Segurança

Data Infrastructure Insights

NetApp
January 10, 2025

Índice

Segurança

Segurança do Insights da infraestrutura de dados

A segurança de dados de produtos e clientes é de extrema importância na NetApp. O Data Infrastructure Insights segue as práticas recomendadas de segurança ao longo do ciclo de vida da versão para garantir que as informações e os dados do cliente estejam 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 físicos e ambientais relacionados à segurança dos servidores de produção do Data Infrastructure Insights, que incluem edifícios, bem como fechaduras ou chaves usadas nas portas, são gerenciados pela AWS. De acordo com a AWS: "O acesso físico é controlado tanto no perímetro quanto no estabelecimento de pontos de entrada pela equipe de segurança profissional que utiliza vigilância por vídeo, sistemas de deteção de intrusão e outros meios eletrônicos. A equipe autorizada utiliza mecanismos de autenticação multifator para acessar andares do data center."

O Data Infrastructure Insights segue as práticas recomendadas do "Modelo de responsabilidade compartilhada" descrito pela AWS.

Segurança do produto

O Data Infrastructure Insights segue um ciclo de vida de desenvolvimento em linha com os princípios ágeis, permitindo-nos, assim, abordar quaisquer defeitos de software orientados para a segurança mais rapidamente, em comparação com metodologias de desenvolvimento de ciclo de lançamento mais longo. Usando metodologias de integração contínua, somos capazes de responder rapidamente às 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 com impactos são formalmente comunicadas, coordenadas, adequadamente revisadas e aprovadas antes de sua liberação no ambiente de produção.

Segurança da rede

O acesso à rede a recursos no ambiente 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 esse recurso execute sua função.

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

Avaliação de risco

A equipe Data Infrastructure Insights segue um processo formalizado de avaliação de risco 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 Data Infrastructure Insights é configurado em uma infraestrutura altamente redundante, utilizando várias zonas de disponibilidade para todos os serviços e componentes. Além da utilização de uma infraestrutura de computação redundante e altamente disponível, o backup de dados críticos em intervalos regulares e as restaurações são testadas periodicamente. Políticas e procedimentos formais de backup minimizam o impactos das interrupções das atividades de negócios e protegem os processos de negócios contra os efeitos de falhas de sistemas de informação ou desastres e garantem sua retomada oportuna e adequada.

Autenticação e gerenciamento de acesso

Todo o acesso do cliente ao Data Infrastructure Insights é feito por meio de interações da interface do usuário do navegador por https. A autenticação é realizada através do serviço de terceiros 3rd, Auth0. A NetApp centralizou-se nisso como a camada de autenticação para todos os serviços de dados de nuvem.

O Data Infrastructure Insights segue as práticas recomendadas do setor, incluindo "menos privilégio" e "controle de acesso baseado em função", sobre o acesso lógico ao ambiente de produção do Data Infrastructure Insights. O acesso é controlado com base em necessidade estrita e só é concedido para pessoal autorizado selecionado usando mecanismos de autenticação multifator.

Coleta e proteção de dados do cliente

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

Desprovisionamento do cliente

As notificações por e-mail são enviadas em vários intervalos para informar o cliente que sua assinatura está expirando. Uma vez que a assinatura expirou, a IU é restrita e um período de carência começa para a coleta de dados. O cliente é então notificado por e-mail. As assinaturas de teste têm um período de carência de 14 dias e as contas de assinatura pagas 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 para estar fora do serviço.

Os locatários expirados e todos os dados associados do cliente são excluídos pela equipe de operações do Data Infrastructure Insights Operations (SRE) no final do período de carência ou mediante 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 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".

Gerenciamento de incidentes de segurança

O Insights de infraestrutura de dados é integrado ao processo da equipe de resposta a incidentes de Segurança de Produtos (PSIRT) da NetApp para localizar, avaliar e resolver vulnerabilidades conhecidas. O PSIRT coleta informações de vulnerabilidades de vários canais, incluindo relatórios de clientes, engenharia interna e fontes amplamente reconhecidas, como o banco de dados CVE.

