Segurança

Data Infrastructure Insights

NetApp
February 11, 2026

Índice

Segurança

Data Infrastructure Insights Segurança

A segurança dos dados dos produtos e dos clientes é de extrema importância na NetApp. O Data Infrastructure Insights segue as melhores práticas de segurança durante todo o ciclo de vida do lançamento para garantir que as informações e os dados do cliente sejam protegidos da melhor maneira possível.

Visão geral de segurança

Segurança física

A infraestrutura de produção do Data Infrastructure Insights é hospedada na Amazon Web Services (AWS). Os controles relacionados à segurança física e ambiental para servidores de produção do Data Infrastructure Insights , que incluem edifícios, bem como fechaduras ou chaves usadas em portas, são gerenciados pela AWS. De acordo com a AWS: “O acesso físico é controlado tanto no perímetro quanto nos pontos de entrada do edifício por uma equipe de segurança profissional que utiliza vigilância por vídeo, sistemas de detecção de intrusão e outros meios eletrônicos. Funcionários autorizados utilizam mecanismos de autenticação multifator para acessar andares do data center.”

O Data Infrastructure Insights segue as melhores práticas do"Modelo de Responsabilidade Compartilhada" descrito pela AWS.

Segurança do produto

O Data Infrastructure Insights segue um ciclo de vida de desenvolvimento alinhado aos princípios Agile, o que nos permite abordar quaisquer defeitos de software voltados à segurança mais rapidamente, em comparação com metodologias de desenvolvimento com ciclos de lançamento mais longos. Usando metodologias de integração contínua, somos capazes de responder rapidamente a mudanças funcionais e de segurança. Os procedimentos e políticas de gerenciamento de mudanças definem quando e como as mudanças ocorrem e ajudam a manter a estabilidade do ambiente de produção. Quaisquer alterações impactantes são formalmente comunicadas, coordenadas, devidamente revisadas e aprovadas antes de serem lançadas no ambiente de produção.

Segurança de rede

O acesso de rede aos recursos no ambiente do Data Infrastructure Insights é controlado por firewalls baseados em host. Cada recurso (como um balanceador de carga ou instância de máquina virtual) tem um firewall baseado em host que restringe o tráfego de entrada apenas às portas necessárias para que o recurso execute sua função.

O Data Infrastructure Insights usa vários mecanismos, incluindo serviços de detecção de intrusão, para monitorar o ambiente de produção em busca de anomalias de segurança.

Avaliação de risco

A equipe do Data Infrastructure Insights segue um processo formalizado de Avaliação de Riscos para fornecer uma maneira sistemática e repetível de identificar e avaliar os riscos para que eles possam ser gerenciados adequadamente por meio de um Plano de Tratamento de Riscos.

Proteção de dados

O ambiente de produção do Data Infrastructure Insights é configurado em uma infraestrutura altamente redundante, utilizando várias zonas de disponibilidade para todos os serviços e componentes. Além de utilizar uma infraestrutura de computação redundante e altamente disponível, os dados críticos são copiados em intervalos regulares e as restaurações são testadas periodicamente. Políticas e procedimentos formais de backup minimizam o impacto de interrupções nas atividades comerciais e protegem os processos comerciais contra os efeitos de falhas de sistemas de informação ou desastres, além de garantir sua retomada oportuna e adequada.

Gerenciamento de autenticação e acesso

Todo o acesso do cliente ao Data Infrastructure Insights é feito por meio de interações da interface do usuário do navegador via https. A autenticação é realizada por meio do serviço de terceiros, Auth0. A NetApp centralizou isso como a camada de autenticação para todos os serviços de dados em nuvem.

O Data Infrastructure Insights segue as melhores práticas do setor, incluindo “Privilégio Mínimo” e “Controle de acesso baseado em função” em relação ao acesso lógico ao ambiente de produção do Data Infrastructure Insights . O acesso é controlado estritamente de acordo com a necessidade e é concedido apenas a pessoal autorizado selecionado, usando mecanismos de autenticação multifator.

