Gerenciamento dos objetivos de segurança do cluster

Active IQ Unified Manager 9.7

NetApp
October 22, 2024

Índice

Gerenciamento dos objetivos de segurança do cluster

O Unified Manager fornece um dashboard que identifica a segurança dos clusters do ONTAP, das máquinas virtuais de storage (SVMs) e dos volumes com base nas recomendações definidas no *Guia de endurecimento de segurança do NetApp para ONTAP 9*.

O objetivo do dashboard de segurança é mostrar todas as áreas em que os clusters do ONTAP não estejam alinhados às diretrizes recomendadas do NetApp para que você possa corrigir esses possíveis problemas. Na maioria dos casos, você corrigirá os problemas usando o Gerenciador de sistema do ONTAP ou a CLI do ONTAP. Sua organização pode não seguir todas as recomendações, então, em alguns casos, você não precisará fazer alterações.

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

Além de informar o status de segurança, o Unified Manager também gera eventos de segurança para qualquer cluster ou SVM que tenha violações de segurança. Você pode rastrear esses problemas na página de inventário do Gerenciamento de Eventos e configurar alertas para esses eventos para que o administrador de armazenamento seja notificado quando novos eventos de segurança ocorrerem.

Quais critérios de segurança estão sendo avaliados

Em geral, os critérios de segurança dos clusters do ONTAP, das máquinas virtuais de armazenamento (SVMs) e dos volumes estão sendo avaliados em relação às recomendações definidas no *Guia de endurecimento de Segurança do NetApp para ONTAP 9*.

Algumas das verificações de segurança incluem:

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

Consulte os tópicos sobre categorias de conformidade e o "Guia de endurecimento de segurança da NetApp para ONTAP 9" para obter informações detalhadas.

> Os eventos de atualização que são relatados da plataforma Active IQ também são considerados eventos de segurança. Esses eventos identificam problemas em que a 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.

Categorias de conformidade de cluster

Esta tabela descreve os parâmetros de conformidade de segurança do cluster que o

Unified Manager avalia, a recomendação do NetApp e se o parâmetro afeta a determinação geral do cluster que está sendo queixa ou não.

Ter SVMs não compatíveis em um cluster afetará o valor de conformidade do cluster. Então, em alguns casos, você pode precisar corrigir problemas de segurança com um SVM antes que a segurança do cluster seja considerada em conformidade.

Note que nem todos os parâmetros listados abaixo aparecem para todas as instalações. Por exemplo, se você não tiver clusters com peering ou se tiver desabilitado o AutoSupport em um cluster, não verá os itens de emparelhamento de cluster ou Transporte HTTPS AutoSupport na página da IU.

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, TLSv1 e SSLv3 são desativados e apenas TLSv1,1 e TLSv1,2 são permitidos.	Ativado	Sim
Telnet	Indica se o acesso Telnet ao sistema está ativado ou desativado. A NetApp recomenda o Shell seguro (SSH) para acesso remoto seguro.	Desativado	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 Login está ativado ou desativado para os usuários que acessam o sistema.	Ativado	Sim

Parâmetro	Descrição	Recomendação	Afeta a conformidade do cluster
Peering de clusters	Indica se a comunicação entre clusters com permissões está encriptada ou não encriptada. A criptografia deve ser configurada nos clusters de origem e destino para que esse parâmetro seja considerado compatível.	Encriptado	Sim
Protocolo de hora de rede	Indica se o cluster tem 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	Indica se existem aplicações no ONTAP que não estão configuradas com OCSP (Protocolo de estado de certificado online) e, por conseguinte, as comunicações não estão encriptadas. As aplicações não compatíveis estão listadas.	Ativado	Não
Registo de auditoria remota	Indica se o encaminhamento de registos (Syslog) está encriptado ou não encriptado.	Encriptado	Sim
Transporte AutoSupport HTTPS	Indica se o HTTPS é usado como o protocolo de transporte padrão para enviar mensagens AutoSupport ao suporte do NetApp.	Ativado	Sim

