

# Cisco Stealthwatch

Guia de instalação e configuração do hardware do Data Store



---

# Índice

<b>Introdução à Instalação e Configuração do Hardware do Data Store</b> .....	<b>5</b>
Descrição geral .....	5
Público-alvo .....	5
Como utilizar este guia .....	5
<b>Conceitos e Arquitetura do Data Store</b> .....	<b>8</b>
<b>Pré-requisitos e Recomendações sobre a Implementação do Data Store</b> ...	<b>13</b>
Suporte de Versão Stealthwatch .....	13
Licenças Stealthwatch .....	13
Requisitos de compatibilidade de hardware e de ligação em rede Stealthwatch .....	13
Considerações de implementação empresarial Stealthwatch .....	15
Credenciais necessárias para a implementação do Data Store .....	15
Considerações sobre comutação e ligação de rede do Data Store .....	15
Requisitos e considerações sobre a implementação do Data Store .....	19
Portas de comunicação do Data Store .....	21
<b>Descrição geral da implementação do Data Store Stealthwatch</b> .....	<b>24</b>
<b>Instalação de hardware do Data Store</b> .....	<b>30</b>
Implementação e considerações sobre o hardware Stealthwatch .....	30
Configuração do SMC para utilização com um Data Store .....	30
Implementação e configuração inicial do hardware do Data Store .....	33
Implementação do UDP Director .....	35
Configuração do Coletor de fluxo para utilização com um Data Store .....	35
Implementação do sensor de fluxo .....	38
Implementação da consola de gestão Stealthwatch de ativação pós-falha .....	38
Inicialização e configuração do Data Store .....	39
Configuração da Consola de Gestão Vertica .....	48
<b>Configuração de retenção do Data Store</b> .....	<b>53</b>

---

<b>Passos seguintes da instalação do Data Store</b> .....	<b>59</b>
<b>Manutenção do Data Store</b> .....	<b>60</b>
Reiniciar um Nós de dados .....	60
Reinicie o Data Store .....	61
Criar uma cópia de segurança do Data Store .....	62
Restaurar uma cópia de segurança do Data Store .....	67
Adicionar três Nós de dados ao Data Store .....	70
Preparar o Data Store para adicionar Nós de dados e reequilibrar .....	70
Adicionar Nós de dados ao Data Store .....	70
Remover um Nós de dados do Data Store .....	74
Substitua um Nós de dados por um Nós de dados sobresselente com um endereço IP diferente .....	75
Preparar o Data Store para substituir um Nós de dados .....	75
Substitua o Nós de dados .....	75
Copie a Informação de confiança do Data Store para um SMC de ativação pós-falha .....	77
<b>Resolução de problemas na implementação do Data Store</b> .....	<b>79</b>
Resolução de problemas na implementação de hardware .....	79
Resolução de problemas do Script setup-sw-datastore-secure-connectivity .....	79
Resolução de problemas do Script install_SDBN_initial.py .....	84
Resolução de problemas do Script update_SDBN.py .....	93
Resolução de problemas com a Consola de Gestão Vertica .....	95
Resolução de problemas do Data Store .....	96
<b>Anexo A. Preparação da instalação</b> .....	<b>98</b>
Avisos relativos à instalação .....	98
Orientações de instalação .....	100
Recomendações de segurança .....	102
Manter a segurança elétrica .....	102
Prevenção de danos resultantes de descarga eletrostática (ESD) .....	103

---

Ambiente do local .....	103
Considerações sobre a fonte de alimentação .....	103
Considerações relativas à configuração do rack .....	104
<b>Anexo B. Instalação de hardware Stealthwatch .....</b>	<b>105</b>
Montagem do dispositivo .....	105
Hardware incluído com o dispositivo .....	105
Hardware adicional necessário .....	105
Ligação do dispositivo à rede .....	106
Ligação do dispositivo .....	107
Ligação com um teclado e um monitor .....	107
Ligação com um computador portátil .....	108
Configurar as definições de rede utilizando a Configuração inicial .....	109
Configuração geral de dispositivo Stealthwatch .....	110
Dispositivos compatíveis com Data Store (SMC 2210, FC 4210) .....	111
Configuração de Nó de dados .....	115
Alteração da palavra-passe do utilizador Sysadmin .....	119
Alteração da palavra-passe do utilizador raiz .....	120
<b>Anexo C. Configurar os seus dispositivos .....</b>	<b>122</b>
Requisitos da ferramenta de configuração de dispositivo .....	122
Geridos .....	122
SMC de ativação pós-falha .....	122
Boas Práticas .....	123
Ordem de configuração .....	123
1. Iniciar sessão .....	124
2. Configure o dispositivo .....	125
3. Registe a Consola de Gestão Stealthwatch .....	127
4. Adicione dispositivos à Gestão Central .....	128
5. Confirme o estado do dispositivo .....	128

# Introdução à Instalação e Configuração do Hardware do Data Store

## Descrição geral

Este guia explica como instalar o Data Store Stealthwatch como parte da implementação de um sistema Stealthwatch. Descreve os componentes do sistema Stealthwatch e a forma como se posicionam no sistema, especialmente em relação ao Data Store.

Este capítulo inclui os seguintes tópicos:

- **Público-alvo**
- **Como utilizar este guia**

## Público-alvo

Este guia foi concebido para orientar a pessoa responsável pela instalação do hardware do sistema Stealthwatch. Parte-se do princípio de que o utilizador já tem conhecimentos gerais acerca da instalação de equipamento de rede (Coletor de fluxo e a Consola de gestão Stealthwatch).

Para informação sobre a configuração dos produtos do sistema Stealthwatch, consulte o *Guia de configuração do sistema Stealthwatch*.

## Como utilizar este guia

Para além desta introdução, este guia contém os seguintes capítulos:

Capítulo	Descrição
<b>Conceitos e Arquitetura do Data Store</b>	Descreve os conceitos básicos da base de dados do Data Store e a arquitetura básica relacionada com a implementação do Data Store em relação a um SMC e aos Coletores de fluxo.
<b>Pré-requisitos e Recomendações sobre a Implementação do Data Store</b>	Descreve o hardware Stealthwatch compatível com o Data Store e indica os requisitos e as recomendações sobre a implementação do seu Data Store, incluindo as portas de comunicação a abrir.

<b>Capítulo</b>	<b>Descrição</b>
<b>Descrição geral da implementação do Data Store Stealthwatch</b>	Fornece uma descrição geral de alto nível da implementação de dispositivos Stealthwatch para utilização com um Data Store.
<b>Instalação de hardware do Data Store</b>	Fornece uma descrição geral completa da implementação de dispositivos Stealthwatch para utilização com um Data Store e instruções de configuração para inicializar a base de dados do Data Store.
<b>Configuração de retenção do Data Store</b>	Fornece informação sobre a configuração do período de retenção de dados do Data Store.
<b>Passos seguintes da instalação do Data Store</b>	Descreve os passos seguintes após terminar a implementação e configuração do seu Data Store.
<b>Manutenção do Data Store</b>	Descreve as tarefas de manutenção do Data Store.
<b>Resolução de problemas na implementação do Data Store</b>	Descreve problemas comuns durante o processo de instalação do Data Store e soluções sugeridas.
<b>Anexo A. Preparação da instalação</b>	Fornece avisos sobre a instalação de hardware.
<b>Anexo B. Instalação de hardware</b>	Fornece uma descrição geral da instalação de dispositivos Stealthwatch e da configuração inicial para atribuir um endereço IP e outra

<b>Capítulo</b>	<b>Descrição</b>
<b>Stealthwatch</b>	informação de gestão relacionada.
<b>Anexo C. Configurar os seus dispositivos</b>	Fornece uma descrição geral da utilização da Ferramenta de configuração de dispositivo para configurar os seus dispositivos Stealthwatch.

# Conceitos e Arquitetura do Data Store



**Não** instale um Data Store Stealthwatch sozinho. Se planejar comprar um Data Store Stealthwatch, contacte os Serviços Profissionais da Cisco para obter apoio na instalação, implementação e configuração como parte da sua implementação Stealthwatch geral.

O Data Store Stealthwatch oferece um repositório central para armazenar a telemetria da sua rede, recolhida pelos seus Coletores de fluxo Stealthwatch. O Data Store é composto por um cluster de Nós de dados, cada um contendo uma parte dos seus dados, e por uma cópia de segurança de dados de Nós de dados separados. Como todos os seus dados estão numa base de dados centralizada e não espalhados por vários Coletores de fluxo, a sua Consola de gestão Stealthwatch pode obter resultados de consulta a partir do Data Store mais rapidamente do que se consultasse todos os seus Coletores de fluxo separadamente. O Data Store oferece melhor tolerância a falhas, melhor resposta de consulta e um preenchimento mais rápido de gráficos e tabelas.

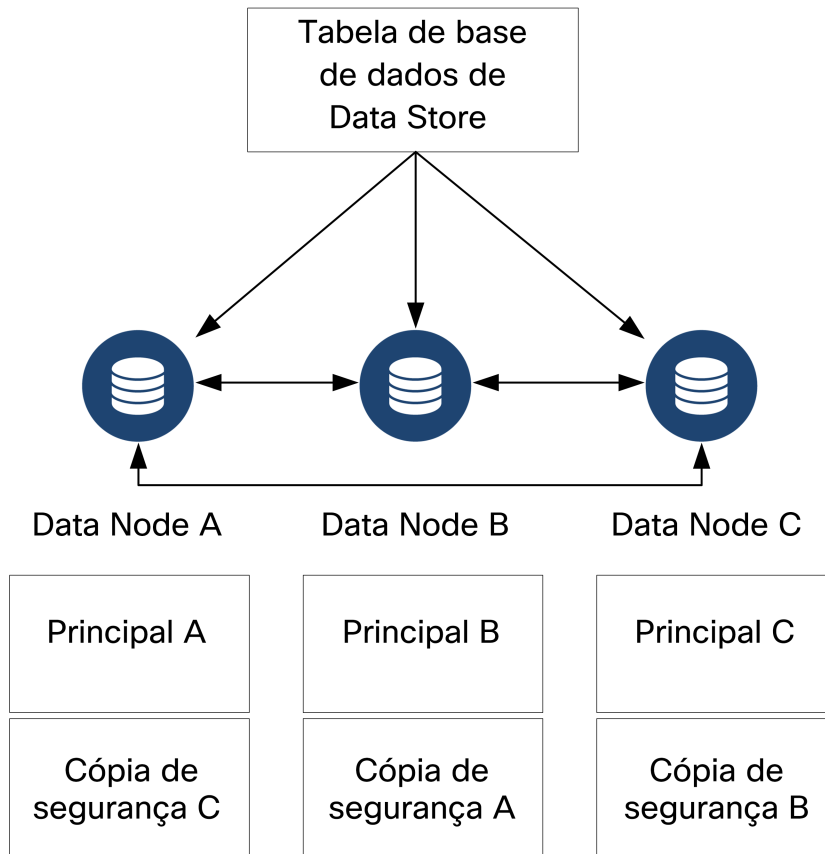
## Data Store Armazenamento e tolerância a falhas

O Data Store recolhe dados de Coletores de fluxo e distribui os mesmos de forma uniforme pelos Nós de dados no cluster. Cada Nós de dados, além de armazenar uma parte da sua telemetria geral, armazena também uma cópia de segurança da telemetria de outro Nós de dados. O armazenamento de dados desta forma:

- contribui para o equilíbrio de tráfego
- distribui o processamento por cada nó
- assegura que todos os dados ingeridos no Data Store têm uma cópia de segurança para tolerância a falhas
- permite um aumento do número de Nós de dados para melhorar o desempenho geral de armazenamento e consulta

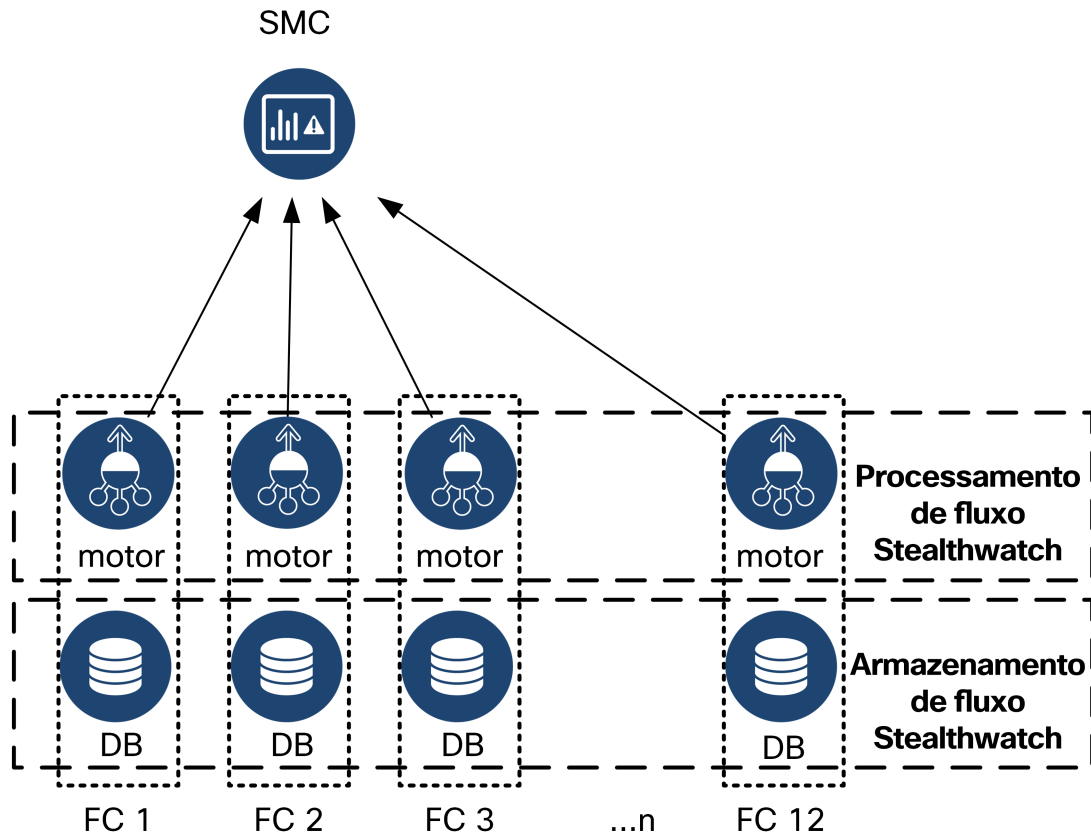
Se um nó ficar inativo, desde que o nó que contém a sua cópia de segurança continue disponível e, pelo menos, metade do número total de Nós de dados continuem ativos, o Data Store geral permanece ativo. Isto dá-lhe tempo para reparar a ligação inativa ou a avaria de hardware. Após substituir o Nós de dados avariado, o Data Store restaura os dados desse nó a partir da cópia de segurança existente armazenada no Nós de dados adjacente e cria uma cópia de segurança dos dados nesse Nós de dados. Consulte o diagrama seguinte para um exemplo da forma como os Nós de dados armazenam telemetria:



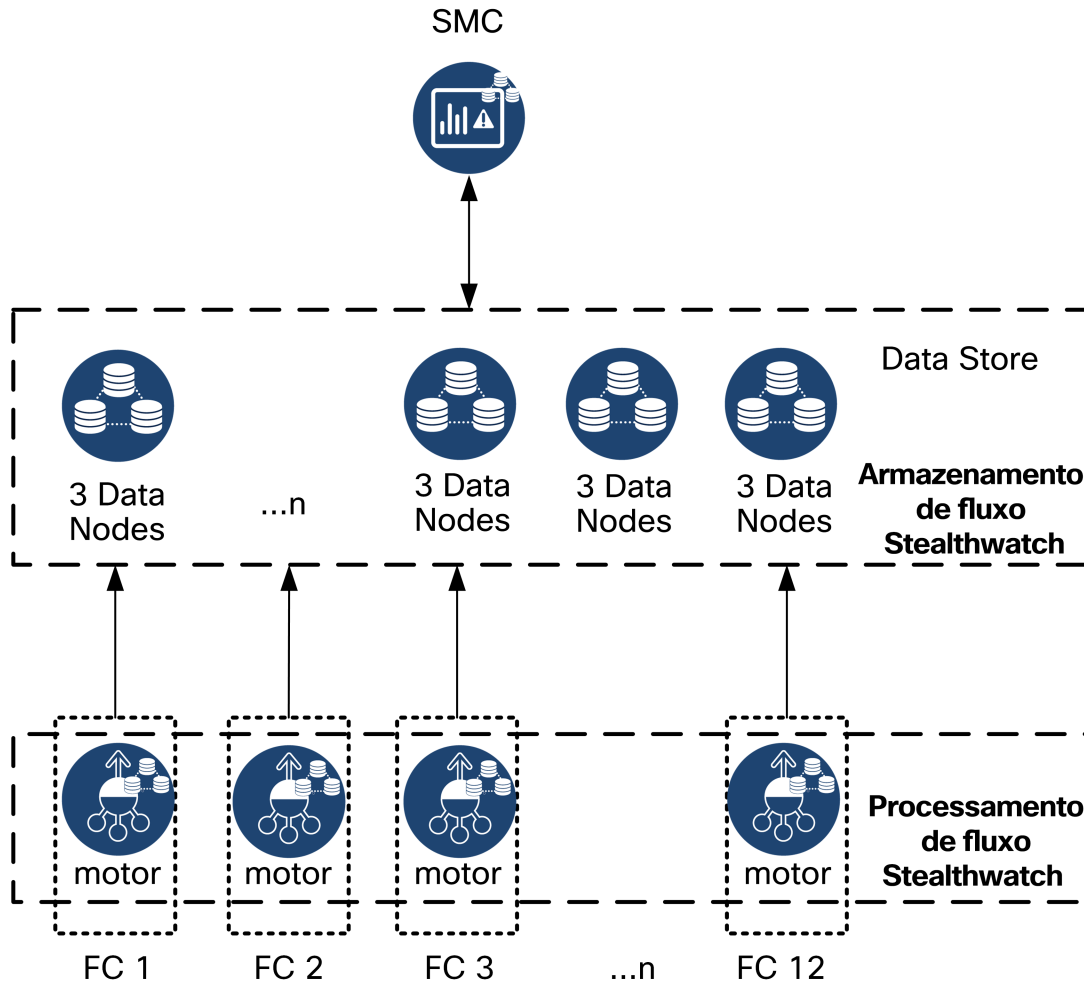


### Arquitetura de implementação do Data Store Stealthwatch

Numa implementação Stealthwatch tradicional sem um Data Store, um ou mais Coletores de fluxo ingerem e duplicam os dados, realizam análise e relatam dados e resultados diretamente ao SMC. Para resolver consultas submetidas pelo utilizador, incluindo gráficos e tabelas, o SMC consulta todos os Coletores de fluxo geridos. Cada Coletor de fluxo devolve resultados de correspondência ao SMC. O SMC recolhe informação de diferentes conjuntos de resultados e, em seguida, gera um gráfico ou tabela que apresenta os resultados. Nesta implementação, cada Coletor de fluxo armazena dados numa base de dados local. Consulte o diagrama seguinte para obter um exemplo.



