativar. b. Clique em **Enable**.

Visualize eventos de segurança no Active IQ Unified Manager

Os eventos de segurança fornecem a você informações sobre o status de segurança dos clusters do ONTAP, das máquinas virtuais de storage (SVMs) e dos volumes, com base nos parâmetros definidos no *NetApp Security Hardening Guide for ONTAP 9*. Esses eventos notificam você sobre possíveis problemas para que você possa avaliar a gravidade deles e corrigir o problema, se necessário.

Os eventos de segurança são agrupados por tipo de origem e incluem o nome do evento e do trap, o nível de impacto e a gravidade. Esses eventos aparecem nas categorias de eventos do cluster e da storage VM.

Informações sobre direitos autorais

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

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

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE 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.