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

Também é possível que um cliente ou pesquisador do Insights de infraestrutura de dados possa identificar um

problema de segurança com o produto Insights de infraestrutura de dados e relatar o problema ao suporte técnico ou diretamente à equipe de resposta a incidentes da NetApp. Nesses casos, a equipe de Data Infrastructure Insights iniciará o processo PSIRT, avaliará e potencialmente corrigirá o problema.

Teste de vulnerabilidade e penetração

O Data Infrastructure Insights segue as melhores práticas do setor e executa testes regulares de vulnerabilidade e penetração usando profissionais e empresas de segurança internas e externas.

Treinamento de conscientização sobre segurança

Todos os funcionários do Data Infrastructure Insights passam por treinamento de segurança, desenvolvido para funções individuais, para garantir que cada funcionário esteja equipado para lidar com os desafios específicos voltados à segurança de suas funções.

Conformidade

O Data Infrastructure Insights realiza auditorias e validações independentes de terceiros de sua segurança, processos e serviços, incluindo a conclusão da Auditoria SOC 2.

Consultores de Segurança da NetApp

Pode visualizar os avisos de segurança disponíveis do 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 performance

  Os 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 iOS fornecido por um sistema de armazenamento, a taxa de transferência de uma porta FibreChannel, o número de páginas entregues por um servidor da 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 é 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 espaços de tabela de um banco de dados, o número e tipo de portas em um switch SAN, nomes de diretório/arquivo (se o Storage Workload Security estiver ativado), 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 polling, valores de tempo limite, etc.

- Segredos

  Os segredos consistem nas credenciais usadas pela Unidade de aquisição do Data Infrastructure Insights para acessar dispositivos e serviços do cliente. Essas credenciais são criptografadas usando criptografia assimétrica forte e as chaves privadas são armazenadas somente nas unidades de aquisição e nunca saem do ambiente do cliente. Mesmo os SREs privilegiados do Insights de infraestrutura de dados não conseguem acessar segredos do cliente em texto simples devido a esse design.

- Dados funcionais

  Esses são dados gerados como resultado do NetApp que fornece o Serviço de dados em nuvem, que informa a NetApp no desenvolvimento, implantação, operações, manutenção e proteção do Serviço de dados em nuvem. Os 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 BlueXP se comunique com sites regionais de informações de infraestrutura de dados, incluindo dados relacionados à autorização do usuário.

- Dados do diretório do usuário de segurança do workload de armazenamento

  Nos casos em que a funcionalidade de Segurança de carga de trabalho está ativada E o cliente optar por ativar o coletor do diretório de utilizadores, o sistema armazenará nomes de apresentação de utilizadores, endereços de correio eletrónico empresariais e outras informações recolhidas no ative 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, e não aos dados sobre os 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 performance, informações de configuração e metadados da infraestrutura, assim como muitos telefônicas dos fornecedores, incluindo suporte automático da NetApp e ActiveIQ. No entanto, dependendo das convenções de nomenclatura de um cliente, os dados para compartilhamentos, volumes, VMs, qtrees, aplicativos, etc. podem conter informações de identificação pessoal.

Se o Workload Security estiver ativado, o sistema também examinará os nomes de arquivos e diretórios em SMB ou outros compartilhamentos, que podem conter informações pessoalmente identificáveis. Quando os clientes ativam o Coletor do diretório de usuários de Segurança de carga de trabalho (que mapeia essencialmente os SIDs do Windows para nomes de usuário por meio do ative 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 fazer 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:

- Informações de telemetria e de ativos/objetos, incluindo contadores e métricas de desempenho

- Informações da Unidade de aquisição
- Dados funcionais
- Faça auditoria de informações sobre as atividades do usuário dentro do Data Infrastructure Insights
- Informações sobre o ative Directory de segurança da 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 Data Infrastructure Insights:

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

Regiões de acolhimento

As regiões de host incluem:

- EUA: US-East-1
- EMEA: eu-central-1
- APAC: ap-sudeste-2

Mais informações

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

- "Centro de confiança"
- "Transferências de dados transfronteiriças"
- "Regras corporativas vinculativas"
- "Resposta 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 internas de usuário, bem como pares de chaves que criptografam e descriptografam senhas.