Coleta e proteção de dados do cliente

Todos os dados do cliente são criptografados em trânsito pelas redes públicas e criptografados em repouso. O Data Infrastructure Insights utiliza criptografia em vários pontos do sistema para proteger os dados do cliente usando tecnologias que incluem Transport Layer Security (TLS) e o algoritmo AES-256 padrão do setor.

Desprovisionamento de clientes

Notificações por e-mail são enviadas em vários intervalos para informar o cliente que sua assinatura está expirando. Após o término da assinatura, a interface do usuário fica restrita e um período de carência começa para a coleta de dados. O cliente é então notificado por e-mail. Assinaturas de teste têm um período de carência de 14 dias e contas de assinatura paga têm um período de carência de 28 dias. Após o término do período de carência, o cliente é notificado por e-mail de que a conta será excluída em 2 dias. Um cliente pago também pode solicitar diretamente o cancelamento do serviço.

Os locatários expirados e todos os dados associados do cliente são excluídos pela equipe de Operações do Data Infrastructure Insights (SRE) no final do período de carência ou após a confirmação da solicitação do cliente para encerrar sua conta. Em ambos os casos, a equipe SRE executa uma chamada de API para excluir a conta. A chamada de API exclui a instância do locatário e todos os dados do cliente. A exclusão do cliente é verificada chamando a mesma API e verificando se o status do locatário do cliente é “EXCLUÍDO”.

Gestão de incidentes de segurança

O Data Infrastructure Insights é integrado ao processo da Equipe de Resposta a Incidentes de Segurança de Produtos (PSIRT) da NetApp para encontrar, avaliar e resolver vulnerabilidades conhecidas. O PSIRT coleta informações sobre vulnerabilidades de vários canais, incluindo relatórios de clientes, engenharia interna e fontes amplamente reconhecidas, como o banco de dados CVE.

Se um problema for detectado pela equipe de engenharia do Data Infrastructure Insights , a equipe iniciará o processo PSIRT, avaliará e possivelmente corrigirá o problema.

Também é possível que um cliente ou pesquisador do Data Infrastructure Insights identifique um problema de segurança com o produto Data Infrastructure Insights e relate o problema ao Suporte Técnico ou diretamente à equipe de resposta a incidentes da NetApp. Nesses casos, a equipe do Data Infrastructure Insights iniciará o

processo PSIRT, avaliará e possivelmente corrigirá o problema.

Teste de vulnerabilidade e penetração

A Data Infrastructure Insights segue as melhores práticas do setor e realiza testes regulares de vulnerabilidade e penetração usando profissionais e empresas de segurança internos e externos.

Treinamento de conscientização sobre segurança

Todo o pessoal da Data Infrastructure Insights passa por treinamento de segurança, desenvolvido para funções individuais, para garantir que cada funcionário esteja equipado para lidar com os desafios específicos de segurança de suas funções.

Conformidade

A Data Infrastructure Insights realiza auditorias e validações independentes de terceiros, por meio de firmas externas de CPA licenciadas, sobre sua segurança, processos e serviços, incluindo a conclusão da auditoria SOC 2.

Avisos de segurança da NetApp

Você pode visualizar os avisos de segurança disponíveis da NetApp"aqui" .

Informação e Região

A NetApp leva a segurança das informações dos clientes muito a sério. Veja como e onde o Data Infrastructure Insights armazena suas informações.

Quais informações o Data Infrastructure Insights armazena?

O Data Infrastructure Insights armazena as seguintes informações:

- Dados de desempenho

  Dados de desempenho são dados de séries temporais que fornecem informações sobre o desempenho do dispositivo/fonte monitorado. Isso inclui, por exemplo, o número de E/S entregues por um sistema de armazenamento, a taxa de transferência de uma porta FibreChannel, o número de páginas entregues por um servidor web, o tempo de resposta de um banco de dados e muito mais.

- Dados de inventário

  Os dados de inventário consistem em metadados que descrevem o dispositivo/fonte monitorado e como ele está configurado. Isso inclui, por exemplo, versões de hardware e software instaladas, discos e LUNs em um sistema de armazenamento, núcleos de CPU, RAM e discos de uma máquina virtual, os tablespaces de um banco de dados, o número e o tipo de portas em um switch SAN, nomes de diretório/arquivo (se a Segurança de Carga de Trabalho de Armazenamento estiver habilitada), etc.