Numa implementação Stealthwatch com um Data Store, o cluster Data Store situa-se entre o seu SMC e os Coletores de fluxo. Um ou mais Coletores de fluxo ingere e duplica os fluxos, realiza análise e relata dados e resultados diretamente para o Data Store, distribuindo de forma praticamente igual por todos os Nós de dados. O Data Store facilita o armazenamento de dados, mantém todo o seu tráfego nesse local centralizado, em vez de espalhado por vários Coletores de fluxo e oferece uma maior capacidade de armazenamento do que múltiplos Coletores de fluxo. Consulte o diagrama seguinte para obter um exemplo.



Para resolver consultas submetidas pelo utilizador, incluindo gráficos e tabelas, o SMC consulta o Data Store. O Data Store localiza os resultados correspondentes nas colunas relevantes para a consulta e, em seguida, obtém as linhas correspondentes e devolve os resultados da consulta ao SMC. O SMC gera o gráfico ou tabela sem necessidade de recolher múltiplos conjuntos de resultados de múltiplos Coletores de fluxo. Isto reduz o custo das consultas, em comparação com a consulta de múltiplos Coletores de fluxo, e melhora o desempenho de consulta.

Devido à arquitetura do Data Store, o SMC e todos os Coletores de fluxo têm de comunicar com o Data Store e têm de ser configurados durante a implementação para trabalhar com o Data Store. Não é possível ter um ambiente "combinado", com alguns Coletores de fluxo a relatar diretamente ao SMC e outros Coletores de fluxo a relatar ao Data Store.

### Arquitetura do Data Store Stealthwatch

Cada Data Store é composto por 3 ou mais Nós de dados. Cada Nós de dados é o seu próprio chassis de hardware. Quando compra um Data Store, recebe múltiplos chassis

de hardware de Nós de dados, correspondentes ao número de nós indicados por esse modelo de Data Store. Por exemplo, um DS 6200 Data Store fornece 3 chassis de hardware de Nós de dados.

Pode comprar mais de um Data Store para a sua implementação. Os Nós de dados podem ser agrupados em cluster como parte do seu Data Store em múltiplos de 3, entre um mínimo de 3 e um máximo de 36.



A Cisco recomenda que configure os seus Nós de dados de modo a que os Nós de dados numerados adjacentes sejam alimentados com fontes de alimentação separadas redundantes. Esta configuração melhora a redundância dos dados e o tempo de atividade geral do Data Store. Consulte [Requisitos e considerações sobre a implementação do Data Store](#) para mais informações.

Para implementar um Data Store, tem de atribuir o seguinte a cada Nós de dados:

- um endereço IP encaminhável para a gestão, ingestão e comunicações de consulta com os seus dispositivos Stealthwatch
- um endereço IP não encaminhável (bloco CIDR 169.254.42.0/24) numa LAN ou VLAN isolada para comunicações entre os Nós de dados como parte do cluster Data Store
- duas ligações 10G, uma para a gestão, ingestão e comunicações de consulta e uma para comunicações inter-Nós de dados
- opcionalmente, para redundância de rede e criticalidade das comunicações inter-Nós de dados, uma ligação 10G adicional e um switch adicional para estabelecimento de um canal de porta no Nós de dados

Consulte [Pré-requisitos e Recomendações sobre a Implementação do Data Store](#) para informações mais detalhadas sobre a implementação e pré-requisitos de implementação.

# Pré-requisitos e Recomendações sobre a Implementação do Data Store

A secção seguinte descreve a informação de pré-requisito e as recomendações para a sua implementação Data Store.



Se planear comprar um Data Store Stealthwatch, contacte os Serviços Profissionais da Cisco para obter apoio na instalação, implementação e configuração como parte da sua implementação Stealthwatch geral.

## Suporte de Versão Stealthwatch

Quando implementar um Data Store, todos os seus dispositivos Stealthwatch têm de ter a mesma versão (versão 7.3+).

## Licenças Stealthwatch

A sua implementação Stealthwatch requer uma Licença Flow Rate (FPS) Smart; o Data Store propriamente dito não requer uma licença adicional.

## Requisitos de compatibilidade de hardware e de ligação em rede Stealthwatch

A tabela seguinte fornece uma descrição geral do hardware necessário para implementar um Data Store.

Componente de hardware	Capacidade suportada
Data Store	<ul style="list-style-type: none"> <li>Mínimo de 3 Data Nodes (DS 6200)</li> <li>Conjuntos adicionais de 3 Nós de dados para expandir o Data Store, máximo de 36 Nós de dados</li> </ul>
Consola de gestão Stealthwatch	<ul style="list-style-type: none"> <li>Mínimo de 1 Consola de Gestão Stealthwatch</li> </ul>
Coletor de fluxo	<ul style="list-style-type: none"> <li>Mínimo de 1 Coletor de fluxo</li> </ul>

Note que tem de obter uma Licença Flow Rate (FPS) Smart para a sua implementação Stealthwatch geral.



Não atualize o dispositivo BIOS, pois pode provocar problemas na funcionalidade do dispositivo.

Se desejar implementar um Data Store, tem de ter, no mínimo, 3 Nós de dados. Um Data Store 6200 com 3 Nós de dados consegue gerir aproximadamente 500 000 fluxos por segundo e reter esses dados durante aproximadamente 90 dias. Pode expandir o seu Data Store com Nós de dados adicionais em múltiplos de 3, até um máximo de 36 Nós de dados.



Estas recomendações apenas consideram a telemetria. O seu desempenho pode variar consoante fatores adicionais, incluindo número de anfitriões, utilização de sensor de fluxo, perfis de tráfego e outras características de rede. Contacte o Suporte da Cisco para obter ajuda com o dimensionamento.



Atualmente, o Data Store não suporta a implementação de Nós de dados sobresselentes como substituições automáticas se um Nós de dados principal ficar inativo. Contacte o Suporte da Cisco para obter ajuda.

Tem de implementar um SMC com o seu Data Store e de configurá-lo para uma utilização com um Data Store. Se pretender uma elevada disponibilidade para o seu SMC, também pode implementar um SMC de ativação pós-falha.

Adicionalmente, tem de implementar, no mínimo, 1 Coletor de fluxo com o seu Data Store e de configurar os Coletores de fluxo para utilização com um Data Store.

Para cada SMC e Coletor de fluxo que implementar, tem de atribuir um endereço IP encaminhável público à porta de gestão `eth0`. Quando implementar um Data Store, pode configurar a utilização de uma porta 1G/10G de cobre BASE-T ou porta 10G de cabo twinax SFP+ para a porta de gestão `eth0` do SMC e Coletor de fluxo. A Cisco requer um débito de 10G para a porta de cobre BASE-T para utilização do Data Store. Os utilizadores que não utilizem um Data Store apenas podem configurar a interface de cobre de 100 Mbps/1 Gbps/10 Gbps como `eth0`.

Pode também implementar os Sensores de fluxo e UDP Directors para a sua implementação Stealthwatch. Como estes dispositivos não comunicam diretamente com o Data Store, não tem de os configurar para utilização com um Data Store.

Consulte as [Folhas de especificações](#) relevantes para mais informações sobre as plataformas suportadas. Consulte a [Matriz de compatibilidade da versão de hardware e software Stealthwatch](#) para mais informações sobre a compatibilidade da versão.

## Considerações de implementação empresarial Stealthwatch

Lembre-se do seguinte:

- Se configurar um Coletor de fluxo para compatibilidade com Data Store, a interface de administração de dispositivo (Administrador de dispositivo) oculta certas funcionalidades. Utilize a Gestão central para realizar a configuração do Coletor de fluxo e outras tarefas relacionadas. Se desejar monitorizar a estatística de armazenamento, transfira a aplicação Report Builder para o seu SMC.
- Utilize a Aplicação Web Stealthwatch para monitorizar e configurar a sua instalação Stealthwatch se implementar um Data Store. O Cliente de ambiente de trabalho Stealthwatch é incompatível com um Data Store.
- Se configurar o seu SMC para utilização com um Data Store, não poderá utilizar as aplicações ETA Cryptographic Audit ou Host Classifier.

## Credenciais necessárias para a implementação do Data Store

Prepare palavras-passe para as seguintes contas de utilizador:

- `root` e `sysadmin` para cada SMC, Nós de dados e Coletor de fluxo. Estes são atribuídos por si durante a configuração inicial do sistema.
- `admin` para cada SMC, Nós de dados e Coletor de fluxo. Estes são atribuídos por si utilizando a Ferramenta de configuração de dispositivo.
- `dbadmin` e `readonlyuser` para o Data Store. Estes são atribuídos por si quando inicializa o Data Store.

## Considerações sobre comutação e ligação de rede do Data Store

A tabela seguinte fornece uma descrição geral das considerações sobre comutação e ligação de rede quando implementa um Data Store.

Considerações sobre rede	Descrição
Credenciais necessárias	Para cada Nós de dados, Consola de Gestão Stealthwatch e Coletor de fluxo:

	<ul style="list-style-type: none"> <li>• Configurado durante a Configuração inicial do sistema: <code>root</code>, <code>sysadmin</code></li> <li>• Configurado utilizando a Ferramenta de configuração de dispositivo: <code>admin</code></li> <li>• Configurado durante a inicialização do Data Store: <code>dbadmin</code>, <code>readonlyuser</code></li> </ul>
Comunicações Inter-Nós de dados	<ul style="list-style-type: none"> <li>• Estabeleça uma latência de tempo de ida e volta (RTT) recomendada inferior a 200 microssegundos entre Nós de dados</li> <li>• Mantenha o desfasamento de relógio em 1 segundo ou menos entre os seus Nós de dados.</li> <li>• Estabeleça um débito recomendado de 6,4 Gbps ou superior (ligação comutada full duplex de 10 Gbps) entre os seus Nós de dados.</li> </ul>
Nós de dados Energia de hardware	<ul style="list-style-type: none"> <li>• Se ocorrer uma falha de energia num Nós de dados de hardware inesperadamente, os dados podem ser corrompidos. Utilize ambas as fontes de alimentação em circuitos separados de fontes de alimentação ininterruptas.</li> <li>• Quando inicializar o cluster do Data Store (consulte <a href="#">Inicialização e configuração do Data Store</a> para mais informações), alterne a configuração do Nós de dados com base nas fontes de alimentação que cada Nós de dados utiliza. Isto permite otimizar a tolerância a falhas minimizando o número de Nós de dados que ficam inativos se ocorrer uma falha de energia.</li> </ul>
Nós de dados Switching	<ul style="list-style-type: none"> <li>• Os Nós de dados requerem que a sua VLAN Camada 2 permita uma comunicação inter-Nós de dados. Os Nós de dados de hardware podem ser ligados a um switch 10G partilhado ou dedicado.</li> <li>• A Cisco recomenda que os Nós de dados de hardware sejam ligados a 2 switches para ajudar a garantir uma conectividade constante durante as falhas e atualizações de switch. Devido à baixa latência necessária para a comunicação inter-Nós de dados, a Cisco recomenda um par redundante de switches,</li> </ul>



	em que 2 switches são interligados e transportam a VLAN Camada 2 em ambos os switches.
Stealthwatch Comunicações de dispositivo	<ul style="list-style-type: none"> <li>• Acesso SSH e acesso root SSH necessários para SMC, Nós de dados e Coletores de fluxo e configurados a partir do SMC</li> <li>• O SMC e os Coletores de fluxo têm de poder alcançar todos os Nós de dados</li> <li>• Nós de dados têm de poder alcançar o SMC, todos os Coletores de fluxo e cada Nós de dados</li> </ul>

Tem de atribuir os seguintes endereços IP a cada Nós de dados:

- um endereço IP encaminhável para comunicação com os seus dispositivos Stealthwatch (`eth0`). Ligue a porta Nós de dados `eth0` à sua rede para permitir a comunicação com o seu SMC e os Coletores de fluxo. Pode configurar a utilização de uma porta 1G/10G de cobre BASE-T ou porta 10G de cabo twinax SFP+ para a porta de gestão Nós de dados `eth0`.

Durante a implementação e configuração do Data Store, mapeará os endereços IP Nós de dados `eth0` para o nome do Data Store para permitir uma distribuição mais uniforme do armazenamento de telemetria e pedido e resposta de consulta.

Consulte [Inicialização e configuração da base de dados do Data Store](#) para mais informações.

- um endereço IP não encaminhável numa LAN ou VLAN privada, a ser utilizado para uma comunicação inter-Nós de dados (`eth2` ou canal de porta com `eth2` e `eth3` para melhor débito e desempenho). Como parte do Data Store, os seus Nós de dados comunicam entre si. Ligue a porta Nós de dados `eth2` ou canal de porta com `eth2` e `eth3` aos switches para comunicação inter-Nós de dados.

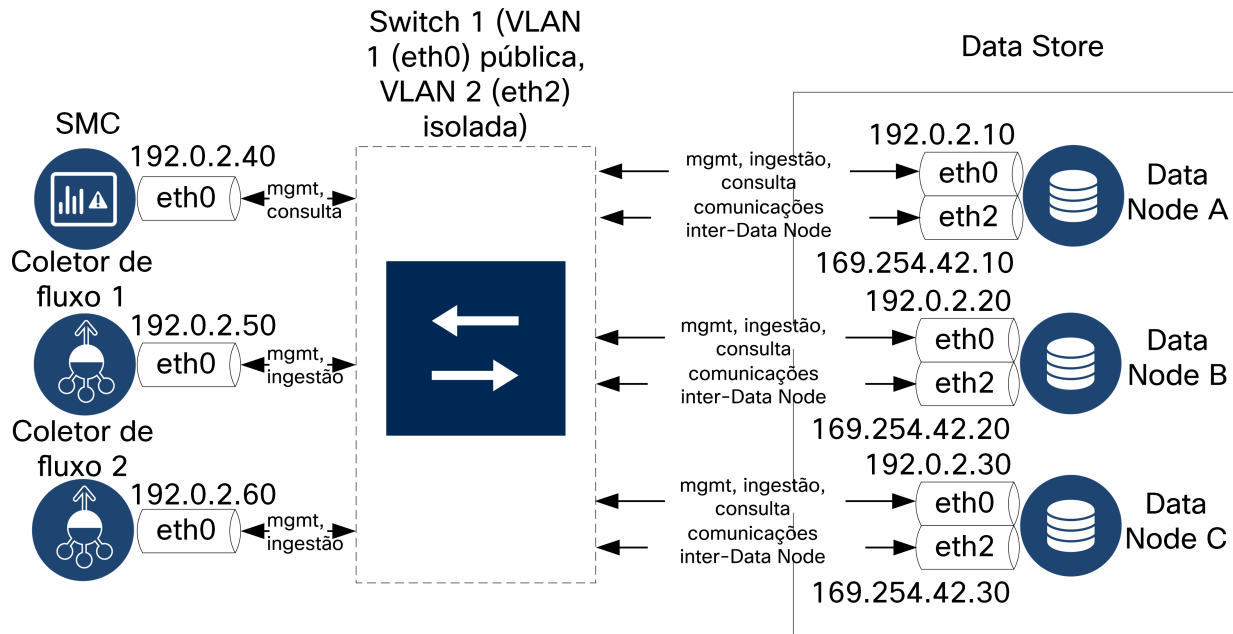


Tem de atribuir os endereços IP não encaminháveis de canal de porta `eth2` ou porta `eth2/eth3` do bloco CIDR `169.254.42.0/24`.

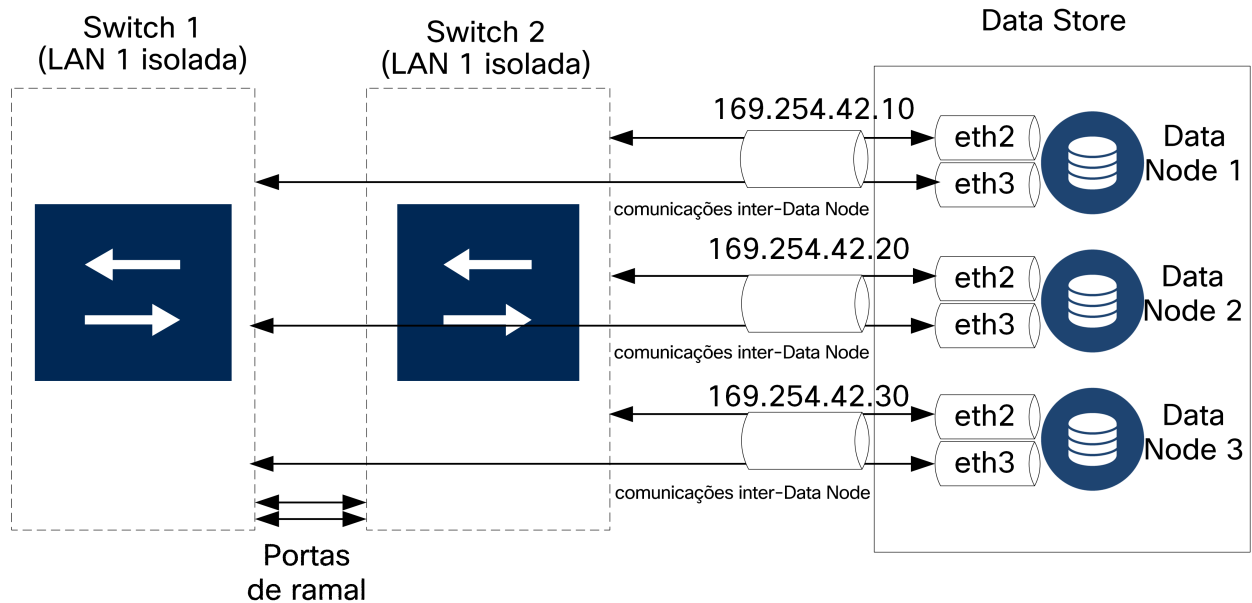
Configurar uma porta `eth2` para um débito de 10G é suficiente para uma comunicação inter-Nós de dados normal. Criar um canal de porta `eth2/eth3` para um débito até 20G permite uma comunicação mais rápida entre Nós de dados e uma adição ou substituição de Nós de dados mais rápida para o Data Store, já que cada novo Nós de dados recebe tráfego de Nós de dados adjacentes para o preenchimento dos seus dados.