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

As senhas criptografadas de origem 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 de 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 sistema Insight contiver configurações de segurança não predefinidas (ou seja, se tiver palavras-passe recodificadas), tem de efetuar uma cópia de segurança das suas configurações de segurança. Instalar um novo software ou, em alguns casos, atualizar o software, reverte o sistema para uma configuração de segurança padrão. Quando o sistema voltar para a configuração padrão, você deve restaurar a configuração não padrão para que o sistema funcione corretamente.

Gestão da segurança na unidade de aquisição

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

Antes de começar

- Tem de ter admin Privileges 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 devem ser adicionados ao grupo *cisys*. O grupo *cisys* é criado durante a instalação da AU.

Após a instalação da AU, a ferramenta SecurityAdmin encontra-se no sistema da unidade de aquisição em qualquer uma destas localizações:

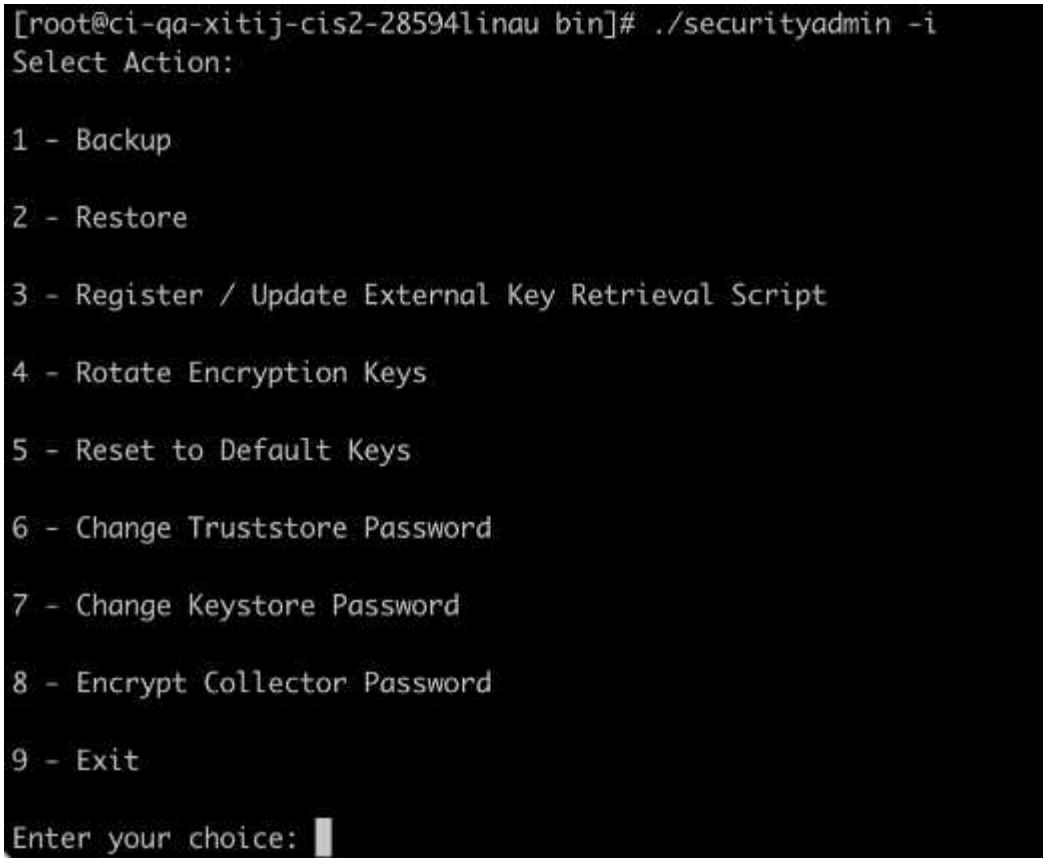
```
Windows - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
Linux - /bin/oci-securityadmin.sh
```

Usando a ferramenta SecurityAdmin

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

> Recomenda-se usar a ferramenta SecurityAdmin no modo interativo, para evitar passar segredos na linha de comando, que pode ser capturada em logs.

São apresentadas as seguintes opções:



1. **Backup**

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

   ```
   Windows - C:\Program Files\SANscreen\backup\vault
   Linux - /var/log/netapp/oci/backup/vault
   ```

   Recomenda-se que os backups do Vault sejam mantidos seguros, pois incluem informações confidenciais.