Parâmetro	Descrição	Recomendação	Afeta a conformidade do cluster
Usuário Administrador padrão	Indica se o Usuário Admin padrão (interno) está ativado ou desativado. A NetApp recomenda bloquear (desativar) quaisquer contas internas desnecessárias.	Desativado	Sim
Usuários SAML	Indica se o SAML está configurado. O SAML permite configurar a autenticação multifator (MFA) como um método de login para logon único.	Sem recomendações	Não
Usuários do ative Directory	Indica se o ative Directory está configurado. O ative Directory e o LDAP são os mecanismos de autenticação preferenciais para usuários que acessam clusters.	Sem recomendações	Não
Utilizadores LDAP	Indica se o LDAP está configurado. O ative Directory e o LDAP são os mecanismos de autenticação preferidos para usuários que gerenciam clusters em usuários locais.	Sem recomendações	Não
Usuários de certificados	Indica se um utilizador de certificado está configurado para iniciar sessão no cluster.	Sem recomendações	Não
Usuários locais	Indica se os utilizadores locais estão configurados para iniciar sessão no cluster.	Sem recomendações	Não

Categorias de conformidade do SVM

Esta tabela descreve os critérios de conformidade de segurança da máquina virtual de storage (SVM) avaliados pelo Unified Manager, a recomendação do NetApp e se o parâmetro afeta a determinação geral da reclamação ou não da SVM.

Parâmetro	Descrição	Recomendação	Diz respeito à conformidade com o SVM
Registo de auditoria	Indica se o registo de auditoria está ativado ou desativado.	Ativado	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 Login está ativado ou desativado para usuários que acessam SVMs no sistema.	Ativado	Sim
Encriptação LDAP	Indica se a encriptação LDAP está ativada ou desativada.	Ativado	Não
Autenticação NTLM	Indica se a autenticação NTLM está ativada ou desativada.	Ativado	Não
Assinatura de carga útil LDAP	Indica se a assinatura de carga útil LDAP está ativada ou desativada.	Ativado	Não
Definições CHAP	Indica se o CHAP está ativado ou desativado.	Ativado	Não
Kerberos V5	Indica se a autenticação Kerberos V5 está ativada ou desativada.	Ativado	Não

Categorias de conformidade de volume

Esta tabela descreve os parâmetros de criptografia de volume avaliados pelo Unified Manager para determinar se os dados nos volumes estão protegidos adequadamente contra o acesso de usuários não autorizados.

Observe que os parâmetros de criptografia de volume não afetam se o cluster ou a VM de armazenamento são considerados compatíveis.

Parâmetro	Descrição
Software criptografado	Exibe o número de volumes protegidos usando as soluções de criptografia de software de criptografia de volume NetApp (NVE) ou NetApp Aggregate Encryption (NAE).
Hardware criptografado	Exibe o número de volumes protegidos usando criptografia de hardware do NetApp Storage Encryption (NSE).
Software e hardware criptografados	Exibe o número de volumes protegidos pela criptografia de software e hardware.
Não encriptado	Exibe o número de volumes que não são criptografados.

O que não está em conformidade significa

Os clusters e as máquinas virtuais de armazenamento (SVMs) são considerados não compatíveis quando nenhum dos critérios de segurança que está sendo avaliado em relação às recomendações definidas no *Guia de endurecimento de Segurança do NetApp para ONTAP 9* não for atendido. Além disso, um cluster é considerado não compatível quando qualquer SVM é sinalizado como não compatível.

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

- - O parâmetro é configurado como recomendado.
- - O parâmetro não está configurado como recomendado.
- - Ou a funcionalidade não está ativada no cluster, ou o parâmetro não está configurado como recomendado, mas este parâmetro não contribui para a conformidade do objeto.

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

Visualização do status de segurança de cluster de alto nível

O painel Segurança no Unified ManagerDashboard mostra o status de segurança de alto nível para todos os clusters ou para um único cluster, dependendo da exibição atual.