Para ativar as comunicações inter-Nós de dados através do canal de porta `eth2` ou `eth2/eth3`, tem de implementar 1 switch que suporte velocidades de 10G. Configure

uma LAN ou VLAN pública para comunicações de Nós de dados `eth0` com o SMC e Coletores de fluxo e uma LAN ou VLAN isolada para comunicações inter-Nós de dados. Pode partilhar estes switches com outros dispositivos, mas deve criar LANs ou VLANs separadas para o tráfego de dispositivos adicional. Consulte o diagrama seguinte para obter um exemplo:



O cluster do Data Store requer um heartbeat contínuo entre os nós dentro da VLAN isolada. Sem este heartbeat, os Nós de dados podem, potencialmente, ficar offline, o que aumenta o risco de o Data Store ficar inativo. Se desejar uma redundância de rede adicional, para efetuar um planeamento de acordo com as atualizações de switch e interrupções planeadas, a Cisco recomenda que configure os seus Nós de dados com canais de porta para uma comunicação inter-Nós de dados dedicada. Ligue cada Nós de dados a 2 switches, com cada porta física ligada a um switch diferente. Consulte o diagrama seguinte para obter um exemplo:



Contacte os Serviços Profissionais da Cisco para obter assistência no planeamento da sua implementação.

## Requisitos e considerações sobre a implementação do Data Store

Posicione cada Nós de dados de forma a poder comunicar com todos os seus Coletores de fluxo, o seu SMC e Nós de dados. Para um melhor desempenho, defina os seus Nós de dados e Coletores de fluxo de forma a minimizar a latência de comunicação e os Nós de dados e SMC para um desempenho de consulta ideal. A Cisco recomenda vivamente que posicione os Nós de dados ao alcance da sua firewall, como dentro de um NOC. Considere o seguinte para o desempenho:

- Estabeleça uma latência de tempo de ida e volta (RTT) recomendada inferior a 200 microssegundos entre Nós de dados quando os implementar.
- Mantenha o desfaseamento de relógio em 1 segundo ou menos entre os seus Nós de dados.
- Estabeleça um débito recomendado de 6,4 Gbps ou superior (ligação comutada full duplex de 10 Gbps) entre os seus Nós de dados.

Se o Data Store ficar inativo devido a falha de energia ou falha de hardware, correrá um risco maior de corrupção ou perda de dados. A Cisco recomenda a instalação dos seus Nós de dados levando em consideração um tempo de atividade constante. Considere o seguinte:

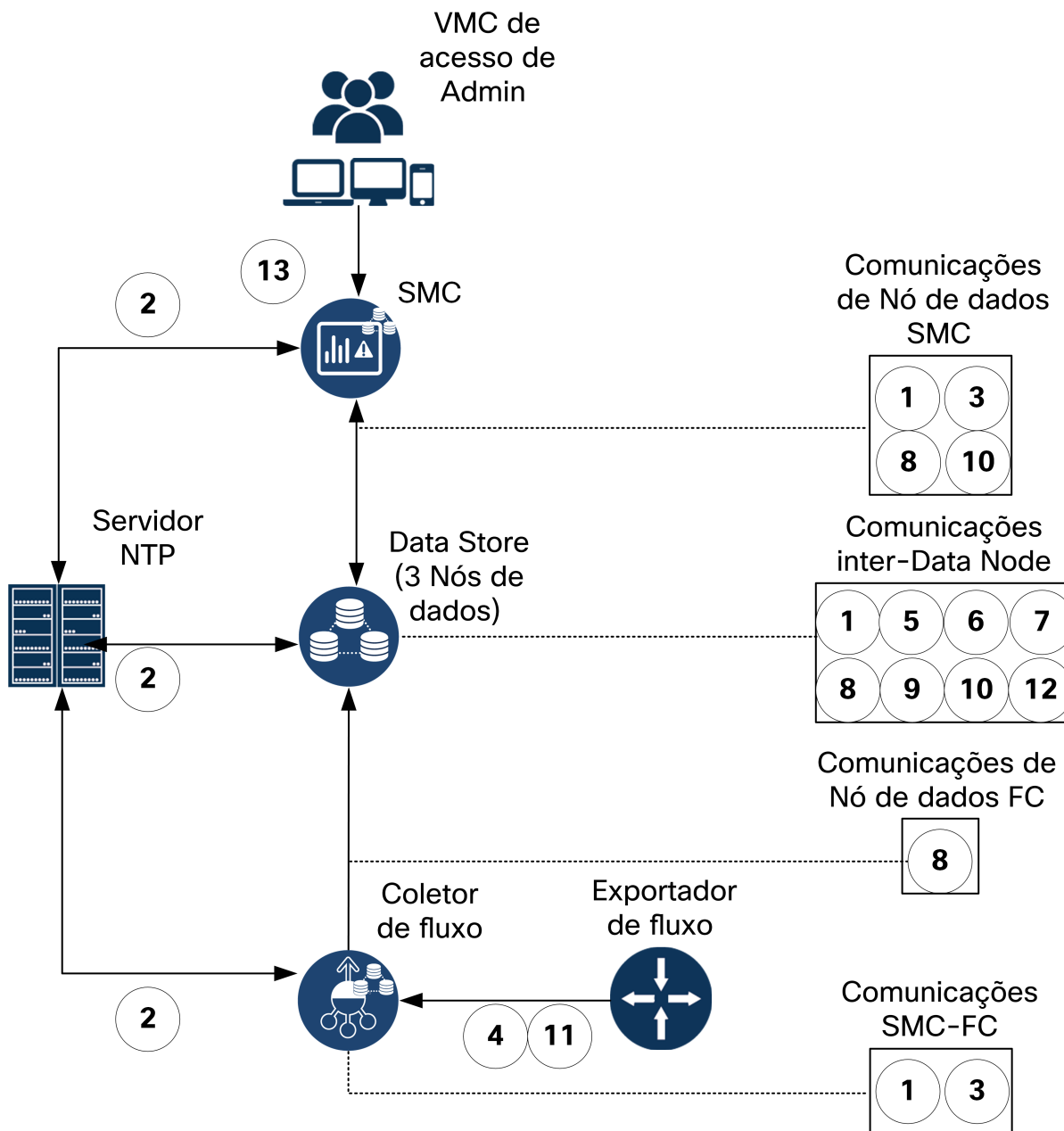
- A Cisco recomenda vivamente a instalação de fontes de alimentação redundantes ou ininterruptas para cada Nós de dados, para ajudar a prevenir a perda ou corrupção de dados em caso de falha de energia.
- Certifique-se de que a política de restabelecimento de energia do Nós de dados é definida para **Restaurar o último estado**, para reiniciar o Nós de dados automaticamente após uma falha de energia e tentar restaurar os processos em execução. Consulte o [Guia de configuração da GUI UCS C-Series](#) para mais informações sobre a configuração da política de restabelecimento de energia no CIMC.
- Quando inicializa o Data Store (consulte [Inicialização e configuração da base de dados do Data Store](#) para mais informações), altere a configuração do Nós de dados com base na fonte de alimentação. O Data Store cria uma cópia de segurança do Nós de dados no próximo Nós de dados sequencial durante a configuração e a última cópia de segurança do Nós de dados no primeiro Nós de dados configurado. Se implementar os seus Nós de dados em duas fontes de alimentação separadas e alternar Nós de dados pares e ímpares com base na fonte de alimentação, se uma fonte de alimentação ficar inativa e tiver um número par de nós, o Data Store pode permanecer ativo porque os dados ou dados de cópia de segurança do Nós de dados são acessíveis a partir dos Nós de dados alimentados.



Se ocorrer uma falha de energia inesperada num Nós de dados e o utilizador reiniciar o dispositivo, a instância da base de dados nesse Nós de dados pode não reiniciar automaticamente. Consulte [Resolução de problemas do Data Store](#) para informação sobre a reinicialização manual da instância da base de dados.

## Portas de comunicação do Data Store

O diagrama seguinte apresenta um exemplo de arquitetura de Stealthwatch com as portas de comunicação que devem ser abertas. Consulte a tabela para conhecer as portas associadas a cada chamada.




A secção seguinte apresenta as portas de comunicação a abrir na sua firewall para implementar o Data Store. Consulte o [Guia de configuração do sistema Stealthwatch](#) para portas de comunicação adicionais a abrir para a sua implementação Stealthwatch geral.

#	De (Cliente)	Para (Servidor)	Porta	Protocolo ou Finalidade
1	SMC	Coletores de fluxo e Nós de dados	22/TCP	SSH, necessário para inicializar a base de dados do Data Store
1	Nó de dados	todos os outros Nós de dados	22/TCP	SSH, necessário para inicializar a base de dados do Data Store e para tarefas de administração da base de dados
2	SMC, Coletores de fluxo e Nós de dados	Servidor NTP	123/UDP	NTP, necessário para sincronização de tempo
2	servidor NTP	SMC, Coletores de fluxo e Nós de dados	123/UDP	NTP, necessário para sincronização de tempo
3	SMC	Coletores de fluxo e Nós de dados	443/TCP	HTTPS, necessário para comunicações seguras entre dispositivos
3	Coletores de fluxo	SMC	443/TCP	HTTPS, necessário para comunicações seguras entre dispositivos
3	Nó de dados	SMC	443/TCP	HTTPS, necessário para comunicações seguras entre dispositivos
4	Exportadores NetFlow	Coletores de fluxo - NetFlow	2055/UDP	Ingestão NetFlow
5	Nó de dados	todos os outros Nós de dados	4803/TCP	Serviço de mensagens inter-Nós de dados


6	Nó de dados	todos os outros Nós de dados	4803/UDP	Serviço de mensagens inter-Nós de dados
7	Nó de dados	todos os outros Nós de dados	4804/UDP	Serviço de mensagens inter-Nós de dados
8	SMC, Coletores de fluxo e Nós de dados	Nó de dados	5433/TCP	Ligações de cliente Vertica
9	Nós de dados	todos os outros Nós de dados	5433/UDP	Monitorização do serviço de mensagens Vertica
10	SMC	Nó de dados	5444/TCP	Comunicações seguras da Consola de Gestão Vertica
10	Nó de dados	SMC e todos os outros Nós de dados	5444/TCP	Comunicações seguras da Consola de Gestão Vertica
11	Exportadores sFlow	Coletores de fluxo - sFlow	6343/UDP	Ingestão sFlow
12	Nó de dados	todos os outros Nós de dados	6543/UDP	Serviço de mensagens inter-Nós de dados
13	Estações de trabalho de administrador para acesso à Consola de Gestão Vertica	SMC	9450/TCP	Acesso de web browser da Consola de Gestão Vertica

# Descrição geral da implementação do Data Store Stealthwatch

 Se planejar comprar um Data Store, contacte os Serviços Profissionais da Cisco para obter apoio na instalação, implementação e configuração como parte da sua implementação Stealthwatch geral. **Não** instale um Data Store sozinho.

A secção seguinte descreve os passos de alto nível para a implementação de Data Store com uma implementação Stealthwatch:

- Implemente os seus dispositivos Stealthwatch, incluindo os seus Nós de dados e configure o seu SMC e Coletores de fluxo para utilização com um Data Store

 Certifique-se de que instala a versão e patch mais recentes para os seus dispositivos após os implementar, mas antes de continuar com a inicialização e configuração do Data Store.


- Prepare a sua implementação Stealthwatch para utilização de Data Store distribuindo as palavras-passe de utilizador e os certificados de identidade.
- Inicialize o Data Store
- Configure a Consola de Gestão Vertica (VMC) no seu SMC e ative as notificações e os limites de alerta
- Configure as definições de retenção do Data Store através da API REST
- Instale as aplicações Stealthwatch no seu SMC para funcionalidade relacionada com Data Store adicional

Consulte estas tarefas antes de iniciar a sua implementação.

Componente e tarefa necessários	Passos
Instalação e configuração do SMC	<p>Consulte <a href="#">Configuração do SMC para utilização com um Data Store</a> para mais informações.</p> <ol style="list-style-type: none"> <li>1. Implemente o seu SMC na sua rede.</li> <li>2. Utilizando CIMC ou ligando diretamente ao seu dispositivo, inicie a sessão na consola do SMC como <code>root</code>. Execute o</li> </ol>



	<p>script de Configuração do sistema <code>systemconfig</code> e utilize o assistente de configuração inicial para configurar informação de gestão básica, incluindo endereço IP de dispositivo, utilização com um Data Store e configuração de porta física <code>eth0</code>.</p> <ol style="list-style-type: none"> <li>3. A partir de um web browser, navegue para o endereço IP <code>eth0</code> do SMC para aceder à Ferramenta de configuração de dispositivo. Utilize a Ferramenta de configuração de dispositivo para configurar as palavras-passe de administrador, domínio de Stealthwatch, servidores DNS e NTP e para instalar a Gestão Central.</li> <li>4. A partir de um web browser, navegue para o endereço IP do SMC após configurar o dispositivo utilizando a Ferramenta de configuração de dispositivo para aceder à Aplicação Web Stealthwatch. A partir da Gestão Central, ative o acesso SSH e o acesso de root SSH ao SMC.</li> <li>5. Atualize o seu SMC para a versão e patch mais recentes. Consulte os <a href="#">guias de atualização</a> para mais informações sobre a atualização para a versão atual e os <a href="#">readmes de patch</a> para mais informação sobre atualizações de patch.</li> </ol>
<p>Instalação e configuração de Nó de dados</p>	<p>Consulte <a href="#">Implementação e configuração inicial do hardware do Data Store</a> para mais informações.</p> <ol style="list-style-type: none"> <li>1. Implemente os seus Nós de dados na sua rede.</li> <li>2. Utilizando CIMC ou ligando diretamente ao seu dispositivo, inicie a sessão na consola de cada Nós de dados como <code>root</code>. Execute o script de Configuração do sistema <code>systemconfig</code> e utilize o assistente de configuração inicial para configurar informação de gestão básica, incluindo o endereço IP de gestão de dispositivo e o endereço IP de comunicação inter-Nós de dados (com configuração de canal de porta opcional). Introduza um endereço IP não encaminhável para o canal de porta <code>eth2</code> ou <code>eth2/eth3</code> a partir do bloco CIDR <code>169.254.42.0/24</code>.</li> <li>3. Para cada Nós de dados, a partir de um web browser, navegue para o endereço IP encaminhável <code>eth0</code> do Nós de dados para aceder à Ferramenta de configuração de dispositivo. Utilize a</li> </ol>

	<p>Ferramenta de configuração de dispositivo em cada Nós de dados para configurar as palavras-passe de administrador, domínio de Stealthwatch, servidores DNS e NTP e para que a Gestão Central faça a gestão do Nós de dados.</p> <ol style="list-style-type: none"> <li>4. A partir da Aplicação Web Stealthwatch, acesse à Gestão Central e ative o acesso SSH e acesso root SSH a cada Nós de dados.</li> <li>5. Atualize os seus Nós de dados para a versão e patch mais recentes. Consulte os <a href="#">guias de atualização</a> para mais informações sobre a atualização para a versão atual e os <a href="#">readmes de patch</a> para mais informação sobre atualizações de patch.</li> </ol> <div style="border: 1px solid #00a0e3; padding: 10px; margin-top: 10px;"> <p>Consulte quaisquer guias de atualização aplicáveis e documentação readme de patch antes de continuar. O</p> <p> processo de atualização de Nós de dados requer passos adicionais em comparação com outros dispositivos Stealthwatch.</p> </div>
<p>Instalação e configuração do Coletor de fluxo</p>	<p>Consulte <a href="#">Configuração do Coletor de fluxo para utilização com um Data Store</a> para mais informações.</p> <ol style="list-style-type: none"> <li>1. Implemente os seus Coletores de fluxo na sua rede.</li> <li>2. Utilizando CIMC ou ligando diretamente ao seu dispositivo, inicie a sessão na consola de cada Coletor de fluxo como <code>root</code>. Execute o script de Configuração do sistema <code>systemconfig</code> e utilize o assistente de configuração inicial para configurar informação de gestão básica, incluindo endereço IP de dispositivo, utilização com um Data Store e configuração de porta física <code>eth0</code>.</li> <li>3. Para cada Coletor de fluxo, a partir de um web browser, navegue para o endereço IP <code>eth0</code> do Coletor de fluxo para aceder à Ferramenta de configuração de dispositivo. Utilize a Ferramenta de configuração de dispositivo em cada Coletor de fluxo para configurar as palavras-passe de administrador, domínio de Stealthwatch, servidores DNS e NTP , número de porta de coleção de fluxo (2055 para NetFlow ou 6343 para</li> </ol>

	<p>sFlow) e para que a Gestão Central faça a gestão do Coletor de fluxo.</p> <ol style="list-style-type: none"> <li>4. A partir da Aplicação Web Stealthwatch, aceda à Gestão Central e ative o acesso SSH e acesso root SSH a cada Coletor de fluxo.</li> <li>5. Atualize os seus Coletores de fluxo para a versão e patch mais recentes. Consulte os <a href="#">guias de atualização</a> para mais informações sobre a atualização para a versão atual e os <a href="#">readmes de patch</a> para mais informação sobre atualizações de patch.</li> </ol>
<p>Inicialização e configuração de Data Store</p>	<p>Consulte <a href="#">Inicialização e configuração da base de dados do Data Store</a> para mais informações.</p> <ol style="list-style-type: none"> <li>1. A partir da Aplicação Web Stealthwatch, aceda à Gestão Central e assegure que todos os Nós de dados e Coletores de fluxo são geridos na Gestão Central, que a ligação está ativa e que o acesso SSH e acesso root SSH estão ativados.</li> <li>2. Inicie a sessão na consola do SMC principal como <code>sysadmin</code>. Utilizando o script de conectividade segura de base de dados <code>setup-sw-datastore-secure-connectivity</code>, distribua as palavras-passe de <code>dbadmin</code> e <code>readonlyuser</code> de base de dados e os certificados de identidade pelo seu SMC, Nós de dados e Coletores de fluxo.</li> <li>3. Com base na indicação do script de conectividade segura <code>setup-sw-datastore-secure-connectivity</code>, inicie a sessão na consola do Nós de dados especificado como <code>root</code>. Copie o ficheiro de configuração de inicialização de base de dados de exemplo <code>install_SDBN_example.cfg</code> como <code>install_SDBN.cfg</code> e atualize-o com os seus endereços IP e subrede de Nós de dados. Execute o script de inicialização, consultando o ficheiro de configuração de inicialização (<code>python install_SDBN_initial.py -i install_SDBN.cfg</code>).</li> <li>4. A partir do Nós de dados em que executou o script de inicialização, obtenha a cadeia de caracteres da chave API a partir de <code>/opt/vertica/config/apikey.dat</code>. Utilizará</li> </ol>