2. **Restaurar**

   Restaura o backup zip do Vault que foi criado. Uma vez restaurado, todas as senhas e chaves são revertidas para valores existentes no momento da criação do backup.

   A restauração pode ser usada para sincronizar senhas e chaves em vários servidores, por exemplo, usando estas etapas: 1) alterar chaves de criptografia na AU. 2) criar um backup do cofre. 3) Restaurar o backup do Vault para cada um dos AUS.

3. **Register / Update External Key Retrieval Script**

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

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

Nota 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 atual é RSA com um mínimo de 2048 bits.
- O script deve retornar as chaves privadas e públicas em texto simples. O script não deve retornar chaves privadas e públicas criptografadas.
- O script deve retornar conteúdo codificado em bruto (somente formato PEM).
- O script externo deve ter permissões *execute*.

4. **Rotate Encryption Keys** (rodar chaves de encriptação)

   Gire suas chaves de criptografia (desRegistra 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 chaves padrão*

   Repõe a palavra-passe do utilizador de aquisição e as chaves de encriptação do utilizador de aquisição para valores predefinidos; os valores predefinidos são os fornecidos durante a instalação.

6. * Alterar senha de armazenamento de confiança*

   Altere a senha do armazenamento de confiança.

7. **Altere a senha do Keystore**

   Altere a senha do keystore.

8. **Encrypt Collector Password**

   Encripte a palavra-passe 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 com consciência de segurança, talvez você não tenha o grupo *cisys*, mas ainda queira que usuários específicos executem a ferramenta SecurityAdmin.

Você pode conseguir isso instalando manualmente o software AU e especificando o usuário/grupo para quem deseja acessar.

- Usando a API, baixe o Instalador de CI para o sistema AU e descompacte-o.
  - Você precisará de um token de autorização única. Consulte a documentação do Swagger da API (*Admin > API Access* e selecione o link *API Documentation*) e localize a seção *GET /au/oneTimeToken* API.
  - Depois de ter o token, use a API _GET /au/instaladores/ 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
Tem de reiniciar a Unidade de aquisição depois de 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 pode 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*. *Key id* pode ser usado para identificar a chave em seu sistema de gerenciamento de chaves. *Tipo de chave* é "pública" ou "privada". Quando o tipo de chave é "pública", o script deve retornar a chave pública. Quando o tipo de chave é "privado", a chave privada deve ser retornada.

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

O script deve ser registrado na unidade de aquisição usando a ferramenta SecurityAdmin, que executará o script juntamente com a unidade de aquisição. O script deve ter permissão *read* e *execute* para o usuário root e "cisys". Se o script shell for modificado após o Registro, o script shell modificado deve ser re-registrado na unidade de aquisição.

parâmetro de entrada: id da chave	Identificador de chave usado para identificar a chave no sistema de gerenciamento de chaves dos clientes.
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 atualmente suportada. As chaves devem ser codificadas e impressas no seguinte formato - formato de chave privada - PEM, PKCS8 PrivateKeyInfo RFC 5958 formato de chave pública - PEM, X,509 subjectPublicKeyInfo RFC 5280 codificado POR DER
código de saída	Código de saída de zero para o 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".
registos	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

Encriptar uma palavra-passe para utilização na API

A opção 8 permite criptografar uma senha, que você pode passar para um coletor de dados via API.

Inicie a ferramenta SecurityAdmin no modo interativo e selecione a opção 8: *Encrypt Password*.

```
 securityadmin.sh -i
É-lhe pedido que introduza a palavra-passe que pretende encriptar. Observe
que os carateres digitados não são exibidos na tela. Digite novamente a
senha quando solicitado.
```