- Dados de configuração

  Isso resume os dados de configuração fornecidos pelo cliente usados para gerenciar o inventário e as operações do cliente, por exemplo, nomes de host ou endereços IP dos dispositivos monitorados, intervalos de pesquisa, valores de tempo limite, etc.

- Segredos

  Os segredos consistem nas credenciais usadas pela Data Infrastructure Insights Acquisition Unit para acessar dispositivos e serviços do cliente. Essas credenciais são criptografadas usando criptografia assimétrica forte, e as chaves privadas são armazenadas apenas nas Unidades de Aquisição e nunca saem do ambiente do cliente. Mesmo os SREs privilegiados do Data Infrastructure Insights não conseguem acessar segredos do cliente em texto simples devido a esse design.

- Dados Funcionais

  Esses são dados gerados como resultado do fornecimento do Serviço de Dados em Nuvem pela NetApp , que informa a NetApp no desenvolvimento, implantação, operações, manutenção e proteção do Serviço de Dados em Nuvem. Dados Funcionais não contêm Informações do Cliente ou Informações Pessoais.

- Dados de acesso do usuário

  Informações de autenticação e acesso que permitem que o NetApp Console se comunique com sites regionais do Data Infrastructure Insights , incluindo dados relacionados à autorização do usuário.

- Dados do diretório do usuário de segurança da carga de trabalho de armazenamento

  Nos casos em que a funcionalidade de segurança de carga de trabalho estiver habilitada E o cliente optar por habilitar o coletor de diretório de usuários, o sistema armazenará nomes de exibição de usuários, endereços de e-mail corporativos e outras informações coletadas do Active Directory.

> Os dados do diretório do usuário referem-se às informações do diretório do usuário coletadas pelo coletor de dados do diretório do usuário do Workload Security, não aos dados sobre os próprios usuários do Data Infrastructure Insights/Workload Security.

Nenhum dado pessoal explícito é coletado de recursos de infraestrutura e serviços. As informações coletadas consistem apenas em métricas de desempenho, informações de configuração e metadados de infraestrutura, assim como muitos provedores de telefonia residencial, incluindo o suporte automático da NetApp e o ActiveIQ. No entanto, dependendo das convenções de nomenclatura do cliente, os dados de compartilhamentos, volumes, VMs, qtrees, aplicativos etc. podem conter informações de identificação pessoal.

Se a Segurança de Carga de Trabalho estiver habilitada, o sistema também analisará nomes de arquivos e diretórios em compartilhamentos SMB ou outros, que podem conter informações de identificação pessoal. Quando os clientes ativam o Workload Security User Directory Collector (que essencialmente mapeia os SIDs do Windows para nomes de usuário por meio do Active Directory), o nome de exibição, o endereço de e-mail corporativo e quaisquer atributos adicionais selecionados serão coletados e armazenados pelo Data Infrastructure Insights.

Além disso, os logs de acesso ao Data Infrastructure Insights são mantidos e contêm os endereços IP e de e-mail dos usuários usados para efetuar login no serviço.

Onde minhas informações são armazenadas?

O Data Infrastructure Insights armazena informações de acordo com a região em que seu ambiente é criado.

As seguintes informações são armazenadas na região do host:

- Telemetria e informações de ativos/objetos, incluindo contadores e métricas de desempenho
- Informações da Unidade de Aquisição

- Dados funcionais
- Auditar informações sobre atividades do usuário dentro do Data Infrastructure Insights
- Informações do Active Directory sobre segurança de carga de trabalho
- Informações de auditoria de segurança de carga de trabalho

As informações a seguir residem nos Estados Unidos, independentemente da região que hospeda seu ambiente do Data Infrastructure Insights :

- Informações do site do ambiente (às vezes chamado de "locatário"), como proprietário do site/conta.
- Informações que permitem que o NetApp Console se comunique com sites regionais do Data Infrastructure Insights , incluindo qualquer coisa relacionada à autorização do usuário.
- Informações relacionadas à relação entre o usuário do Data Infrastructure Insights e o locatário.