	<p>esta chave API para estabelecer uma ligação entre a base de dados do Data Store e o VMC num passo posterior.</p> <ol style="list-style-type: none"> <li>5. A partir da Aplicação Web Stealthwatch, aceda à Gestão Central, e para o SMC e os Coletores de fluxo utilize a Resolução Local para mapear o nome de base de dados do Data Store (<code>sw-datastore</code>) para cada endereço IP encaminhável do Nós de dados. Para um desempenho ideal, mapeie os endereços IP do Nós de dados <code>eth0</code> pela mesma ordem para cada dispositivo.</li> </ol>
<p>Instalação e configuração da Consola de Gestão Vertica (VMC) no SMC</p>	<p>Consulte <a href="#">Configuração da Consola de Gestão Vertica</a> para mais informações.</p> <ol style="list-style-type: none"> <li>1. Copie o certificado de servidor <code>/lancope/var/admin/cds/ server.crt</code> do seu SMC para a sua estação de trabalho local.</li> <li>2. A partir de um web browser na sua estação de trabalho local, navegue para <code>[smc-ipv4-address]:9450/webui/login</code> para aceder ao VMC. Realize uma instalação e configuração inicial do VMC. Desative as ligações que utilizam versões menos seguras de TLS. Utilize a cadeia de caracteres da chave API e o ficheiro de certificado <code>server.crt</code> para estabelecer uma ligação com o Data Store. Configure os limites de alerta e as notificações de alerta para receber alertas do estado de funcionamento do Data Store.</li> </ol>
<p>Retenção de dados do Data Store</p>	<p>Consulte <a href="#">Configuração de retenção do Data Store</a> para mais informações.</p> <ul style="list-style-type: none"> <li>• Utilize a API REST para configurar o período de retenção do seu Data Store.</li> </ul>
<p>Consulte os passos seguintes após concluir a implementação do Data Store</p>	<p>Consulte os <a href="#">Passos seguintes da instalação do Data Store</a>:</p> <ol style="list-style-type: none"> <li>1. Instale a aplicação Stealthwatch Report Builder no seu SMC para executar relatórios na sua implementação Stealthwatch e para visualizar estatística de armazenamento do Data Store. Consulte as <a href="#">notas da versão</a> para mais informações.</li> </ol>

2. Consulte a ajuda online da Aplicação Web Stealthwatch para mais informações sobre como utilizar o Stealthwatch.

Opcionalmente, pode realizar o seguinte:


<b>Componente e tarefa opcionais</b>	<b>Passos</b>
Instalação e configuração do UDP Director	<ul style="list-style-type: none"> <li>• Implemente o UDP Director, conforme descrito no <a href="#">Guia de instalação de hardware do Stealthwatch x2xx Series</a> e <a href="#">Guia de configuração do sistema Stealthwatch</a>. Atualize o seu UDP Director para a versão e patch mais recentes. Consulte os <a href="#">guias de atualização</a> para mais informações sobre a atualização para a versão atual e os <a href="#">readmes de patch</a> para mais informação sobre atualizações de patch.</li> </ul>
Sensor de fluxo	<ul style="list-style-type: none"> <li>• Implemente o Sensor de fluxo, conforme descrito no <a href="#">Guia de instalação de hardware do Stealthwatch x2xx Series</a> e <a href="#">Guia de configuração do sistema Stealthwatch</a>. Atualize o seu Sensor de fluxo para a versão e patch mais recentes. Consulte os <a href="#">guias de atualização</a> para mais informações sobre a atualização para a versão atual e os <a href="#">readmes de patch</a> para mais informação sobre atualizações de patch.</li> </ul>
Instalação e configuração do SMC de ativação pós-falha	<ul style="list-style-type: none"> <li>• Implemente o SMC de ativação pós-falha, conforme descrito no <a href="#">Guia de instalação de hardware do Stealthwatch x2xx Series</a>, <a href="#">Guia de configuração do sistema Stealthwatch</a> e <a href="#">Guia de configuração de ativação pós-falha Stealthwatch</a>. Atualize o seu SMC para a versão e patch mais recentes. Consulte os <a href="#">guias de atualização</a> para mais informações sobre a atualização para a versão atual e os <a href="#">readmes de patch</a> para mais informação sobre atualizações de patch.</li> </ul>


# Instalação de hardware do Data Store

-  Se planejar comprar um Data Store Stealthwatch, contacte os Serviços Profissionais da Cisco para obter apoio na instalação, implementação e configuração como parte da sua implementação Stealthwatch geral.

## Implementação e considerações sobre o hardware Stealthwatch

Implemente e configure os seus dispositivos SMC, Nós de dados e Coletor de fluxo Stealthwatch com base nas seguintes instruções e instale os switches para o Data Store, na sua rede. Quando implementar os seus Nós de dados e os ligar à sua rede, consulte [Requisitos e considerações sobre a implementação do Data Store](#). Assegure que o seu SMC, Nós de dados e Coletores de fluxo têm a mesma versão (7.3+). Consulte o [Manual de instalação do hardware Stealthwatch x210 Series](#) ou **Anexo A. Preparação da instalação** e **Anexo B. Instalação de hardware Stealthwatch** para mais informações sobre a instalação e configuração do dispositivo inicial.

-  Se desejar implementar um Data Store na sua rede como parte de uma implementação Stealthwatch existente, trabalhe em colaboração com os Serviços Profissionais da Cisco para integrar o Data Store. Contacte o Suporte da Cisco para mais informações.

-  Utilize a Aplicação Web Stealthwatch para monitorizar e configurar a sua instalação Stealthwatch se implementar um Data Store. O Cliente de ambiente de trabalho Stealthwatch é incompatível com um Data Store.


## Configuração do SMC para utilização com um Data Store


Implemente e configure o seu SMC para utilização com um Data Store e para gerir os seus Nós de dados e Coletores de fluxo.

Se tiver um SMC secundário, configure esse primeiro, para que o SMC principal possa comunicar com o mesmo. Consulte o [Guia de configuração do sistema Stealthwatch](#) para mais informações sobre o estabelecimento de um par SMC de ativação pós-falha. Consulte [Implementação da consola de gestão Stealthwatch de ativação pós-falha](#) para mais contexto sobre a implementação e configuração de um SMC secundário para trabalhar com um Data Store.

Realize o seguinte:

1. Primeiro, implemente o seu SMC na sua rede. Em seguida, ligue o seu dispositivo CIMC, um teclado e um monitor ou computador portátil e inicie a sessão na consola como `root`. Execute `systemconfig` e utilize o Assistente de configuração inicial para atualizar as definições da porta de gestão, utilize com um Data Store e as palavras-passe de utilizador de `root` e `sysadmin`. Consulte o [Manual de instalação do hardware Stealthwatch x210 Series](#) ou [Anexo A. Preparação da instalação](#) e [Anexo B. Instalação de hardware Stealthwatch](#) para mais informação.

 Apenas na primeira vez que acede à Configuração do sistema, o sistema irá conduzi-lo à Configuração inicial, que o acompanha através do processo de configuração inicial do dispositivo.

 Se optar por configurar o seu SMC ou Coletor de fluxo para utilização com um Data Store, não pode atualizar a configuração do dispositivo para alterar esta configuração. Tem de submeter o dispositivo a RFD se selecionar a opção errada. Ative esta opção apenas se planear implementar um Data Store na sua rede.

2. Em seguida, num web browser, navegue para o endereço IP que tiver atribuído à porta de gestão. Utilize a Ferramenta de configuração de dispositivo para realizar uma configuração adicional, incluindo a atribuição da palavra-passe do utilizador `admin` (e as palavras-passe de utilizador de `root` e `sysadmin` se não as tiver atribuído durante a Configuração do sistema), configuração de domínio Stealthwatch, outra configuração de rede, definições de DNS e NTP e instalação da Gestão Central no SMC. Consulte o [Guia de configuração do sistema Stealthwatch](#) ou o [Anexo C. Configurar os seus dispositivos](#) para mais informações.
3. Em seguida, ative o acesso SSH e acesso root SSH no seu SMC. Para inicializar o Data Store, conforme descrito em [Inicialização e configuração do Data Store](#),

tem de executar um script baseado em acesso SSH para cada dispositivo.



Quando o SSH está ativado, o risco de comprometer o sistema aumenta. É importante ativar o SSH apenas quando necessita do mesmo. Quando parar de utilizar o SSH, desative-o.

## Atualize a permissão de acesso SSH do SMC:

### Antes de começar

- Inicie a sessão na Aplicação Web SMC como administrador do sistema.

### Procedimento

1. Aceda ao Painel do Gestor de Dispositivos. Tem as seguintes opções:
  - A Ferramenta de configuração de dispositivo abre-se no painel do Gestor de dispositivos se tiver concluído a configuração de dispositivo.
  - Clique no ícone **Definições globais**. Selecione **Gestão Central**. O Painel do Gestor de Dispositivos aparece.
2. Para a entrada linha-item SMC, clique no menu Ações e selecione **Editar configuração de dispositivo**.
3. Selecione o separador Dispositivo.
4. No painel SSH , selecione **Ativar SSH**.
5. Selecione **Ativar acesso root SSH**.
6. Clique em **Aplicar Definições**.

### O que fazer a seguir

- Atualize o seu SMC para a versão e patch mais recente, conforme descrito no passo seguinte.
1. Por fim, atualize o seu SMC para a versão e patch mais recentes. Consulte os [guias de atualização](#) para mais informações sobre a atualização para a versão atual e os [readmes de patch](#) para mais informação sobre atualizações de patch.

Após atualizar o seu SMC, tem as seguintes opções:

- Regressar à Descrição geral da implementação do Data Store [Stealthwatch](#) para rever o processo de implementação.
- Implementar e configurar os seus Nós de dados conforme descrito na secção seguinte.



## Implementação e configuração inicial do hardware do Data Store

Após implementar o seu SMC, implemente e configure os seus dispositivos Nós de dados. Quando implementar os seus Nós de dados e os ligar à sua rede, consulte [Requisitos e considerações sobre a implementação do Data Store](#).

Para cada Nós de dados, realize o seguinte:

1. Primeiro, implemente o Nós de dados na rede. Em seguida, ligue ao dispositivo Nós de dados com CIMC, um teclado e um monitor ou computador portátil e inicie a sessão na consola como `root`. Execute `systemconfig` e utilize o Assistente de configuração inicial para atualizar as definições da porta de gestão, as definições de porta de comunicação inter-Nós de dados e as palavras-passe de utilizador de `root` e `sysadmin`. Consulte o [Manual de instalação do hardware Stealthwatch x210 Series](#) ou [Anexo A. Preparação da instalação](#) e [Anexo B. Instalação de hardware Stealthwatch](#) para mais informações.



Apenas na primeira vez que acede à Configuração do sistema, o sistema irá conduzi-lo à Configuração inicial, que o acompanha através do processo de configuração inicial do dispositivo.

2. Em seguida, num web browser, navegue para o endereço IP que tiver atribuído à porta de gestão. Utilize a Ferramenta de configuração de dispositivo para realizar uma configuração adicional, incluindo a atribuição da palavra-passe do utilizador `admin` (e as palavras-passe de utilizador de `root` e `sysadmin` se não as tiver atribuído durante a Configuração do sistema), configuração de domínio Stealthwatch, outra configuração de rede, definições de DNS e NTP e possibilitar a gestão do Nós de dados através da Gestão Central. Consulte o [Guia de configuração do sistema Stealthwatch](#) ou o [Anexo C. Configurar os seus dispositivos](#) para mais informações.
3. Por fim, ative o acesso SSH e acesso root SSH no seu Nós de dados. Para inicializar o Data Store, conforme descrito em [Inicialização e configuração do Data Store](#), tem de executar um script baseado em acesso SSH para cada dispositivo.



Quando o SSH está ativado, o risco de comprometer o sistema aumenta. É importante ativar o SSH apenas quando necessita do mesmo. Quando parar de utilizar o SSH, desative-o.

# Atualize uma permissão de acesso SSH do Nós de dados:

## Antes de começar

- Inicie a sessão na Aplicação Web SMC como administrador do sistema.

## Procedimento

1. Acesse ao Painel do Gestor de Dispositivos. Tem as seguintes opções:
  - A Ferramenta de configuração de dispositivo abre-se no painel do Gestor de dispositivos se tiver concluído a configuração de dispositivo.
  - Clique no ícone **Definições globais**. Selecione **Gestão Central**. O Painel do Gestor de Dispositivos aparece.

Consulte a lista de dispositivos e confirme que o seu Nós de dados está na lista e que o seu Estado de Dispositivo é **Ativo**.

2. Para a entrada linha-item Nós de dados, clique no menu Ações e selecione **Editar configuração de dispositivo**.
3. Selecione o separador Dispositivo.
4. No painel SSH , selecione **Ativar SSH**.
5. Selecione **Ativar acesso root SSH**.
6. Clique em **Aplicar Definições**.

## O que fazer a seguir

- Atualize o seu Nós de dados para a versão e patch mais recente, conforme descrito no passo seguinte.
1. Por fim, atualize o seu Data Node para a versão e patch mais recentes. Consulte os [guias de atualização](#) para mais informações sobre a atualização para a versão atual e os [readmes de patch](#) para mais informação sobre atualizações de patch.



Consulte quaisquer guias de atualização aplicáveis e documentação readme de patch antes de continuar. O processo de atualização de Nós de dados requer passos adicionais em comparação com outros dispositivos Stealthwatch.

Após atualizar o seu Nós de dados, tem as seguintes opções:

- Regressar à Descrição geral da implementação do Data Store [Stealthwatch](#) para rever o processo de implementação.
  - Regressar à **Implementação e configuração inicial do hardware do Data Store** e repetir este processo de instalação e configuração inicial do Nós de dados, configuração da Ferramenta de configuração de dispositivo e configuração de Gestão Central para os seus Nós de dados restantes.
2. Após ter implementado e configurado todos os seus Nós de dados, tem as seguintes opções:
- Configurar o seu UDP Director, se tiver um, conforme descrito na secção seguinte.
  - Configurar os seus Coletores de fluxo, se não tiver um UDP Director, conforme descrito em **Configuração do Coletor de fluxo para utilização com um Data Store**.

## Implementação do UDP Director

Se desejar implementar um UDP Director, siga as instruções do [Guia de instalação de hardware do Stealthwatch x210 Series](#) e [Guia de configuração do sistema Stealthwatch](#). Note que o processo de instalação do UDP Director permanece inalterado, independentemente de implementar ou não um Data Store. Não tem de configurar um UDP Director para utilização com um Data Store.

Após implementar o seu UDP Director, tem as seguintes opções:

- Regressar à Descrição geral da implementação do Data Store [Stealthwatch](#) para rever o processo de implementação.
- Implementar e configurar os seus Coletores de fluxo, conforme descrito na secção seguinte.

## Configuração do Coletor de fluxo para utilização com um Data Store

Após configurar os seus Nós de dados e UDP Directors, se os tiver implementado, implemente e configure os seus Coletores de fluxo.

Para cada Coletor de fluxo, realize o seguinte:

1. Primeiro, implemente o Coletor de fluxo na sua rede. Em seguida, ligue ao Coletor de fluxo com CIMC, um teclado e um monitor ou computador portátil e inicie a sessão na consola como `root`. Execute `systemconfig` e utilize o Assistente de

configuração inicial para atualizar as definições da porta de gestão, utilize com um Data Store e as palavras-passe de utilizador de `root` e `sysadmin`. Consulte o [Manual de instalação do hardware Stealthwatch x210 Series](#) ou **Anexo**

**A. Preparação da instalação** e **Anexo B. Instalação de hardware Stealthwatch** para mais informações.



Apenas na primeira vez que acede à Configuração do sistema, o sistema irá conduzi-lo à Configuração inicial, que o acompanha através do processo de configuração inicial do dispositivo.



Se optar por configurar o seu SMC ou Coletor de fluxo para utilização com um Data Store, não pode atualizar a configuração do dispositivo para alterar esta configuração. Tem de submeter o dispositivo a RFD se selecionar a opção errada. Ative esta opção apenas se planear implementar um Data Store na sua rede.

2. Em seguida, num web browser, navegue para o endereço IP que tiver atribuído à porta de gestão. Utilize a Ferramenta de configuração de dispositivo para realizar uma configuração adicional, incluindo a atribuição da palavra-passe do utilizador `admin` (e palavras-passe de utilizador de `root` e `sysadmin` se não as tiver atribuído durante uma Configuração do sistema), seleção de domínio Stealthwatch, outra configuração de rede, definições de DNS e NTP, número de porta de coleção de fluxo (2055 para NetFlow ou 6343 para sFlow) e possibilitar que o Coletor de fluxo seja gerido pela Gestão Central. Consulte o [Guia de configuração do sistema Stealthwatch](#) ou o **Anexo C. Configurar os seus dispositivos** para mais informações.



Se configurar um Coletor de fluxo para utilização com um Data Store, a interface de administração de dispositivo (Administrador de dispositivo) oculta certas funcionalidades. Utilize a Gestão central para realizar a configuração do Coletor de fluxo e outras tarefas relacionadas. Se desejar monitorizar a estatística de armazenamento, transfira a aplicação Data Store Storage Statistics para o seu SMC.

3. Por fim, ative o acesso SSH e acesso root SSH nos seus Coletores de fluxo. Para inicializar o Data Store, conforme descrito em **Inicialização e configuração do Data Store**, tem de executar um script baseado em acesso SSH para cada dispositivo.



Quando o SSH está ativado, o risco de comprometer o sistema aumenta. É importante ativar o SSH apenas quando necessita do mesmo. Quando parar de utilizar o SSH, desative-o.

## Atualize uma permissão de acesso a SSH do Coletor de fluxo:

### Antes de começar

- Inicie a sessão na Aplicação Web SMC como administrador do sistema se não estiver a utilizar a Ferramenta de configuração de dispositivo.

### Procedimento

1. Aceda ao Painel do Gestor de Dispositivos. Tem as seguintes opções:
  - A Ferramenta de configuração de dispositivo abre-se no painel do Gestor de dispositivos se tiver concluído a configuração de dispositivo.
  - Clique no ícone **Definições globais**. Selecione **Gestão Central**. O Painel do Gestor de Dispositivos aparece.

Consulte a lista de dispositivos e confirme que o seu Coletor de fluxo está na lista e que o seu Estado de Dispositivo é **Ativo**.

2. Para a entrada linha-item do Coletor de fluxo, clique no menu Ações e selecione **Editar configuração de dispositivo**.
3. Selecione o separador Dispositivo.
4. No painel SSH , selecione **Ativar SSH**.
5. Selecione **Ativar acesso root SSH**.
6. Clique em **Aplicar Definições**.

### O que fazer a seguir

- Atualize o seu Coletores de fluxo para a versão e patch mais recente, conforme descrito no passo seguinte.
1. Por fim, atualize o seu Coletores de fluxo para a versão e patch mais recentes. Consulte os [guias de atualização](#) para mais informações sobre a atualização para a versão atual e os [readmes de patch](#) para mais informação sobre atualizações de patch.

Após atualizar o seu Coletores de fluxo, tem as seguintes opções:

- Regressar à Descrição geral da implementação do Data Store [Stealthwatch](#) para rever o processo de implementação.
  - Para cada um dos seus Coletores de fluxo, repita o processo descrito em [Configuração do Coletor de fluxo para utilização com um Data Store](#) de instalação e configuração do Coletor de fluxo, configuração através da Ferramenta de configuração de dispositivo e configuração da Gestão Central para os seus Coletores de fluxo restantes.
2. Após ter implementado e configurado todos os seus Coletores de fluxo, tem as seguintes opções:
- Configure o seu Sensor de fluxo se tiver um, conforme descrito na secção seguinte.
  - Configure o seu SMC secundário, se tiver um, conforme descrito em [Implementação da consola de gestão Stealthwatch de ativação pós-falha](#).
  - Se não tiver um Sensor de fluxo ou SMC secundário, inicialize e configure o Data Store, conforme descrito em [Inicialização e configuração do Data Store](#).