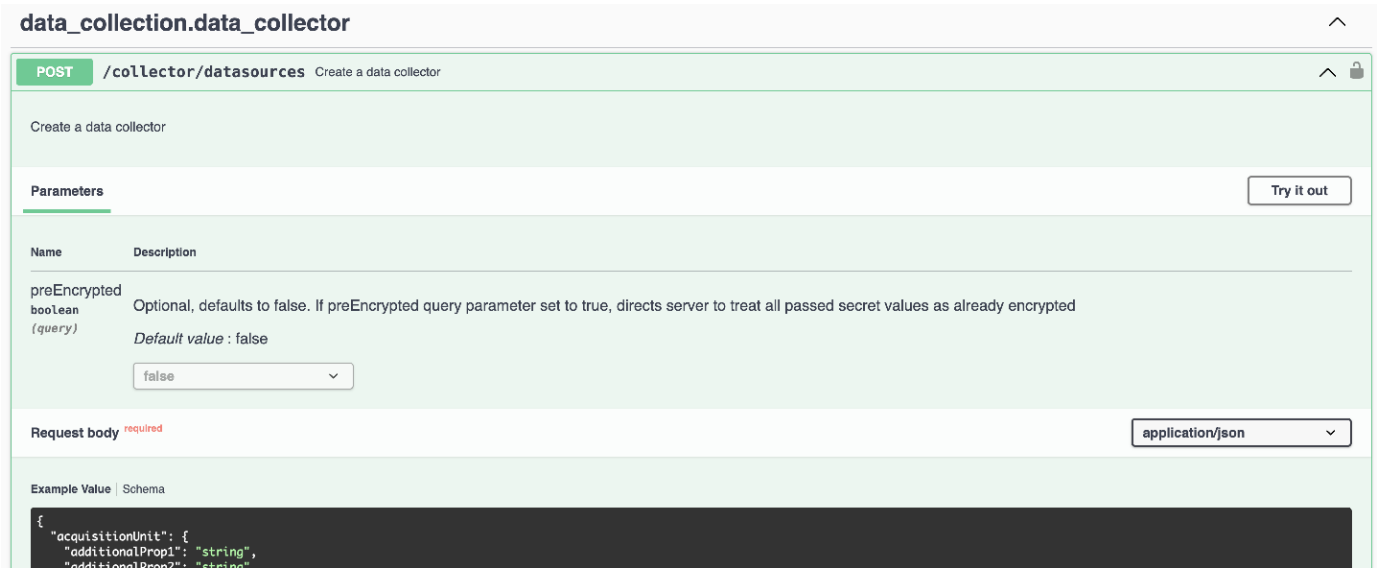
Alternativamente, se você usar o comando em um script, em uma linha de comando use *securityadmin.sh* com o parâmetro "-enc", passando sua senha não criptografada:

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

A palavra-passe encriptada é apresentada no ecrã. Copie toda a cadeia, incluindo quaisquer símbolos à esquerda ou à direita.

```
[root@ci-eng-srivardh-learn bin]# securityadmin.sh -i
Select Action:

1 - Backup

2 - Restore

3 - Change Encryption Keys

4 - Reset to Default Keys

5 - Check for Default Encryption Keys

6 - Change Truststore Password

7 - Change Keystore Password

8 - Encrypt Password

9 - Exit

Enter your choice: 8
Please enter your password to encrypt:
Please confirm your password to encrypt:

Your Encrypted Password below

ciYJAMpdEncBsLQwF2gobbiERl4Jrwb7tLWOfYhu0dERGZZU3L+uWfcCXdNSXTWr6SFuumwsWVFib3h78vnM0s6vM7G/2klBd8gqJiQ+tS/lZkmJ6XKgTDcf3LGn8UqzQy
RnOv5jJBGip6nCysrt9dapsEiRVHrMJVr8btGYbb4Zoz62qudMfW9uQdm3qyzSKbIY0L0An89yDPC0kDkaXreyLfpjuOG5UmeZzlKGCT0aBTggri/JIYyyr4w2ZLnGOw21
LGm59vor7OGUOiKZYabLd+7LpsdCCBi1eF86BCj2RkxXOof891sHN+E7zTvZEofdGVWepc7b/HNah5XiXgVk1viCZ/WqkyQ==
```

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 > API Access** e clique no link "API Documentation". Selecione o tipo de API "coleta de dados". No título *data_Collection.data_Collector*, escolha a API */Collector/datasources* POST para este exemplo.



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

https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true


```
{
"name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
"J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnlBVsAWyLmORxFAw
vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
+nfPDDyH8Tq6AM5WsVCKqnZAa2ZlY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAyPoyw/JT0nXHDuf683uE
K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```

Informações sobre direitos autorais

Informações sobre marcas comerciais