Regiões anfitriãs

As regiões anfitriãs incluem:

- EUA: us-east-1
- EMEA: eu-central-1
- APAC: ap-sudeste-2

Mais informações

Você pode ler mais sobre privacidade e segurança da NetApp nos seguintes links:

- "Centro de Confiança"
- "Transferências de dados transfronteiriças"
- "Regras corporativas vinculativas"
- "Respondendo a solicitações de dados de terceiros"
- "Princípios de privacidade da NetApp"

Ferramenta SecurityAdmin

O Data Infrastructure Insights inclui recursos de segurança que permitem que seu ambiente opere com segurança aprimorada. Os recursos incluem melhorias na criptografia, hash de senha e a capacidade de alterar senhas de usuários internos, bem como pares de chaves que criptografam e descriptografam senhas.

Para proteger dados confidenciais, a NetApp recomenda que você altere as chaves padrão e a senha do usuário *Acquisition* após uma instalação ou atualização.

As senhas criptografadas da fonte de dados são armazenadas no Data Infrastructure Insights, que usa uma chave pública para criptografar senhas quando um usuário as insere em uma página de configuração do coletor de dados. O Data Infrastructure Insights não tem as chaves privadas necessárias para descriptografar as senhas do coletor de dados; somente as Unidades de Aquisição (AUs) têm a chave privada do coletor de dados necessária para descriptografar as senhas do coletor de dados.

Considerações sobre atualização e instalação

Quando o seu sistema Insight contém configurações de segurança não padrão (ou seja, você redigitou senhas), você deve fazer backup de suas configurações de segurança. A instalação de um novo software ou, em alguns casos, a atualização de um software reverte o sistema para uma configuração de segurança padrão. Quando o sistema retorna à configuração padrão, você deve restaurar a configuração não padrão para que o sistema funcione corretamente.

Gerenciando a segurança na unidade de aquisição

A ferramenta SecurityAdmin permite que você gerencie as opções de segurança do Data Infrastructure Insights e é executada no sistema da unidade de aquisição. O gerenciamento de segurança inclui gerenciar chaves e senhas, salvar e restaurar configurações de segurança criadas por você ou restaurar configurações para as configurações padrão.

Antes de começar

- Você deve ter privilégios de administrador no sistema AU para instalar o software da Unidade de Aquisição (que inclui a ferramenta SecurityAdmin).
- Se você tiver usuários não administradores que posteriormente precisarão acessar a ferramenta SecurityAdmin, eles deverão ser adicionados ao grupo *cisys*. O grupo *cisys* é criado durante a instalação do AU.