## Implementação do sensor de fluxo

Se desejar implementar um Sensor de fluxo, siga as instruções do [Guia de instalação de hardware do Stealthwatch x210 Series](#) e [Guia de configuração do sistema Stealthwatch](#). Note que o processo de instalação do Sensor de fluxo permanece inalterado, independentemente de implementar ou não um Data Store. Não tem de configurar um Sensor de fluxo para utilização com um Data Store.

Após ter implementado e configurado o seu Sensor de fluxo, tem as seguintes opções:

- Regressar à Descrição geral da implementação do Data Store [Stealthwatch](#) para rever o processo de implementação.
- Configure o seu SMC secundário como SMC de ativação pós-falha se tiver um, conforme descrito na secção seguinte.
- Se não tiver um SMC secundário, inicialize o Data Store, conforme descrito em [Inicialização e configuração do Data Store](#).

## Implementação da consola de gestão Stealthwatch de ativação pós-falha

Se tiver um SMC secundário que pretenda configurar como SMC de ativação pós-falha, siga as instruções no [Guia de instalação do hardware do Stealthwatch x210 Series](#),

[Guia de configuração do sistema Stealthwatch](#) e [Guia de configuração de ativação pós-falha Stealthwatch](#).

Após terminar a configuração do SMC secundário e com o SMC principal a geri-lo através da Gestão Central, tem as seguintes opções:

- Regressar à Descrição geral da implementação do Data Store [Stealthwatch](#) para rever o processo de implementação.
- Se tiver um SMC secundário e promover o seu SMC secundário a SMC principal, é necessária uma configuração adicional antes de utilizar novamente o script `setup-sw-datastore-secure-connectivity`. Consulte [Copiar informação de confiança do Data Store para um SMC de ativação pós-falha](#) para mais informações.
- Inicialize e configure o Data Store, conforme descrito em [Inicialização e configuração do Data Store](#).

## Inicialização e configuração do Data Store

Após implementar e configurar o seu SMC, Nós de dados e Coletores de fluxo, inicialize e configure o Data Store. Certifique-se de que todos os seus SMCs, Nós de dados e Coletores de fluxo são atualizados para a versão e patch mais recentes antes de continuar.



Se tiver um SMC secundário e promover o seu SMC secundário a SMC principal, é necessária uma configuração adicional antes de utilizar novamente o script `setup-sw-datastore-secure-connectivity`. Consulte [Copiar informação de confiança do Data Store para um SMC de ativação pós-falha](#) para mais informações.

Realize o seguinte:

1. Primeiro, assegure que todos os Nós de dados, Coletores de fluxo e SMC secundário, se tiver implementado um, são geridos através da Gestão Central e que todos têm SSH e o acesso root SSH ativado.
2. Em seguida, a partir do SMC, execute um script para distribuir as palavras-passe de Data Store `dbadmin` e `readonlyuser` e certificados de identidade para comunicações seguras de Data Store com os seus dispositivos Stealthwatch.
3. Em seguida, a partir do Nós de dados especificado no passo anterior, execute um script para inicializar o Data Store e estabelecer ligações seguras entre os Nós de dados e os seus dispositivos Stealthwatch.

4. Por fim, na Gestão Central, mapeie um nome de Data Store interno (`sw-datastore`) para os endereços IP do Nós de dados no seu SMC e Coletores de fluxo para melhorar a distribuição de carga e o desempenho de consulta do Nós de dados.

## Certifique-se de que os seus Nós de dados e Coletores de fluxo são geridos através da Gestão Central:

### Antes de começar

- Faça uma lista de todos os endereços IP e nomes de anfitrião de Nós de dados e Coletor de fluxo que espera que sejam geridos na Gestão Central.
- Inicie a sessão na Aplicação Web SMC como administrador do sistema e aceda à Gestão Central.

### Procedimento

1. No Inventário de dispositivos, compare a sua lista de Nós de dados, Coletores de fluxo e SMC secundário, se tiver implementado um, com a lista no Inventário e certifique-se de que o **Estado de Dispositivo** de cada um é **Ativo**. **Não** continue com a inicialização do Data Store até todos os seus dispositivos esperados serem geridos e o seu **Estado de Dispositivo** ser **Ativo**.

Se um estado do dispositivo for **Inativo**, reveja a sua configuração de dispositivo e a ligação entre o SMC e esse dispositivo.

Se um dispositivo não aparecer no Inventário, adicione o dispositivo.

2. Para cada dispositivo, clique no menu Ações e selecione **Editar configuração de dispositivo**.
3. Selecione o separador Dispositivo. Assegure que **Ativar SSH** e **Ativar acesso root SSH** estão selecionados. **Não** continue com a inicialização do Data Store até todos os seus dispositivos esperados terem o acesso SSH e acesso root SSH ativados.

Se um ou ambos não estiverem selecionados, selecione a opção e, em seguida, clique em **Aplicar definições**.

## Distribua as palavras-passe de Data Store pelo seu SMC, Nós de dados e Coletores de fluxo:

A partir da interface de linha de comando do SMC, pode executar um script que prepara



a sua implementação de Stealthwatch para a inicialização do Data Store distribuindo a informação necessária para estabelecer ligações seguras de Data Store. A primeira opção do script permite-lhe criar palavras-passe para as contas de utilizador `dbadmin` e `readonlyuser` e fazer a sua distribuição em segurança pelo SMC, Nós de dados e Coletores de fluxo. Cada palavra-passe tem de cumprir os seguintes requisitos:

- no mínimo, 1 número
- no mínimo, 1 carácter de minúsculas
- no mínimo, 1 carácter de maiúsculas
- no mínimo, 1 carácter especial da lista seguinte: `<> . , ? / ' " | : ; ` ~ ! @ # $ % ^ & * ( ) - _ + = { } [ ]`
- no mínimo, 8 caracteres, sem comprimento máximo
- apenas caracteres com codificação ASCII

Quando executa um script para inicializar o Data Store, o script utiliza esta informação para definir as credenciais das contas de utilizador `dbadmin` e `readonlyuser` e estabelecer ligações seguras entre cada dispositivo e o Data Store.



Se definir estas palavras-passe e as perder em seguida, contacte o Suporte da Cisco para assistência na sua recuperação.

Note que utilizará esta opção quando implementa pela primeira vez o Data Store. Se já tiver inicializado o Data Store e pretender atualizar estas palavras-passe, consulte [Atualizar as palavras-passe de dbadmin e readonlyuser Data Store](#) para mais informações.

### Antes de começar

- Efetue uma compilação de uma lista de palavras-passe `root` para o seu SMC, Nós de dados, Coletores de fluxo e um SMC secundário se tiver implementado um.
- Inicie a sessão na consola do SMC como `root`.

### Procedimento

1. A partir da linha de comandos, introduza `cd /lancope/admin/cds` e prima `Enter` para alterar os diretórios.
2. Introduza `./setup-sw-datastore-secure-connectivity` e prima `Enter` para executar o script `bash` de conectividade segura do Data Store.
3. A partir do menu principal do script, seleccione **1. Distribua a palavra-passe do**

## SW DataStore pelos dispositivos.

O script apresenta uma lista de SMC, Nós de dados geridos pelo SMC, Coletores de fluxo suportados por Data Store geridos pelo SMC e qualquer SMC secundário suportado por Data Store gerido pelo SMC principal.

4. Confirme a lista de dispositivos e selecione **OK**. Na primeira vez que executa este script quando configura a sua implementação de Stealthwatch ou utilização de Data Store, todos os dispositivos são selecionados.
5. Na linha de comandos, quando lhe for solicitada a palavra-passe `root` para cada dispositivo, introduza a palavra-passe e prima Enter.



Uma vez que introduz múltiplas palavras-passe, certifique-se de que introduz a palavra-passe correta para o respetivo dispositivo.

Após introduzir todas as palavras-passe `root` dos dispositivos, o script pede-lhe as palavras-passe de `dbadmin` e `readonlyuser`.

6. Introduza a palavra-passe de **dbadmin**.
7. Introduza a mesma palavra-passe de `dbadmin` no campo **dbadmin (confirmação)**.
8. Introduza a palavra-passe de **readonlyuser**.
9. Introduza a mesma palavra-passe de `readonlyuser` no campo **readonlyuser (confirmação)**.



Não introduza a mesma palavra-passe para `dbadmin` e `readonlyuser`. A atribuição da mesma palavra-passe provoca uma falha do script e a não atribuição de palavra-passe a qualquer uma das contas de utilizador.

10. Selecione **OK**.

O script distribui estas palavras-passe de forma segura pelos dispositivos selecionados. Quando termina, apresenta uma lista dos dispositivos atualizados.

11. Selecione **OK** para regressar ao menu principal do script.

## O que fazer a seguir

- Distribua os certificados de identidade do Data Store para comunicações seguras, conforme descrito no procedimento seguinte.

## Distribua certificados de identidade para comunicações seguras de Data Store com os seus dispositivos

No script para estabelecer ligações seguras de Data Store, a segunda opção permite-lhe gerar um certificado de identidade e distribuí-lo pelo SMC, Nós de dados e Coletores de fluxo. Quando executa um script para inicializar o Data Store, o script utiliza este certificado de identidade para estabelecer ligações seguras entre os seus dispositivos e o Data Store.

O certificado de identidade é auto-assinado, válido por 5 anos e emitido para o nome comum `sw-datastore.stealthwatch.cisco.com`.

### Antes de começar

- A partir da linha de comandos SMC, execute o script `setup-sw-datastore-secure-connectivity`.

### Procedimento

1. A partir do menu principal do script, seleccione **2. Distribua os Certificados para Ligação DB Segura**.
2. O script apresenta uma lista de SMC, Nós de dados geridos pelo SMC, Coletores de fluxo geridos pelo SMC e qualquer SMC secundário gerido pelo SMC principal.  
Se já tiver confirmado a lista dos dispositivos após seleccionar **1. Distribua a palavra-passe do SW DataStore pelos dispositivos**, o script pode não apresentar esta lista de dispositivos. Avance para o passo 4.
3. Confirme a lista de dispositivos e seleccione **OK**. Na primeira vez que executa este script quando configura a sua implementação de Stealthwatch ou utilização de Data Store, todos os dispositivos são seleccionados.

O script gera um certificado de identidade, a ser utilizado para comunicações seguras e a chave privada emparelhada.

4. Na linha de comandos, quando lhe for solicitada a palavra-passe `root` para cada dispositivo, introduza a palavra-passe e prima Enter.



Uma vez que introduz múltiplas palavras-passe, certifique-se de que introduz a palavra-passe correta para o respetivo dispositivo.

5. Se o script for bem sucedido, apresenta uma mensagem de sucesso e um endereço IP de Nós de dados. No procedimento seguinte, inicie a sessão na consola desse Nós de dados utilizando o SSH para executar o script de inicialização do Data Store.



Grave este endereço IP antes de sair desta mensagem. Não é possível recuperá-lo após sair da mensagem.

## O que fazer a seguir

- Inicialize o Data Store, conforme descrito no procedimento seguinte.

## Execute um script para inicializar o Data Store e assegure ligações seguras

Após distribuir as palavras-passe de utilizador `dbadmin` e `readonlyuser` e o certificado de identidade pelos seus dispositivos, inicie a sessão no Nós de dados, conforme especificado no procedimento anterior, modifique o ficheiro de configuração `install_SDBN.cfg` e execute o script de inicialização `install_SDBN.initial.py`. Este script inicializa o Data Store, ligando os seus Nós de dados, define as credenciais de `dbadmin` e `readonlyuser` fornecidas e assegura o requisito de ligações seguras entre os seus dispositivos Stealthwatch e o Data Store.

Após inicializar o Data Store, copie a chave API do Data Store principal deste Nós de dados. Utilizará esta informação na [Configuração da Consola de Gestão Vertica](#) para instalar a Consola de Gestão Vertica (VMC) no seu SMC.

### Antes de começar

- Faça a compilação de uma lista de todos os seus endereços IP públicos Nós de dados `eth0` e endereços IP privados de canal de porta `eth2` ou `eth2/eth3`.
- Como `root`, inicie a sessão na consola do Nós de dados cujo endereço IP foi apresentado após ter distribuído certificados de identidade utilizando o script de ligação segura do Data Store, conforme descrito em [Distribua certificados de identidade para comunicações seguras de Data Store com os seus dispositivos](#).

### Procedimento

1. A partir da linha de comandos, introduza `cd /lancope/database` e prima Enter para alterar os diretórios.
2. Introduza `cp install_SDBN_example.cfg install_SDBN.cfg` e prima Enter para efetuar uma cópia do ficheiro de configuração de exemplo.
3. Introduza `vi install_SDBN.cfg` e prima Enter para modificar o ficheiro de configuração num editor de texto.

4. Crie secções [nodeN] numeradas consecutivamente de forma a corresponder ao número de Nós de dados que implementou. Por exemplo, se tiver implementado 6 Nós de dados, o seu ficheiro inclui o seguinte:

```
[node1]
private = 169.254.42.30
public = 10.0.16.30
[node2]
private = 169.254.42.31
public = 10.0.16.31
[node3]
private = 169.254.42.32
public = 10.0.16.32
[node4]
private = 169.254.42.33
public = 10.0.16.33
[node5]
private = 169.254.42.34
public = 10.0.16.34
[node6]
private = 169.254.42.35
public = 10.0.16.35
[common]
subnet = 10.0.16.0
```

5. Começando pela secção [node1], introduza os endereços IP privados (canal de porta eth2 ou eth2/eth3) e públicos (eth0) para cada Nó de dados. Lembre-se do seguinte:
  - Este script atribui Nós de dados ao Data Store pela ordem que estão listados. Se tiver implementado os seus Nós de dados com fontes de alimentação redundantes, alterne a atribuição de nó com base na fonte de alimentação para maximizar o tempo de atividade geral e a redundância de dados do Data Store.
  - Os endereços IP privados devem ser não encaminháveis, numa LAN ou VLAN privada. Tem de atribuir endereços IP no bloco CIDR 169.254.42.0/24.
  - Não sobreponha endereços IP entre Nós de dados.
  - Apenas adicione Nós de dados que pretende que façam parte do Data Store.

6. Na secção `[common]`, atualize a `subnet` para ser o endereço IP mais baixo no bloco CIDR de endereço IP público.
7. Prima Esc, introduza `:wq` e prima Enter para guardar as suas alterações e sair do editor de texto.
8. A partir da linha de comandos, introduza `python install_SDBN_initial.py -i install_SDBN.cfg` e prima Enter para executar a inicialização do script python do Data Store. Este script utiliza o ficheiro de configuração `install_SDBN.cfg` para inicializar os Nós de dados pela ordem que tiver especificado.

Após o script terminar, reveja as mensagens de estado CLI para garantir que o script foi bem sucedido.

Para cada Nós de dados, a consola indica `Prerequisites not fully met during local (OS) configuration` e lista uma série de mensagens de registo: `HINT (S0305), HINT (S0041), HINT (S0040), WARN (N0010), FAIL (s0180) e FAIL (s0311)`. Estas mensagens de registo são antecipadas e não indicam uma falha na inicialização do Data Store. Consulte [Resolução de problemas na implementação do Data Store](#) para mais informações sobre estas mensagens.

Para cada Nós de dados, a consola indica `INFO 6403: SSLCA config parameter is not set; client certificates will not be requested or verified`. Estas mensagens de registo são antecipadas e não indicam uma falha no estabelecimento de ligações seguras com o Data Store. Consulte [Resolução de problemas na implementação do Data Store](#) para mais informações sobre estas mensagens.

9. Introduza `cd /opt/vertica/config` para alterar os diretórios.
10. Introduza `cat apikeys.dat` para exibir a cadeia de caracteres da chave API na consola.
11. Copie a cadeia de caracteres da chave API e cole-a num editor de texto simples. Utiliza esta chave API na [Configuração da Consola de Gestão Vertica](#) para configurar o VMC no seu SMC.
12. Anote o endereço IP deste Data Node. Utiliza este endereço IP na [Configuração da Consola de Gestão Vertica](#) para configurar o VMC no seu SMC.

## O que fazer a seguir

- Utilize a Resolução Local na Gestão Central para mapear os endereços IP do Nós de dados para o nome do Data Store, conforme descrito no procedimento seguinte.

## Mapeie o nome do Data Store para os seus Nós de dados utilizando a Resolução Local

Após inicializar o Data Store, utilize a Gestão Central para mapear o nome do Data Store (`sw-datastore`) para todos os seus endereços IP do Nós de dados para o seu SMC e Coletores de fluxo. Como o Data Store contém múltiplos Nós de dados, este mapeamento de Resolução Local ajuda a distribuir o armazenamento de fluxo e pedidos de consulta de forma mais uniforme nos seus Nós de dados, melhorando o desempenho e a resposta.



Para um desempenho ideal, mapeie os endereços IP `eth0` do Nós de dados pela **mesma ordem** para cada dispositivo.


### Antes de começar

- Faça uma compilação de uma lista de todos os endereços IP públicos do seu Nós de dados.
- Faça uma compilação de uma lista dos seus Coletores de fluxo geridos na Gestão Central.
- Inicie a sessão na Aplicação Web SMC como administrador e aceda à Gestão Central.

### Procedimento

1. Começando pelo SMC, clique no menu Ações e selecione **Editar configuração de dispositivo**.
2. Selecione o separador Serviços de rede.
3. Na secção Resolução local, clique em **Adicionar novo**.
4. Introduza `sw-datastore` no campo **Nome de anfitrião**.
5. Introduza o primeiro endereço IP público do Nós de dados da sua lista.
6. Clique em **Adicionar**.
7. Repita os três passos anteriores para todos os seus Nós de dados restantes, utilizando a lista de endereços IP públicos do Nós de dados.
8. Clique em **Aplicar definições** e confirme as suas alterações.

9. Repita este procedimento para todos os seus Coletores de fluxo da sua lista e o seu SMC secundário se tiver implementado um.

 Para um desempenho ideal, mapeie os endereços IP `eth0` do Nós de dados pela **mesma ordem** para cada dispositivo.


### O que fazer a seguir

- Regressar à Descrição geral da implementação do Data Store [Stealthwatch](#) para rever o processo de implementação.
- Configure a Consola de Gestão Vertica (VMC) no seu SMC. Consulte a secção seguinte para mais informações.

