



Quais critérios de segurança estão sendo avaliados

Active IQ Unified Manager 9.10

NetApp
January 31, 2025

Índice

- Quais critérios de segurança estão sendo avaliados..... 1
 - Categorias de conformidade de cluster 1
 - Categorias de conformidade de VM de storage..... 5
 - Categorias de conformidade de volume 6

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 |
| 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 |

| Parâmetro | Descrição | Recomendação | Afeta a conformidade do cluster |
|------------------------------|--|---------------------|--|
| 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 |
| 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 |

| Parâmetro | Descrição | Recomendação | Afeta a conformidade do cluster |
|-----------------------------|---|---------------------|--|
| Usuários SAML | Indica se o SAML está configurado. O SAML permite configurar a autenticação multifator (MFA) como um método de login para logon único. | Não | 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. | Não | 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. | Não | Não |
| Usuários de certificados | Indica se um utilizador de certificado está configurado para iniciar sessão no cluster. | Não | Não |
| Usuários locais | Indica se os utilizadores locais estão configurados para iniciar sessão no cluster. | Não | Não |
| Shell remoto | Indica se o RSH está ativado. Por razões de segurança, o RSH deve ser desativado. O Secure Shell (SSH) para acesso remoto seguro é o preferido. | Desativado | Sim |

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

Categorias de conformidade de VM de storage

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 |

| Parâmetro | Descrição | Recomendação | Diz respeito à conformidade com o SVM |
|-------------------------------|---|---------------------|--|
| 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 |
| Autenticação NIS | Indica se o uso da autenticação NIS está configurado. | Desativado | Não |
| Estado FPolicy ativo | Indica se FPolicy foi criado ou não. | Sim | Não |
| Encriptação SMB ativada | Indica se SMB -assinatura e selagem não estão ativados. | Sim | Não |
| Assinatura SMB ativada | Indica se a assinatura SMB não está ativada. | Sim | 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). |

| Parâmetro | Descrição |
|------------------------------------|--|
| 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. |

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.