Passos

1. No painel de navegação esquerdo, clique em **Dashboard**.
2. Dependendo se você deseja exibir o status de segurança para todos os clusters monitorados ou para um único cluster, selecione **todos os clusters** ou selecione um único cluster no menu suspenso.
3. Veja o painel **Security** para ver o status geral.

Este painel apresenta:

- uma lista dos eventos de segurança recebidos nas últimas 24 horas
- Um link de cada um desses eventos para a página de detalhes do evento
- Um link para que você possa exibir todos os eventos de segurança ativos na página de inventário do Gerenciamento de Eventos
- o status de segurança do cluster (número de clusters que estão em conformidade ou não estão em conformidade)
- O status de segurança da SVM (número de SVMs em conformidade ou não em conformidade)
- o status da criptografia de volume (número de volumes criptografados ou não criptografados)

4. Clique na seta para a direita na parte superior do painel para ver os detalhes de segurança na página **Segurança**.

Visualização do status de segurança detalhado para clusters e SVMs

A página Segurança mostra o status de segurança de alto nível para todos os clusters e o status de segurança detalhado para clusters individuais. O status detalhado do cluster inclui conformidade de cluster, conformidade com SVM e conformidade de criptografia de volumes.

Passos

1. No painel de navegação esquerdo, clique em **Dashboard**.
2. Dependendo se você deseja exibir o status de segurança para todos os clusters monitorados ou para um único cluster, selecione **todos os clusters** ou selecione um único cluster no menu suspenso.
3. Clique na seta para a direita no painel **Segurança**.

   A página Segurança exibe as seguintes informações:

   - o status de segurança do cluster (número de clusters que estão em conformidade ou não estão em conformidade)
   - O status de segurança da SVM (número de SVMs em conformidade ou não em conformidade)
   - o status da criptografia de volume (número de volumes criptografados ou não criptografados)
   - os métodos de autenticação de cluster que estão sendo usados em cada cluster
4. Consulte o "Guia de endurecimento de segurança da NetApp para ONTAP 9" para obter instruções sobre como tornar todos os clusters, SVMs e volumes compatíveis com as recomendações de segurança da NetApp.

Exibição de eventos de segurança que podem exigir atualizações de software ou firmware

Existem certos eventos de segurança que têm uma área de impactos do "Upgrade". Esses eventos são relatados da plataforma Active IQ e identificam problemas em que a 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

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Sobre esta tarefa

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

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos**.

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

2. No menu Exibir, selecione **Atualizar eventos**.

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

Visualização de como a autenticação do usuário está sendo gerenciada em todos os clusters

A página Segurança exibe os tipos de autenticação que estão sendo usados para autenticar usuários em cada cluster e o número de usuários que estão acessando o cluster usando cada tipo. Isso permite verificar se a autenticação do usuário está sendo executada de forma segura, conforme definido pela sua organização.

Passos

1. No painel de navegação esquerdo, clique em **Dashboard**.
2. Na parte superior do painel, selecione **todos os clusters** no menu suspenso.
3. Clique na seta para a direita no painel **Segurança** e a página **Segurança** será exibida.
4. Exiba o cartão **Cluster Authentication** para ver o número de usuários que estão acessando o sistema usando cada tipo de autenticação.
5. Exiba o cartão **Cluster Security** para exibir os mecanismos de autenticação que estão sendo usados para autenticar usuários em cada cluster.

Resultados

Se houver alguns usuários acessando o sistema usando um método inseguro ou usando um método que não é recomendado pelo NetApp, você pode desativar o método.

Exibindo o status de criptografia de todos os volumes

Você pode exibir uma lista de todos os volumes e seu status de criptografia atual para determinar se os dados em seus volumes estão adequadamente protegidos contra o acesso de usuários não autorizados.

Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Sobre esta tarefa

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

- Software - volumes protegidos com as soluções de criptografia de software NVE (NetApp volume Encryption) ou NetApp Aggregate Encryption (NAE).
- Hardware - volumes que são protegidos com a criptografia de hardware do NetApp Storage Encryption (NSE).
- Software e hardware - volumes protegidos pela criptografia de software e hardware.
- Nenhum - volumes que não são criptografados.