## Configuração da Consola de Gestão Vertica

Após inicializar e configurar o Data Store, configure a Consola de Gestão Vertica (VMC) no seu SMC para ligar ao Data Store. Pode utilizar o VMC para monitorizar o estado do Data Store e receber notificações com base nos limites configuráveis. Realize o seguinte:

1. A partir de um web browser na sua estação de trabalho local, realize a configuração inicial do VMC, incluindo a configuração do VMC para desativar a utilização de TLS 1.0 e 1.1 para acesso de web browser e notificações de e-mail.
2. No VMC, configure uma ligação segura com o seu Data Store.
3. No VMC, configure notificações automáticas (como e-mail) e limites de notificação.

 Se utilizar a opção **3. Atualize a palavra-passe do SW DataStore nos dispositivos** em `setup-sw-datastore-secure-connectivity` para atualizar a palavra-passe de `dbadmin` após a definir inicialmente. Tem de iniciar a sessão no VMC como `dbadmin` para atualizar manualmente a palavra-passe. Consulte [Atualizar as palavras-passe de dbadmin e readonlyuser do Data Store após a inicialização](#) para mais informações.

## Realize uma configuração inicial do VMC

Realiza uma configuração inicial do VMC na primeira vez que acede ao VMC.

Por predefinição, o VMC permite ligações TLS 1.0 e TLS 1.1 a partir de um web browser. Como estas versões mais antigas de TLS são menos seguras do que TLS 1.2+, configure o VMC para não permitir quaisquer ligações através de TLS 1.0 e TLS 1.1.



## Antes de começar

- Tenha disponível o seu endereço SMC IPv4.
- Assegure que a porta de comunicação 9450/TCP está aberta entre a sua estação de trabalho e o SMC.

## Procedimento

1. Na sua estação de trabalho, abra um web browser e introduza `https://[smc-ipv4-address]:9450/webui/login` na barra de endereço. Substitua `[smc-ipv4-address]` pelo endereço IPv4 do seu SMC. Navegue para esse URL.
2. Aceite a licença Vertica e, em seguida, clique em **Seguinte**.
3. Introduza a palavra-passe de **dbadmin** e introduza-a em **Confirmar palavra-passe**.



Esta conta de utilizador de `dbadmin` é uma conta de utilizador VMC que é mais tarde mapeada para a sua conta de utilizador de Data Store `dbadmin`. Pode atribuir a esta conta uma palavra-passe diferente da atribuída à sua conta de utilizador de Data Store `dbadmin`.

4. Introduza `dbadmin` como **Nome de grupo Unix**.
5. Não altere os caminhos de ficheiro predefinidos (`/home/dbadmin`) ou a porta predefinida (5450) e, em seguida, clique em **Seguinte**.  
São apresentadas as opções de armazenamento.
6. Clique em **Next** (Seguinte).  
São apresentadas as opções de autorização da consola de gestão.
7. Clique em **Next** (Seguinte). Aguarde pelo reinício do serviço Vertica.  
Podem ser necessários 20 minutos ou mais. Se a janela de browser não atualizar automaticamente, atualize a página.
8. Introduza as suas credenciais de `dbadmin` e clique em **Iniciar sessão** para iniciar sessão no VMC.
9. A partir da página principal do VMC, clique em **Definições de MC**.
10. Clique no separador Configuração.
11. Selecione **Desativar ligações TLS 1.0 e 1.1 do browser** e, em seguida, guarde as suas alterações.

## Configure uma ligação segura de VMC ao Data Store

Antes de começar a configurar esta ligação segura, copie o ficheiro `/lancope/var/admin/cds/server.crt` do seu SMC para a sua estação de trabalho local. Utilizará este ficheiro para estabelecer uma ligação segura entre a VMC e o Data Store.

### Antes de começar

- Copie o ficheiro `/lancope/var/admin/cds/server.crt` do seu SMC para a sua estação de trabalho local.
- Tenha disponível uma cópia da sua chave API principal do Data Store, conforme descrito em [Execute um script para inicializar o Data Store e assegure ligações seguras](#).
- Tenha disponível o endereço IP do Nós de dados a partir do qual copiou a chave API, conforme descrito em [Execute um script para inicializar o Data Store e assegure ligações seguras](#).

### Procedimento

1. A partir da página principal do VMC , clique em **Importar um cluster de base de dados Vertica**.
2. Introduza o **endereço IP** do endereço IP Nós de dados `eth0` a partir do qual copiou a chave API e, em seguida, clique em **Seguinte**.
3. Opcionalmente, altere o **Nome do cluster**.
4. Introduza a chave API principal do Data Store e clique em **Continuar**.  
O VMC localiza o Data Store.
5. Introduza o `dbadmin` como **Nome do utilizador** e a palavra-passe `dbadmin`.
6. Selecione **Utilizar TLS**.
7. Clique em **Configurar TLS e Importar DB**.  
Aparece a janela Configurar certificados de ligação TLS.
8. Clique em **Configurar ligação TLS**.
9. Selecionar **Carregar um novo Certificado CA** e, em seguida, clique em **Seguinte**.
10. Clique em **Pesquisar** e, em seguida, selecione o ficheiro `server.crt` que guardou na sua estação de trabalho local a partir do SMC.
11. Introduza `sw-datastore-cert` como alias de **Certificado CA** e clique em **Seguinte**.
12. Clique em **Rever**.

13. Clique em **Configurar TLS para DB**.

O VMC configura ligações seguras ao Data Store.

14. Clique em **Fechar**.



Pode ver a mensagem "Error while importing database on MC. undefined". Esta mensagem é antecipada e não indica uma falha no estabelecimento de uma ligação segura ao Data Store.

## Configure notificações de alerta de VMC através e-mail

Pode configurar o VMC para enviar notificações de alerta de e-mail.

### Antes de começar

- Inicie a sessão no VMC como `dbadmin`.

### Procedimento

1. A partir da página Definições de MC, clique no separador Gateway de e-mail.
2. Introduza um **Servidor SMTP (Nome de anfitrião)**. Pode introduzir um nome com até 255 caracteres ou um endereço IP.
3. Introduza uma **porta de servidor SMTP**.
4. Selecione **Utilizar TLS** para **Tipo de sessão (SSL ou TLS)**.
5. Introduza um **Nome do utilizador SMTP**.
6. Introduza uma **Palavra-passe SMTP**.
7. Introduza um **Alias de e-mail de origem**, a partir do qual o VMC enviará alertas de e-mail.
8. Clique em **Testar** para testar as suas definições.  
Atualize as definições se não receber um e-mail de teste.
9. Clique em **Aplicar**.

## Configure o limite de alerta do VMC

Pode configurar vários limites mínimos e máximos de acordo com os quais a VMC gera um alerta se o Data Store exceder um valor de limite.

### Antes de começar

- Inicie a sessão no VMC como `dbadmin`.

## Procedimento

1. Selecione **Definições > Limites**.
2. Selecione uma caixa de verificação de item de linha de limite de notificação de alerta para ativar ou anule a seleção da caixa de verificação para desativar. A Cisco recomenda a ativação da notificação `Node State Change` para receber notificações quando um Nós de dados fica inativo.



Quando configura limites mínimos, pode criar notificações excessivas de falso positivo. Por exemplo, se definir o seu limite mínimo de CPU de nó, isso pode ser desencadeado frequentemente quando ocorrem flutuações de utilização da CPU.

3. Selecione *Prioridade 1* para cada limite de notificação de acordo com o qual pretende receber e-mails.
4. Se seleccionar *Prioridade 1*, clique no ícone de procura junto a **Destino de e-mail**.
5. Introduza um endereço de e-mail em **Introduzir novo campo** e clique no ícone **+**.
6. Clique em **OK**.
7. Selecione um **Intervalo de e-mail** para determinar a frequência de e-mail quando o Data Store exceder um limite.
8. Clique em **Aplicar**.

## O que fazer a seguir

- Regressar à Descrição geral da implementação do Data Store [Stealthwatch](#) para rever o processo de implementação.
- Configure a retenção de dados do seu Data Store, conforme descrito na secção seguinte.

---

# Configuração de retenção do Data Store

Por predefinição, o Data Store retém dados por um máximo de sete (7) dias antes de os eliminar automaticamente. Utilizando a API REST Stealthwatch, pode alterar este período de retenção:

- para um número de dias diferente, até 3000, ou
- armazenar os dados durante tanto tempo quanto possível, até o Data Store atingir a sua capacidade máxima.

Note o seguinte sobre a retenção do Data Store:

- Após atualizar as definições de retenção de dados, não tem de reiniciar qualquer dispositivo Stealthwatch ou o Data Store. As definições têm efeito após alguns minutos.
- Quando altera a retenção para um período mais longo, tem de aguardar que a diferença de tempo expire para que os dados armazenados correspondam exatamente às definições de retenção. Até esse momento, os dados são exibidos com a resolução mais reduzida (ou seja, mais grosseira). Por exemplo, se alterar a retenção de 3 dias para 10 dias, terá de aguardar 7 dias para que os dados armazenados correspondam exatamente às definições de retenção.
- Os seus dados podem ser eliminados mais cedo do que o período de retenção que selecionar, devido a um corte crítico dos dados de acordo com a utilização do disco. Se optar por armazenar dados durante o máximo de tempo possível, quando o Data Store atingir a capacidade máxima, o sistema começa a eliminar os dados mais antigos.
- Se não desejar armazenar dados, pode aceder à interface do utilizador de Administrador para cada um dos seus Coletores de fluxo e selecionar **Suporte > Definições avançadas**. Para cada Coletor de fluxo, altere a entrada "interface\_retention\_days" na coluna da Etiqueta Opção para 0 (zero) e reinicie o seu Coletor de fluxo (ou motor de Coletor de fluxo, se disponível).

Para atualizar estas definições, utilize a API REST para realizar o seguinte:

## Autentique segundo a API REST do SMC

Solicite informação de recurso

Recursos	Descrição
URI	<code>https://[smc-eth0-ip]/token/v2/authenticate</code>
Descrição	Autentique segundo a API REST do SMC.
Parâmetro URI	<ul style="list-style-type: none"> <li><code>[smc-eth0-ip]</code> - Endereço IP de gestão eth0 de SMC</li> </ul>
Método HTTP	POST
Corpo do pedido Tipo MIME	<code>application/x-www-form-urlencoded</code>
Corpo do pedido	<code>username=[username]&amp;password=[password]</code>
Parâmetros do corpo do pedido	<ul style="list-style-type: none"> <li><code>[username]</code> - (NECESSÁRIO) utilizador administrador SMC</li> <li><code>[password]</code> - (NECESSÁRIO) palavra-passe para a conta de utilizador administrador SMC</li> </ul>

#### Definição e código da resposta de sucesso

Resposta	Descrição
Código da resposta	200 - Sucesso
Corpo da resposta	O corpo da resposta contém informação de cookies, a qual tem de passar nas chamadas de API REST subsequentes para esta sessão. A sua sessão é válida durante 20 minutos.

### Recupere as definições de retenção de dados atuais do Data Store

Solicite informação de recurso

Recursos	Descrição
URI	<code>https://[smc-eth0-ip]/smc-configuration/rest/v1/cds/retentionsettings</code>

Recursos	Descrição
Descrição	Recupere as definições de retenção de dados atuais do Data Store.
Parâmetro URI	<ul style="list-style-type: none"> <li><code>[smc-eth0-ip]</code> - Endereço IP de gestão eth0 de SMC</li> </ul>
Método HTTP	GET
Corpo do pedido Tipo MIME	n/a
Corpo do pedido	n/a
Parâmetros do corpo do pedido	n/a


#### Informação e código da resposta de sucesso

Recursos	Descrição
Código da resposta	200 - Sucesso
Corpo da resposta	O corpo da resposta contém as definições de retenção de dados do Data Store atuais. Se não as tiver alterado anteriormente, o valor predefinido é de 7 dias.

### Atualize as definições de retenção de dados do Data Store

#### Solicite informação de recurso

Recursos	Descrição
URI	<code>https://[smc-eth0-ip]/smc-configuration/rest/v1/cds/retentionsettings</code>
Descrição	Atualize as definições de retenção de dados atuais do Data Store.

Recursos	Descrição
Parâmetro URI	<ul style="list-style-type: none"> <li><code>[smc-eth0-ip]</code> - Endereço IP de gestão eth0 de SMC</li> </ul>
Método HTTP	PUT
Corpo do pedido Tipo MIME	application/json
Corpo do pedido	<pre>{   "interfaceRetentionType": "[type]",   "interfaceRetentionAmount": "[#]" }</pre>
Parâmetros do corpo do pedido	<ul style="list-style-type: none"> <li><code>[type]</code> - (NECESSÁRIO) O tipo de retenção de dados, definido para um dos seguintes valores de cadeia: <ul style="list-style-type: none"> <li>AMOUNT - Armazene os dados até o número de dias definido em <code>interfaceRetentionAmount</code> antes de os eliminar</li> <li>FOREVER - Armazene os dados durante o máximo de tempo possível, até ser atingida a capacidade máxima do Data Store antes de os eliminar</li> </ul> </li> <li><code>[#]</code> - (NECESSÁRIO) O número máximo de dias durante os quais o Data Store retém os dados antes de os eliminar, definido para um número inteiro entre 1-3000.</li> </ul> <div style="border: 1px solid #00a0e3; padding: 10px; margin-top: 10px;"> <p>Se definir <code>interfaceRetentionType</code> para <code>FOREVER</code>, terá ainda assim de passar um <code>interfaceRetentionAmount</code>, que o sistema  ignora. Armazena o valor internamente como 7 como valor predefinido, independentemente do <code>interfaceRetentionAmount</code> que passar nesta situação.</p> </div>

### Informação e código da resposta de sucesso



Recursos	Descrição
Código da resposta	204 - Sucesso (Sem conteúdo)
Corpo da resposta	O corpo da resposta não tem conteúdo.

Consulte a Documentação de API REST [Stealthwatch Enterprise](#) para mais informações sobre a API REST.

O procedimento seguinte fornece a sintaxe curl para atualizar o período de retenção de dados do Data Store:

## Atualize o período de retenção do Data Store:

### Antes de começar

- Inicie a sessão na consola de um dispositivo baseado em Linux com curl instalado.

### Procedimento

1. Copie o comando seguinte e cole-o num editor de texto simples:

```
curl -c cookies.txt -d "username=[username]&password=[password]" https://[smc-eth0-ip]/token/v2/authenticate
```

2. Substitua `[username]` por um nome do utilizador administrador SMC.
3. Substitua `[password]` pela palavra-passe de administrador SMC.
4. Substitua `[smc-eth0-ip]` pelo endereço IP `eth0` do SMC.
5. Copie o comando atualizado, cole-o na linha de comandos e prima Enter para autenticar no SMC para utilização de API REST.

A sua sessão é válida durante 20 minutos.

6. Copie o comando seguinte e cole-o num editor de texto simples:

```
curl -X GET -b cookies.txt https://[smc-eth0-ip]/smc-configuration/rest/v1/cds/retentionsettings
```

7. Substitua `[smc-eth0-ip]` pelo endereço IP `eth0` do SMC.
8. Copie o comando atualizado, cole-o na linha de comandos e prima Enter para recuperar as definições de retenção atuais do Data Store.

Se esta é a primeira vez que está a verificar, o Data Store está configurado com um período de retenção predefinido de 7 dias.

9. Copie o comando seguinte e cole-o num editor de texto simples:

```
curl -X PUT -b cookies.txt -H "Content-Type:application/json" -d '{"interfaceRetentionType": "[type]", "interfaceRetentionAmount": "[#]"}' https://[smc-eth0-ip]/smc-configuration/rest/v1/cds/retentionsettings
```

10. Substitua `[type]` por um dos seguintes:

- `AMOUNT` se desejar definir um número de dias para retenção.
- `FOREVER` se desejar armazenar dados durante o máximo de tempo possível.

11. Substitua `[#]` por um número inteiro entre 1–3000 para o número de dias de retenção.

Tem de definir este valor mesmo que defina `[type]=FOREVER`. Neste caso, o sistema ignora este valor e define-o como 7 internamente.

12. Substitua `[smc-eth0-ip]` pelo endereço IP `eth0` do SMC.
13. Copie o comando atualizado, cole-o na linha de comandos e prima Enter para atualizar as definições de retenção.



Após atualizar as definições de retenção, não tem de reiniciar qualquer dispositivo Stealthwatch ou o Data Store. As definições têm efeito após alguns minutos. No entanto, quando altera a retenção para um período mais longo, tem de aguardar que a diferença de tempo expire para que os dados armazenados correspondam exatamente às definições de retenção.

## O que fazer a seguir

- Regresse à Descrição geral da implementação do Data Store [Stealthwatch](#) para rever o processo de implementação.
- Reveja os passos seguintes, conforme descrito na próxima secção.

# Passos seguintes da instalação do Data Store

Após implementar e configurar a sua implementação do Stealthwatch para utilização com um Data Store:

- Instale a aplicação Stealthwatch Report Builder no seu SMC para executar relatórios na sua implementação Stealthwatch e para visualizar estatística de armazenamento do Data Store. Consulte as [notas da versão](#) para mais informações.
- Consulte a ajuda online da Aplicação Web Stealthwatch para mais informações sobre como utilizar o Stealthwatch.
- Regresse à Descrição geral da implementação do Data Store [Stealthwatch](#) para rever o processo de implementação.

# Manutenção do Data Store

A secção seguinte descreve o Data Store e tarefas de manutenção relacionadas com o Data Store, incluindo:

- reiniciar um Nós de dados e o Data Store
- cópia de segurança e restauro do Data Store
- adicionar, remover e substituir Nós de dados
- copiar informação de confiança para um SMC de ativação pós-falha antes de promover a SMC principal



Contacte os Serviços Profissionais da Cisco para obter assistência no planeamento e implementação destas tarefas.

## Reiniciar um Nós de dados



Contacte os Serviços Profissionais da Cisco para obter assistência no planeamento e implementação destas tarefas.

Se tiver de reiniciar um Nós de dados, emita o comando para o parar e, em seguida, emita o comando para o reiniciar.

## Pare e, em seguida, reinicie o Nós de dados

### Antes de começar

- Inicie a sessão na consola de um Nós de dados como `root`.

### Procedimento

1. Introduza `su - dbadmin` e prima Enter para executar os seguintes comandos como utilizador `dbadmin`.

2. Copie o comando seguinte e cole-o num editor de texto simples:

```
/opt/vertica/bin/admintools -t stop_node -s [data-node-hostname]
```

3. Substitua `[data-node-hostname]` pelo nome de anfitrião do Nós de dados que pretende parar, antes de o reiniciar.

4. Copie o comando atualizado, cole-o na linha de comando e prima Enter para parar o Nós de dados.

5. Copie o comando seguinte e cole-o num editor de texto simples:

```
/opt/vertica/bin/admintools -t restart_node -s [data-node-hostname]
```

6. Substitua `[data-node-hostname]` pelo nome de anfitrião de Nós de dados que pretende reiniciar.
7. Copie o comando atualizado, cole-o na linha de comando e prima Enter para reiniciar o Nós de dados.

## Reinicie o Data Store



Contacte os Serviços Profissionais da Cisco para obter assistência no planeamento e implementação destas tarefas.