Após a instalação do AU, a ferramenta SecurityAdmin pode ser encontrada no sistema da unidade de aquisição em qualquer um destes locais:

```
Windows - <install_path>\Cloud Insights\Acquisition
Unit\acq\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

Usando a ferramenta SecurityAdmin

Inicie a ferramenta SecurityAdmin no modo interativo (-i).

É recomendável usar a ferramenta SecurityAdmin no modo interativo, para evitar passar segredos na linha de comando, que podem ser capturados em logs.

As seguintes opções são exibidas:

[Opções para a ferramenta SecurityAdmin (Linux)]

1. **Backup**

   Cria um arquivo zip de backup do cofre contendo todas as senhas e chaves e coloca o arquivo em um local especificado pelo usuário ou nos seguintes locais padrão:

   ```
   Windows - <install_path>\Cloud Insights\Acquisition
   Unit\acq\securityadmin\backup\vault
   Linux - /var/log/netapp/oci/backup/vault
   ```

É recomendável que os backups do cofre sejam mantidos seguros, pois incluem informações confidenciais.

2. **Restaurar**

   Restaura o backup zip do cofre que foi criado. Uma vez restauradas, todas as senhas e chaves serão revertidas para os valores existentes no momento da criação do backup.

   A restauração pode ser usada para sincronizar senhas e chaves em vários servidores, por exemplo, seguindo estas etapas: 1) Alterar chaves de criptografia na AU. 2) Crie um backup do cofre. 3) Restaure o backup do cofre para cada uma das AUs.

3. **Registrar/Atualizar Script de Recuperação de Chave Externa**

   Use um script externo para registrar ou alterar as chaves de criptografia AU usadas para criptografar ou descriptografar senhas de dispositivos.

   Ao alterar as chaves de criptografia, você deve fazer backup da sua nova configuração de segurança para poder restaurá-la após uma atualização ou instalação.

   Observe que esta opção só está disponível no Linux.

   Ao usar seu próprio script de recuperação de chave com a ferramenta SecurityAdmin, tenha em mente o seguinte:

   - O algoritmo suportado atualmente é RSA com no mínimo 2048 bits.
   - O script deve retornar as chaves privada e pública em texto simples. O script não deve retornar chaves públicas e privadas criptografadas.
   - O script deve retornar conteúdo bruto e codificado (somente formato PEM).
   - O script externo deve ter permissões *execute*.

4. **Girar chaves de criptografia**

   Gire suas chaves de criptografia (cancela o registro das chaves atuais e registra novas chaves). Para usar uma chave de um sistema de gerenciamento de chaves externo, você deve especificar o ID da chave pública e o ID da chave privada.

5. **Redefinir para as teclas padrão**

   Redefine a senha do usuário de aquisição e as chaves de criptografia do usuário de aquisição para os valores padrão. Os valores padrão são aqueles fornecidos durante a instalação.

6. **Alterar senha do Truststore**

   Alterar a senha do truststore.

7. **Alterar senha do Keystore**

   Alterar a senha do keystore.

8. **Criptografar senha do coletor**

   Criptografar senha do coletor de dados.

9. **Saída**

Saia da ferramenta SecurityAdmin.

Escolha a opção que deseja configurar e siga as instruções.

Especificando um usuário para executar a ferramenta

Se você estiver em um ambiente controlado e preocupado com a segurança, talvez não tenha o grupo *cisys*, mas ainda assim poderá querer que usuários específicos executem a ferramenta SecurityAdmin.

Você pode fazer isso instalando manualmente o software AU e especificando o usuário/grupo ao qual deseja acesso.

- Usando a API, baixe o instalador do CI para o sistema AU e descompacte-o.
  - Você precisará de um token de autorização único. Consulte a documentação do API Swagger (*Admin > API Access* e selecione o link *API Documentation*) e encontre a seção *GET /au/oneTimeToken* da API.
  - Depois de obter o token, use a API *GET /au/installers/{platform}/{version}* para baixar o arquivo do instalador. Você precisará fornecer a plataforma (Linux ou Windows), bem como a versão do instalador.
- Copie o arquivo do instalador baixado para o sistema AU e descompacte-o.
- Navegue até a pasta que contém os arquivos e execute o instalador como root, especificando o usuário e o grupo:

```
./cloudinsights-install.sh <User> <Group>
```

Se o usuário e/ou grupo especificado não existir, eles serão criados. O usuário terá acesso à ferramenta SecurityAdmin.

Atualizando ou removendo proxy

A ferramenta SecurityAdmin pode ser usada para definir ou remover informações de proxy para a Unidade de Aquisição executando a ferramenta com o parâmetro *-pr*:

```
[root@ci-eng-linau bin]# ./securityadmin -pr
usage: securityadmin -pr -ap <arg> | -h | -rp | -upr <arg>

The purpose of this tool is to enable reconfiguration of security aspects
of the Acquisition Unit such as encryption keys, and proxy configuration,
etc. For more information about this tool, please check the Data
Infrastructure Insights
Documentation.