Passos

1. No painel de navegação esquerdo, clique em **Storage** > **volumes**.
2. No menu **View**, selecione **Health** > **volumes Encryption**
3. Na exibição **Health: Volumes Encryption**, classifique no campo **Encryption Type** ou use o filtro para exibir volumes que tenham um tipo de criptografia específico ou que não estejam criptografados (Encryption Type of "'None'").

Visualizar todos os eventos de segurança ativos

Você pode exibir todos os eventos de segurança ativos e, em seguida, atribuir cada um deles a um usuário que pode resolver o problema. Além disso, se houver certos eventos de segurança que você não deseja receber, esta lista pode ajudá-lo a identificar os eventos que deseja desativar.

Antes de começar

Tem de ter a função Operador, Administrador de aplicações ou Administrador de armazenamento.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de eventos**.

   Por padrão, eventos novos e confirmados são exibidos na página de inventário do Gerenciamento de Eventos.

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

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

Adicionar alertas para eventos de segurança

Você pode configurar alertas para eventos de segurança individuais, como qualquer outro evento recebido pelo Unified Manager. Além disso, se você quiser tratar todos os eventos de segurança da mesma forma e mandar e-mails para a mesma pessoa, você pode criar um único alerta para notificá-lo quando quaisquer eventos de segurança forem acionados.

Antes de começar

Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

Sobre esta tarefa

O exemplo abaixo mostra como criar um alerta para o evento de segurança ""Protocolo Telnet ativado"". Isso enviará um alerta se o acesso Telnet estiver configurado para acesso administrativo remoto ao cluster. Você pode usar essa mesma metodologia para criar alertas para todos os eventos de segurança.

Passos

1. No painel de navegação esquerdo, clique em **Gerenciamento de armazenamento** > **Configuração de alerta**.
2. Na página **Configuração de alerta**, clique em **Adicionar**.
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 cluster no qual deseja ativar esse alerta.
5. Clique em **Eventos** e execute as seguintes ações:
   a. Na lista gravidade do evento, selecione **Aviso**.
   b. Na lista Eventos correspondentes, selecione **Protocolo Telnet ativado**.
6. Clique em **ações** e selecione o nome do usuário que receberá o e-mail de alerta no campo **alertar esses usuários**.
7. Configure quaisquer outras opções nesta página para frequência de notificação, emissão de toques SNMP e execução de um script.
8. Clique em **Salvar**.

Desativar eventos de segurança específicos

Todos os eventos são ativados por padrão. Você pode desativar eventos específicos para impedir a geração de notificações para os eventos que não são importantes em seu ambiente. Você pode ativar eventos desativados se quiser retomar o recebimento de notificações para eles.

Antes de começar

Tem de ter a função Administrador de aplicações ou Administrador de armazenamento.

Sobre esta tarefa

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

Passos

1. No painel de navegação à esquerda, clique em **Gerenciamento de armazenamento** > **Configuração do evento**.
2. Na página **Configuração do evento**, 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 Desativar eventos, selecione a gravidade **Aviso**. 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 mover esses eventos para a coluna Desativar eventos. d. Clique em **Salvar e fechar**. e. Verifique se os eventos desativados são apresentados na vista de lista da página Configuração de eventos.
Ativar eventos	a. Na lista de eventos desativados, marque a caixa de seleção do evento ou eventos que deseja reativar. b. Clique em **Ativar**.

Eventos de segurança

Os eventos de segurança fornecem informações sobre o status de segurança de clusters do ONTAP, máquinas virtuais de armazenamento (SVMs) e volumes com base nos parâmetros definidos no *Guia de endurecimento de Segurança do NetApp para 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 da armadilha, o nível de impactos e a gravidade. Esses eventos aparecem nas categorias de eventos de VM de armazenamento e cluster.

Informações sobre direitos autorais

Informações sobre marcas comerciais