Para reiniciar o Data Store, emita o comando para o parar e, em seguida, emita o comando para o reiniciar.

## Pare e, em seguida, reinicie o Data Store

### Antes de começar

- Assegure que os seus Coletores de fluxo não são ligados ao Data Store e que passam dados.
- Assegure que o seu SMC não é ligado ao Data Store e que não está a consultar ou atualizar o Data Store.
- Inicie a sessão na consola de um Nós de dados como `root`.

### Procedimento

1. Introduza `su - dbadmin` e prima Enter para executar os seguintes comandos como utilizador `dbadmin`.
2. Tem as seguintes opções:
  - A partir da linha de comandos, introduza `/opt/vertica/bin/admintools -t stop_db -d sw` e prima Enter para parar o Data Store.
  - A partir da linha de comandos, introduza `/opt/vertica/bin/admintools -t stop_db -d sw -F` e prima Enter para parar o Data Store, anulando quaisquer Coletores de fluxo ou ligações de SMC.

3. A partir da linha de comandos, introduza `/opt/vertica/bin/admintools -t start_db -d sw` e prima Enter para reiniciar o Data Store.

## Criar uma cópia de segurança do Data Store



Contacte os Serviços Profissionais da Cisco para obter assistência no planeamento e implementação destas tarefas.

Para efetuar uma cópia de segurança do seu Data Store, tem de realizar o seguinte:

- Calcular o tamanho da cópia de segurança
- Preparar um anfitrião de cópia de segurança com o dobro da capacidade de armazenamento do tamanho da cópia de segurança



Utilize um anfitrião baseado em Linux separado dos seus dispositivos Stealthwatch.

- Instalar o Python 3.7 e rsync 3.0.5 no anfitrião de cópia de segurança
- Assegurar que todos os Nós de dados alcançam o anfitrião de cópia de segurança utilizando um acesso SSH sem palavra-passe
- Inicializar o diretório de cópia de segurança no anfitrião de cópia de segurança
- Efetuar a cópia de segurança do Data Store

## Calcular os requisitos de armazenamento do anfitrião de cópia de segurança

### Antes de começar

- Inicie a sessão numa consola de Nós de dados como `root`.

### Procedimento

1. Copie o comando seguinte, cole-o na linha de comando e prima Enter para ligar à base de dados utilizando `vsq` e executar a consulta. Introduza a sua palavra-passe, se lhe for pedido. Anote os resultados.

```
/opt/vertica/bin/vsqli -U dbadmin -c "SELECT SUM(used_bytes) FROM storage_containers;"
```

2. Multiplique a soma por 2 para calcular a quantidade de espaço de armazenamento requerido pelo seu anfitrião de cópia de segurança.

## Prepare um anfitrião de cópia de segurança:

## Antes de começar

- Com base nos requisitos de armazenamento que tiver calculado na tarefa anterior, identifique um anfitrião que execute Linux na sua rede para armazenar a cópia de segurança ou implemente um anfitrião que execute Linux com os requisitos de armazenamento necessários.



Utilize um anfitrião baseado em Linux separado dos seus dispositivos Stealthwatch.

- Inicie a sessão na consola do anfitrião de cópia de segurança como `root`.

## Procedimento

1. A partir da linha de comandos, introduza `python --version` e prima Enter para ver a versão de Python que tem instalada. Tem as seguintes opções:
  - Se estiver instalado o Python 3.7, continue para o passo 4.
  - Caso contrário, instale o Python 3.7. Continue para o passo 2.
2. Introduza `sudo apt-get update` e prima Enter para transferir versões atualizadas de pacotes, incluindo o Python. Introduza a sua palavra-passe, se lhe for pedido.
3. Introduza `sudo apt-get install python3.7` e prima Enter para instalar o Python 3.7.
4. A partir da linha de comandos, introduza `rsync -version` e prima Enter para ver que versão do rsync tem instalada. Tem as seguintes opções:

Se tiver instalado o rsync 3.0.5, continue para o passo 7.

Caso contrário, instale o rsync 3.0.5. Continue para o passo 5.
5. Introduza `sudo apt-get update` e prima Enter para transferir versões atualizadas de pacotes, incluindo o rsync. Introduza a sua palavra-passe, se lhe for pedido.
6. Introduza `sudo apt-get install rsync` e prima Enter para instalar o rsync.
7. A partir da linha de comandos, introduza `getent passwd | grep dbadmin` e prima Enter para determinar se existe uma conta de utilizador `dbadmin` neste anfitrião. Tem as seguintes opções:
  - Se existir uma conta de utilizador `dbadmin`, o anfitrião de cópia de segurança está pronto. Continue para [Ativar acesso SSH sem palavra-passe para dbadmin](#).

- Caso contrário, crie uma conta de utilizador `dbadmin` neste anfitrião. Continue para o passo 5.
8. A partir da linha de comandos, introduza `useradd dbadmin` e prima `Enter` para criar uma conta de utilizador `dbadmin`.
  9. Introduza `passwd dbadmin` e prima `Enter` para atribuir uma palavra-passe a `dbadmin`.
  10. Introduza uma **Nova palavra-passe** e prima `Enter` para definir a palavra-passe de `dbadmin`. Confirme a palavra-passe quando lhe for solicitada.

### O que fazer a seguir

- Ative o acesso SSH sem palavra-passe para a conta de utilizador `dbadmin`, conforme descrito na secção seguinte.

## Ativar acesso SSH sem palavra-passe para `dbadmin`:

### Antes de começar

- Abra a porta 22/TCP entre o anfitrião de cópia de segurança e cada Nós de dados para SSH, e a porta 50000/TCP entre o anfitrião de cópia de segurança e cada Nós de dados para `rsync`.
- Consulte a documentação do OpenSSH sobre `ssh-copy-id` para mais informações.
- Inicie a sessão no primeiro Nós de dados como `root`.

### Procedimento

1. Copie o comando seguinte e cole-o num editor de texto simples:

```
ssh-copy-id -i dbadmin@[hostname]
```

2. Substitua `[hostname]` pelo nome de anfitrião de cópia de segurança.
3. Copie o comando atualizado, cole-o na linha de comando e prima `Enter` para copiar a chave autorizada de SSH `dbadmin` para o anfitrião de cópia de segurança.
4. Copie o comando seguinte e cole-o num editor de texto simples:

```
ssh 'dbadmin@[hostname]'
```

5. Substitua `[hostname]` pelo nome de anfitrião de cópia de segurança.
6. Copie o comando atualizado, cole-o na linha de comandos e prima `Enter` para confirmar que pode iniciar a sessão na consola do anfitrião remoto através de SSH sem necessidade de palavra-passe deste Nós de dados.



# Inicialize o diretório de cópia de segurança no anfitrião de cópia de segurança:

## Antes de começar

- Inicie a sessão na consola do primeiro Nós de dados como root.

Anote o Nós de dados que utiliza para inicializar o diretório de cópia de segurança. Pode também realizar a cópia de segurança a partir deste Nós de dados, conforme descrito em [Cópia de segurança do Data Store](#).

## Procedimento

1. Introduza `su - dbadmin` e prima Enter para executar os seguintes comandos como utilizador `dbadmin`.
2. Copie o comando seguinte para um editor de texto: `ssh [backup-host-ip]`
3. Substitua `[backup-host-ip]` pelo endereço IP do seu anfitrião de cópia de segurança.
4. Copie o comando atualizado, cole-o na linha de comandos e prima Enter para confirmar que pode iniciar a sessão na interface do anfitrião de cópia de segurança como `dbadmin` sem lhe ser pedida uma palavra-passe. Se o anfitrião de cópia de segurança lhe pedir uma palavra-passe, verifique as suas definições.
5. Introduza `cd /home/dbadmin` e prima Enter para alterar os diretórios.
6. Introduza `mkdir backups` e prima Enter para criar o diretório `backups`.
7. Introduza `exit` e prima Enter para voltar à linha de comandos do Nós de dados.
8. Introduza `vi pw.ini` e prima Enter para criar o ficheiro de palavra-passe de cópia de segurança `pw.ini` e editá-lo.



Se atualizar a palavra-passe de `dbadmin` utilizando o script `setup-sw-datastore-secure-connectivity`, também tem de atualizar a palavra-passe armazenada no ficheiro de palavra-passe de cópia de segurança `pw.ini` ou não será possível efetuar a sua cópia de segurança. Consulte [Atualizar as palavras-passe de dbadmin e readonlyuser do Data Store após a inicialização](#) para mais informações.

9. Copie as linhas seguintes para um editor de texto simples:

```
[Passwords]
dbPassword = [dbadmin-password]
```

10. Atualize `[dbadmin-password]` para a palavra-passe de Data Store `dbadmin`.
11. Copie as linhas atualizadas e cole-as no ficheiro de palavra-passe de cópia de segurança `pw.ini`.
12. Prima Esc, introduza `:wq` e prima Enter para sair e guardar as suas alterações.
13. Introduza `chmod 640 pw.ini` e prima Enter para alterar as permissões de ficheiro `pw.ini` para permitir que o utilizador `dbadmin` leia e edite o ficheiro.
14. Introduza `vi config.ini` e prima Enter para criar o ficheiro de configuração de cópia de segurança `config.ini` e editá-lo.
15. Copie as linhas seguintes e cole-as num editor de texto simples:

```
[Mapping]
v_sw_node0001 = backup-host-ip:/home/dbadmin/backups
v_sw_node0002 = backup-host-ip:/home/dbadmin/backups
v_sw_node0003 = backup-host-ip:/home/dbadmin/backups
```

```
[Misc]
snapshotName = data_store_backup
passwordFile = /home/dbadmin/pw.ini
enableFreeSpaceCheck = True
retryCount = 2
retryDelay = 1
```

```
[Transmission]
encrypt = true
checksum = true
concurrency_backup = 2
concurrency_restore = 2
```

16. Substitua `backup-host-ip` pelo endereço IP do anfitrião de cópia de segurança.
17. Se os nomes de anfitrião em `[Mapping]` não corresponderem aos seus Nós de dados, atualize estes nomes de anfitrião.
18. Assegure que tem uma entrada para cada Nós de dados se tiver implementado mais de 3 no seu ambiente.
19. Copie as linhas atualizadas e cole-as no ficheiro `config.ini`.
20. Prima Esc, introduza `:wq` e prima Enter para sair e guardar as suas alterações.

21. Introduza `vbr -t init -c config.ini` e prima Enter para inicializar o diretório `/home/dbadmin/backups` no anfitrião de cópia de segurança para receber cópias de segurança do Data Store.

## Faça uma cópia de segurança da base de dados do Data Store

### Antes de começar

- Como `root`, inicie a sessão na consola do Nós de dados a partir do qual inicializou o diretório de anfitrião de cópia de segurança, conforme descrito em [Inicializar o diretório de cópia de segurança no anfitrião de cópia de segurança](#).

### Procedimento

1. Introduza `su - dbadmin` e prima Enter para executar os seguintes comandos como utilizador `dbadmin`.
2. Introduza `vbr -t backup -c config.ini --debug 3 --dry-run` e prima Enter para realizar um teste da cópia de segurança sem criar a cópia de segurança. Tem as seguintes opções:
  - Se o teste de cópia de segurança for efetuado com sucesso, efetue uma cópia de segurança do Data Store. Continue para o passo 2.
  - Se o teste de cópia de segurança falhar, consulte os ficheiros de registo de depuração no diretório `/tmp/vbr`, resolva a causa raiz e, em seguida, teste novamente a cópia de segurança. Contacte o suporte da Cisco para obter ajuda se não conseguir resolver o problema.
3. Introduza `vbr -t backup -c config.ini` e prima Enter para efetuar uma cópia de segurança do Data Store para o diretório `/home/dbadmin/backups` no anfitrião de cópia de segurança.

## Restaurar uma cópia de segurança do Data Store



Contacte os Serviços Profissionais da Cisco para obter assistência no planeamento e implementação destas tarefas.

Para restaurar o Data Store a partir de uma cópia de segurança, tem de assegurar o seguinte:

- O Data Store está inativo. Apenas pode parar o Data Store se os seus Coletores de fluxo e o SMC não estiverem ligados e a efetuar alterações.

- A cópia de segurança e o Data Store têm nomes de nó idênticos e o mesmo número de nós.

## Pare o Data Store:

### Antes de começar

- Assegure que os seus Coletores de fluxo não são ligados ao Data Store e que passam dados.
- Assegure que o seu SMC não é ligado ao Data Store e que não está a consultar ou atualizar o Data Store.
- Inicie a sessão na consola de um Nós de dados como `root`.

### Procedimento

1. Introduza `su - dbadmin` e prima Enter para executar os seguintes comandos como utilizador `dbadmin`.
2. Tem as seguintes opções:
  - A partir da linha de comandos, introduza `/opt/vertica/bin/admintools -t stop_db -d sw` e prima Enter para parar o Data Store.
  - A partir da linha de comandos, introduza `/opt/vertica/bin/admintools -t stop_db -d sw -F` e prima Enter para parar o Data Store, anulando quaisquer Coletores de fluxo ou ligações de SMC.

## Restaure o Data Store a partir de uma cópia de segurança:

### Antes de começar

- Se tiver atualizado a palavra-passe de `dbadmin` utilizando o script `setup-sw-datastore-secure-connectivity`, também tem de atualizar a palavra-passe armazenada no ficheiro de palavra-passe de cópia de segurança `pw.ini` ou não será possível efetuar o seu restauro. Consulte [Atualizar as palavras-passe de dbadmin e readonlyuser do Data Store após a inicialização](#) para mais informações.
- Identifique o Nós de dados em que armazenou o ficheiro de configuração de cópia de segurança `config.ini` e inicie a sessão na sua consola como `root`.

## Procedimento

1. Introduza `su - dbadmin` e prima Enter para executar os seguintes comandos como utilizador `dbadmin`.
2. A partir da linha de comandos, introduza `vbr --task restore --config-file config-file.ini` e prima Enter para restaurar o Data Store a partir do anfitrião de cópia de segurança.

## Inicie o Data Store:

### Antes de começar

- Inicie a sessão na consola de um Nós de dados como `root`.

### Procedimento

1. Introduza `su - dbadmin` e prima Enter para executar os seguintes comandos como utilizador `dbadmin`.
2. A partir da linha de comandos, introduza `/opt/vertica/bin/admintools -t start_db -d sw` e prima Enter para iniciar o Data Store.

### O que fazer a seguir

- Remova o instantâneo de catálogo, conforme descrito na secção seguinte.

## Remova o instantâneo de catálogo:

Após reiniciar o Data Store, remova o instantâneo com o nome `catalog`. Este instantâneo não é necessário após a conclusão do restauro e impede que o Vertica execute a gestão de retenção.

### Antes de começar

- Inicie a sessão na consola de um Nós de dados como `root`.

### Procedimento

1. Introduza `su - dbadmin` e prima Enter para executar os seguintes comandos como utilizador `dbadmin`.
2. Copie o comando seguinte e cole-o num editor de texto simples:

```
/opt/vertica/bin/vsql -U dbadmin -w [password] -c "select  
remove_database_snapshot('catalog');"
```

3. Substitua [password] pela sua palavra-passe de dbadmin.
4. Copie o comando atualizado, cole-o na linha de comando e prima Enter para remover o instantâneo de catalog.

### O que fazer a seguir

- Ligue novamente os seus Coletores de fluxo ao Data Store e assegure que estão a passar dados.
- Ligue novamente o seu SMC ao Data Store.

## Adicionar três Nós de dados ao Data Store



Contacte os Serviços Profissionais da Cisco para obter assistência no planeamento e implementação destas tarefas.

Pode expandir o seu Data Store em incrementos de três Nós de dados ou múltiplos de três Nós de dados. Se pretender expandir o número de Nós de dados no seu Data Store, realize as tarefas seguintes:

### Preparar o Data Store para adicionar Nós de dados e reequilibrar

Antes de adicionar um Nós de dados, realize o seguinte:

- Efetue uma cópia de segurança do Data Store. Consulte [Criar uma cópia de segurança do Data Store](#) para mais informações.
- Assegure que os seus Coletores de fluxo não são ligados ao Data Store e que passam dados.
- Assegure que o seu SMC não é ligado ao Data Store e que não está a consultar ou atualizar o Data Store.
- Elimine partições de dados antigas e não utilizadas. Contacte os Serviços Profissionais da Cisco para obter ajuda na identificação destas partições.
- Desative segmentos locais. A partir de vsql, emita `SELECT DISABLE_LOCAL_SEGMENTS ();`
- Atualize as suas definições de rede de recursos. A partir de vsql, emita `alter resource pool REFRESH MAXCONCURRENCY 2 PLANNEDCONCURRENCY 2 MEMORYSIZE '40%' MAXMEMORYSIZE '70%';`

### Adicionar Nós de dados ao Data Store

Em seguida, se ainda não o tiver feito, implemente os Nós de dados na sua rede em múltiplos de 3. Realize a configuração inicial em Configuração do sistema utilizando a Configuração inicial e a Ferramenta de configuração de dispositivo para completar a

configuração inicial. Consulte o [Anexo B. Instalação de hardware Stealthwatch](#) e [Anexo C. Configurar os seus dispositivos](#) para mais informações.

Após ter configurado os Nós de dados, incluindo a atribuição de um endereço IP de gestão `eth0` encaminhável e um endereço IP de canal de porta `eth2` ou `eth2/eth3` não encaminhável, realize o seguinte:

- Inicie a sessão num Nós de dados e configure o ficheiro de configuração `update_SDBN.cfg` para adicionar novos Nós de dados.
- Execute o script `update_SDBN.py` para adicionar os Nós de dados ao Data Store e, opcionalmente, adicioná-los também à base de dados do Data Store

## Adicionar Nós de dados ao Data Store:

### Antes de começar

- Inicie a sessão numa consola de Nós de dados como `root`.