-ap,--add-proxy <arg>       add a proxy server.  Arguments: ip=ip
                             port=port user=user password=password
                             domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
-h,--help
-rp,--remove-proxy          remove proxy server
-upr,--update-proxy <arg>   update a proxy.  Arguments: ip=ip port=port
                             user=user password=password domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
```

Por exemplo, para remover o proxy, execute este comando:

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
Você deve reiniciar a Unidade de Aquisição após executar o comando.
```

Para atualizar um proxy, o comando é

```
./securityadmin -pr -upr <arg>
```

Recuperação de Chave Externa

Se você fornecer um script de shell UNIX, ele poderá ser executado pela unidade de aquisição para recuperar

a **chave privada** e a **chave pública** do seu sistema de gerenciamento de chaves.

Para recuperar a chave, o Data Infrastructure Insights executará o script, passando dois parâmetros: *key id* e *key type*. *ID da chave* pode ser usado para identificar a chave no seu sistema de gerenciamento de chaves. O *Tipo de chave* é "público" ou "privado". Quando o tipo de chave é "pública", o script deve retornar a chave pública. Quando o tipo de chave é "privada", a chave privada deve ser retornada.

Para enviar a chave de volta para a unidade de aquisição, o script deve imprimir a chave na saída padrão. O script deve imprimir *apenas* a chave na saída padrão; nenhum outro texto deve ser impresso na saída padrão. Depois que a chave solicitada for impressa na saída padrão, o script deverá sair com um código de saída 0; qualquer outro código de retorno será considerado um erro.

O script deve ser registrado na unidade de aquisição usando a ferramenta SecurityAdmin, que executará o script junto com a unidade de aquisição. O script deve ter permissão de *leitura* e *execução* para o usuário root e "cisys". Se o script de shell for modificado após o registro, o script de shell modificado deverá ser registrado novamente na unidade de aquisição.

parâmetro de entrada: id da chave	Identificador de chave usado para identificar a chave no sistema de gerenciamento de chaves do cliente.
parâmetro de entrada: tipo de chave	público ou privado.
saída	A chave solicitada deve ser impressa na saída padrão. A chave RSA de 2048 bits é suportada atualmente. As chaves devem ser codificadas e impressas no seguinte formato: formato de chave privada - PEM, codificado em DER PKCS8 PrivateKeyInfo RFC 5958 formato de chave pública - PEM, codificado em DER X.509 SubjectPublicKeyInfo RFC 5280
código de saída	Código de saída zero para sucesso. Todos os outros valores de saída são considerados falha.
permissões de script	O script deve ter permissão de leitura e execução para o usuário root e "cisys".
toras	As execuções de script são registradas. Os logs podem ser encontrados em - /var/log/netapp/cloudinsights/securityadmin/securityadmin.log /var/log/netapp/cloudinsights/acq/acq.log

Criptografando uma senha para uso na API

A opção 8 permite que você criptografe uma senha, que pode então ser passada para um coletor de dados via API.

Inicie a ferramenta SecurityAdmin no modo interativo e selecione a opção 8: *Criptografar senha*.

```
 securityadmin.sh -i
Você será solicitado a digitar a senha que deseja criptografar.  Observe
que os caracteres digitados não são exibidos na tela.  Digite a senha
novamente quando solicitado.
```

Como alternativa, se você for usar o comando em um script, em uma linha de comando use *securityadmin.sh* com o parâmetro "-enc", passando sua senha não criptografada:

```
 securityadmin -enc mypassword
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["Exemplo de CLI"]
```

A senha criptografada é exibida na tela. Copie a sequência inteira, incluindo quaisquer símbolos iniciais ou finais.

[Modo interativo Criptografar senha, largura=640]

Para enviar a senha criptografada para um coletor de dados, você pode usar a API de coleta de dados. O swagger para esta API pode ser encontrado em **Admin > Acesso à API** e clique no link "Documentação da API". Selecione o tipo de API "Coleta de dados". No título *data_collection.data_collector*, escolha a API POST */collector/datasources* para este exemplo.

[API para coleta de dados]

Se você definir a opção *preEncrypted* como *True*, qualquer senha que você passar pelo comando da API será tratada como **já criptografada**; a API não criptografará novamente a(s) senha(s). Ao criar sua API, basta colar a senha criptografada anteriormente no local apropriado.

[Exemplo de API, largura=600]

Informações sobre direitos autorais

Informações sobre marcas comerciais