### Procedimento

1. Introduza `su - dbadmin` e prima Enter para executar os seguintes comandos como utilizador `dbadmin`.
2. A partir da linha de comandos, introduza `cd /lancope/database` e prima Enter para alterar os diretórios.
3. Introduza `cp update_SDBN_example.cfg update_SDBN.cfg` e prima Enter para efetuar uma cópia do ficheiro de configuração exemplo de adicionar Nós de dados.
4. Introduza `vi update_SDBN.cfg` e prima Enter para modificar o ficheiro de configuração de adicionar Nós de dados num editor de texto.
5. Crie secções de `[nodeN]` numeradas consecutivamente de forma a corresponder ao número de novos Nós de dados que pretende adicionar ao Data Store. Por exemplo, se já tiver 3 Nós de dados implementados na sua rede e pretender adicionar 6 Nós de dados, o seu ficheiro teria o seguinte:

```
[node1]
private = 169.254.42.30
public = 10.0.16.114
[node2]
private = 169.254.42.31
public = 10.0.16.115
[node3]
private = 169.254.42.32
```

```
public = 10.0.16.116
[node4]
private = 169.254.42.33
public = 10.0.16.117
[node5]
private = 169.254.42.34
public = 10.0.16.118
[node6]
private = 169.254.42.35
public = 10.0.16.119
[common]
subnet = 10.0.16.0
firstNode = 4
```

6. Começando pela secção `[node1]`, introduza os endereços IP privados e públicos para cada novo Nós de dados. Lembre-se do seguinte:
  - Este script adiciona Nós de dados ao Data Store pela ordem em que estão listados, com uma numeração consecutiva segundo o seu Nós de dados de numeração mais alta que já faz parte do Data Store. Se tiver implementado os seus Nós de dados em racks diferentes, alterne a atribuição de nó entre os racks para maximizar a redundância de dados.
  - Os endereços IP privados devem ser não encaminháveis, numa LAN ou VLAN privada. Tem de atribuir endereços IP no bloco CIDR `169.254.42.0/24`.
  - Não sobreponha endereços IP entre Nós de dados.
  - Não adicione o seu Nós de dados sobresselente aqui mesmo que o tenha implementado no seu ambiente sem o configurar. Apenas adicione Nós de dados que pretende que façam parte do Data Store.
7. Na secção `[common]`, atualize `subnet` de forma a corresponder aos seus endereços IP públicos.
8. Na secção `[common]`, atualize o valor de `firstNode` para ser um valor superior ao número de Nós de dados que já fazem parte da sua implementação Data Store.
9. Prima Esc, introduza `:wq` e prima Enter para guardar as suas alterações e sair do editor de texto.
10. A partir da linha de comandos, tem as seguintes opções:

Introduza `python update_SDBN.py -i update_SDBN.cfg` e prima Enter para executar o script python adicionar Nós de dados. Este script utiliza o ficheiro de configuração `update_SDBN.cfg` para adicionar os novos Nós de dados ao



Data Store pela ordem que tiver especificado. Note que **não** são adicionados à base de dados neste caso.

Introduza `python update_SDBN.py -i update_SDBN.cfg -d` e prima Enter para executar o script python adicionar Nós de dados. Este script utiliza o ficheiro de configuração `update_SDBN.cfg` para adicionar os novos Nós de dados ao Data Store pela ordem que tiver especificado e adiciona também os Nós de dados como parte da base de dados.

Após o script terminar, reveja as mensagens de estado CLI para garantir que o script foi bem sucedido.

11. Introduza `cd /opt/vertica/config` para alterar os diretórios.
12. Introduza `vi apikeys.dat` para abrir o ficheiro de chaves API num editor de texto.
13. Prima Esc e, em seguida, introduza `q!` e prima Enter para sair do editor de texto sem guardar alterações.
14. Anote o endereço IP deste Data Node. Utiliza este endereço IP na [Manutenção do Data Store](#) para configurar o VMC no seu SMC.

Se não adicionar os novos Nós de dados à base de dados utilizando o script `update_SDBN.py`, pode, em vez disso, adicionar manualmente os Nós de dados. Inicie sessão num Nós de dados no seu Data Store e adicione os Nós de dados ao Data Store.

## Adicione novos Nós de dados ao Data Store:

### Antes de começar

- Inicie a sessão num Nós de dados como `root`.

### Procedimento

1. Introduza `su - dbadmin` e prima Enter para executar os seguintes comandos como utilizador `dbadmin`.
2. Copie o comando seguinte e cole-o num editor de texto simples:

```
admintools -t db_add_node -d sw -p '[dbadmin-password]' -s [data-node-eth0-addresses]
```

3. Substitua `[dbadmin-password]` pela sua palavra-passe de `dbadmin`.
4. Substitua `[data-node-eth0-addresses]` por uma lista separada por vírgulas dos novos endereços IP Nós de dados `eth0` encaminháveis.

5. Copie o comando atualizado, cole-o na linha de comandos e prima Enter para adicionar os novos Nós de dados à base de dados.

Após adicionar os Nós de dados à sua base de dados, reequilibre os dados nos Nós de dados para criar um armazenamento de dados equilibrado em cada Nós de dados.

## Reequilibre os dados no Data Store:

### Antes de começar

- Inicie a sessão num Nós de dados como `root`.

### Procedimento

1. Introduza `su - dbadmin` e prima Enter para executar os seguintes comandos como utilizador `dbadmin`.

2. Copie o comando seguinte e cole-o num editor de texto simples:

```
/opt/vertica/bin/vsql --timing -x -c "SELECT rebalance_
cluster()" -a -d sw -U dbadmin -w [dbadmin-password]
```

3. Substitua `[dbadmin-password]` pela palavra-passe de `dbadmin`.
4. Copie o comando atualizado, cole-o na linha de comandos e prima Enter para iniciar o reequilíbrio de dados. Note que pode ser necessário algum tempo, dependendo de múltiplos fatores, incluindo número de projeções, quantidade de dados e outros fatores.
5. Após a conclusão do reequilíbrio, atualize as suas definições de rede de recursos. A partir de `vsql`, emita `alter resource pool REFRESH MAXCONCURRENCY 2 PLANNEDCONCURRENCY 2 MEMORYSIZE '40%' MAXMEMORYSIZE '0%;`

## Remover um Nós de dados do Data Store



Contacte os Serviços Profissionais da Cisco para obter assistência no planeamento e implementação destas tarefas.

Se pretender remover um Nós de dados do Data Store, note o seguinte:

- O Data Store tem de estar a ser executado.
- Primeiro, execute uma cópia de segurança. Consulte [Criar uma cópia de segurança do Data Store](#) para mais informações.
- Tem de ter, no mínimo, 3 nós no Data Store devido às definições de tolerância a falhas. Se pretender substituir um nó, consulte [Substitua um Nós de dados por](#)

um **Nós de dados sobresselente com um endereço IP diferente** para mais informações.

## Remova um nó do Data Store:

### Antes de começar

- Inicie a sessão na Consola de Gestão Vertica como `dbadmin`.

### Procedimento

1. Selecione **Gerir**. Aparece a página Gerir.
2. Selecione o nó que pretende remover e, em seguida, clique em **Remover nó**.

## Substitua um Nós de dados por um Nós de dados sobresselente com um endereço IP diferente



Contacte os Serviços Profissionais da Cisco para obter assistência no planeamento e implementação destas tarefas.

## Preparar o Data Store para substituir um Nós de dados avariado

- Efetue uma cópia de segurança do Data Store. Consulte **Criar uma cópia de segurança do Data Store** para mais informações.
- Adicionar o Nós de dados sobresselente ao Data Store. Consulte **Adicionar Nós de dados ao Data Store:** para mais informações.

## Substitua o Nós de dados

Se o Vertica ainda estiver a ser executado no Nós de dados que pretende substituir, pare o Vertica. Em seguida, substitua o Nós de dados anterior pelo Nós de dados novo e distribua a configuração necessária pelo novo Data Node. Remova o Nós de dados anterior e reinicie o novo Nós de dados.

## Pare o Vertica num Nós de dados

Se o Nós de dados que pretende remover ainda estiver a executar o Vertica, pare o Vertica nesse Nós de dados. Se esse Nós de dados estiver inativo ou não estiver a executar o Vertica, avance para o passo seguinte.

### Antes de começar

- Inicie a sessão numa consola de Nós de dados como `root`.

## Procedimento

1. Introduza `su - dbadmin` e prima Enter para executar os seguintes comandos como utilizador `dbadmin`.
2. Copie o comando seguinte e cole-o num editor de texto simples:

```
/opt/vertica/bin/admintools -t stop_host -s [node-ip-addresses]
```

3. Substitua `[node-ip-addresses]` por uma lista separadas por vírgulas dos endereços IP Nós de dados `eth0` encaminháveis que pretende remover do Data Store.
4. Copie o comando atualizado, cole-o na linha de comandos e prima Enter para parar o Vertica nesse Nós de dados.

## Substitua um Nós de dados

### Antes de começar

- Inicie a sessão numa consola de Nós de dados como `root`.

## Procedimento

1. Introduza `su - dbadmin` e prima Enter para executar os seguintes comandos como utilizador `dbadmin`.
2. Copie o comando seguinte e cole-o num editor de texto simples:

```
/opt/vertica/bin/admintools -t db_replace_node -d sw -o [old-data-node-hostname] -n [new-data-node-hostname]
```

3. Substitua `[old-data-node-hostname]` pelo nome de anfitrião de Nós de dados que pretende remover do Data Store.
4. Substitua `[new-data-node-hostname]` pelo nome de anfitrião de Nós de dados que pretende adicionar como substituição ao Data Store.
5. Copie o comando atualizado, cole-o na linha de comandos e prima Enter para substituir o Nós de dados anterior pelo novo Nós de dados.
6. Copie `/opt/vertica/bin/admintools -t distribute_config_files`, cole-o na linha de comandos e prima Enter para distribuir os ficheiros de configuração pelo novo Nós de dados.
7. Copie o comando seguinte e cole-o num editor de texto simples:

```
/opt/vertica/sbin/update_vertica --remove-hosts [old-data-node-hostname]
```

8. Substitua `[old-data-node-hostname]` pelo nome de anfitrião de Nós de dados que pretende remover do Data Store.
9. Copie o comando atualizado, cole-o na linha de comandos e prima Enter para remover o Nós de dados anterior do Data Store.
10. Copie o comando seguinte e cole-o num editor de texto simples:

```
/opt/vertica/bin/admintools -t restart_node -s [new-data-node-hostname]
```

11. Substitua `[new-data-node-hostname]` pelo nome de anfitrião de Nós de dados que pretende adicionar como substituição ao Data Store.
12. Copie o comando atualizado, cole-o na linha de comandos e prima Enter para reiniciar o novo Nós de dados.

## Copie a Informação de confiança do Data Store para um SMC de ativação pós-falha

Se implementar um SMC de ativação pós-falha no seu ambiente e for gerido pelo seu SMC principal, quando executa o script `setup-sw-datastore-secure-connectivity`, certas informações de confiança, incluindo as palavras-passe de `dbadmin` e `readonlyuser` e os certificados de identidade para comunicações seguras com os Nós de dados não são copiados para o SMC de ativação pós-falha. Antes de promover o SMC de ativação pós-falha a SMC principal numa implementação Data Store, tem de copiar os ficheiros do seu SMC principal para o SMC de ativação pós-falha. Se não copiar estas informações de confiança, o seu SMC não pode ser ligado ao Data Store.

Adicionalmente, se já tiver promovido o seu SMC de ativação pós-falha a SMC principal, despromovido o seu SMC principal a SMC de ativação pós-falha e pretender adicionar novos dispositivos à sua implementação Stealthwatch, tem de copiar as informações de confiança para o novo SMC de ativação pós-falha antes de executar `setup-sw-datastore-secure-connectivity`. Se não copiar estas informações de confiança, o script pode falhar.

## Copie as informações de segurança entre SMCs:

### Antes de começar

- Identifique os endereços IP e as credenciais de raiz do SMC principal e SMC de ativação pós-falha.
- Se o seu SMC de ativação pós-falha tiver sido recentemente promovido a SMC principal, inicie a sessão na consola desse SMC como `root`.

## Procedimento

1. Copie o comando seguinte e cole-o num editor de texto simples:

```
scp root@[demoted-smc-ip-address]:/lancope/var/admin/cds/sw-datastore-*/lancope/var/admin/cds
```

2. Substitua `[demoted-smc-ip-address]` pelo endereço IP do seu SMC recém-despromovido (atual SMC de ativação pós-falha).
3. Copie o comando atualizado, cole-o na linha de comandos e prima Enter para copiar as informações de confiança do Data Store do seu SMC recém-despromovido (atual ativação pós-falha) para o seu SMC recém-promovido (atual principal). Introduza a sua palavra-passe `root` para o SMC recém-despromovido (atual ativação pós-falha) quando isso lhe for solicitado.

# Resolução de problemas na implementação do Data Store

## Resolução de problemas na implementação de hardware

Para problemas na implementação ou configuração do seu SMC ou Coletores de fluxo, consulte o [Manual de instalação do hardware do Stealthwatch x210](#) e o [Guia de configuração do sistema Stealthwatch](#) para mais informações.

## Resolução de problemas do Script setup-sw-datastore-secure-connectivity

Se tiver promovido um SMC de ativação pós-falha a SMC principal, consulte [Copiar informação de confiança do Data Store para um SMC de ativação pós-falha](#) para informação sobre a cópia de informação de confiança de Data Store para o seu SMS recém-promovido (atualmente principal).

O script de ligação segura do Data Store `setup-sw-datastore-secure-connectivity` registra mensagens em ficheiros de registo em `/lancope/var/logs/containers/setup-sw-datastore-secure-connectivity.log`. Consulte para informações adicionais.

## Mensagens gerais de erro setup-sw-datastore-secure-connectivity

A tabela seguinte apresenta mensagens de erro que podem ser exibidas se ocorrer um erro com o script `setup-sw-datastore-secure-connectivity`, assim como soluções possíveis para o problema.

Mensagem de Erro	Descrição	Soluções possíveis
Erro na autorização de início de sessão remoto para [ip-address]	O script <code>setup-sw-datastore-secure-connectivity</code> não pôde iniciar	<ul style="list-style-type: none"> <li>• Certifique-se de que forneceu a palavra-passe raiz correta para acesso.</li> <li>• Verifique se o dispositivo está a funcionar atualmente.</li> <li>• Verifique se a ligação entre o script</li> </ul>

	sessão remotamente num dispositivo para fornecer informação essencial.	e o dispositivo está atualmente ativa.
Erro ao gerar par de chaves.	Ocorreu um erro no script <code>setup-sw-datastore-secure-connectivity</code> ao gerar as chaves associadas aos certificados de identidade utilizados para ligações seguras de Data Store.	<ul style="list-style-type: none"> <li>• Contacte o Suporte da Cisco para mais informações.</li> </ul>
Falhou a autenticação com autoridade de token.	O script <code>setup-sw-datastore-secure-connectivity</code> não pôde estabelecer uma ligação com a Gestão Central.	<ul style="list-style-type: none"> <li>• Contacte o Suporte da Cisco para mais informações.</li> </ul>
Falhou a obtenção do inventário a partir do SMC.	O script	<ul style="list-style-type: none"> <li>• Consulte <code>/lancope/var/logs/contain</code></li> </ul>



	<p>setup-sw-datastore-secure-connectivity não pôde obter informação corretamente a partir da Gestão Central.</p>	<p>er/svc-central-management.log para tentar determinar se existe um problema com a Gestão Central.</p> <ul style="list-style-type: none"> <li>• Contacte o Suporte da Cisco para mais informações.</li> </ul>
<p>Nenhum Cliente DB encontrado.</p>	<p>O SMC e os Coletores de fluxo não foram corretamente configurados para utilização com um Data Store.</p>	<ul style="list-style-type: none"> <li>• Inicie sessão no CLI do dispositivo, execute a Configuração do Sistema e ative a utilização com um Data Store.</li> </ul>
<p>A palavra-passe não está disponível. Pode desejar eliminar /lancope/var/etc/keystore/store e executar novamente setup-sw-datastore-secure-connectivity.</p>	<p>Ocorreu um erro com o script setup-sw-datastore-secure-connectivity ao guardar ou distribuir as palavras-passe de dbadmin e readonlyuser.</p>	<ul style="list-style-type: none"> <li>• Elimine os conteúdos de /lancope/var/etc/keystore/store e, em seguida, execute novamente o script setup-sw-datastore-secure-connectivity.</li> </ul>

<p>Registe os nós de dados com a Gestão Central antes de tentar configurar a ligação segura.</p>	<p>Os seus Nós de dados não são geridos pela Gestão Central.</p>	<ul style="list-style-type: none"> <li>• Faça a gestão dos seus Nós de dados com a Gestão Central.</li> </ul>
<p>O inventário SMC está vazio. Adicione um dispositivo à Gestão Central.</p>	<p>A Gestão Central não está a gerir quaisquer Nós de dados ou Coletores de fluxo.</p>	<ul style="list-style-type: none"> <li>• Faça a gestão dos seus Coletores de fluxo e Nós de dados com a Gestão Central.</li> </ul>
<p>sw-datastore-dbadmin-password and/or sw-datastore-readonlyuser-password não presente na entrada</p>	<p>A palavra-passe de dbadmin ou readonlyuser não foi definida.</p>	<ul style="list-style-type: none"> <li>• No script, execute <b>1. Distribua a palavra-passe do SW DataStore novamente pelos dispositivos</b>, se ainda não tiver inicializado o Data Store e defina uma palavra-passe de dbadmin e uma palavra-passe de readonlyuser.</li> <li>• Se tiver inicializado o Data Store, no script, execute <b>3. Atualize a palavra-passe do SW DataStore nos dispositivos</b> para atualizar a palavra-passe de dbadmin e readonlyuser.</li> </ul>
<p>Palavras-passe do SW Datastore já inicializadas em [ip-address].</p>	<p>O Data Store já está inicializado, não pode utilizar <b>1. Distribua a palavra-passe do SW DataStore</b></p>	<ul style="list-style-type: none"> <li>• No script, execute <b>3. Atualize a palavra-passe do SW DataStore nos dispositivos</b> para atualizar a palavra-passe de dbadmin e readonlyuser.</li> </ul>

	<p><b>re pelos dispositivos</b></p> <p>em <code>setup-sw-datastore-secure-connectivity</code> para alterar as palavras-passe de <code>dbadmin</code> ou <code>readonlyuser</code>.</p>	
<p>As palavras-passe do SW Datastore não são armazenadas devido a: Valor vazio</p>	<p>A palavra-passe de <code>dbadmin</code> ou <code>readonlyuser</code> não foi definida.</p>	<ul style="list-style-type: none"> <li>No script, execute <b>1. Distribua a palavra-passe do SW DataStore novamente pelos dispositivos</b>, se ainda não tiver inicializado o Data Store e defina uma palavra-passe de <code>dbadmin</code> e uma palavra-passe de <code>readonlyuser</code>.</li> <li>Se tiver inicializado o Data Store, no script, execute <b>3. Atualize a palavra-passe do SW DataStore nos dispositivos</b> para atualizar a palavra-passe de <code>dbadmin</code> e <code>readonlyuser</code>.</li> </ul>
<p>Não existem nós de dados geridos atualmente.</p>	<p>Os seus Nós de dados não são geridos pela Gestão Central.</p>	<ul style="list-style-type: none"> <li>Faça a gestão dos seus Nós de dados com a Gestão Central.</li> </ul>
<p>Não existem SMC/FCs geridos atualmente.</p>	<p>Os seus Coletores de fluxo (e</p>	<ul style="list-style-type: none"> <li>Faça a gestão dos seus Coletores de fluxo e (SMC de ativação pós-falha) com a Gestão Central.</li> </ul>

	qualquer SMC de ativação pós-falha) não são geridos pela Gestão Central.	
Código de erro desconhecido: [error-code] em [ip-address]	Ocorreu um erro no script ao tentar distribuir as palavras-passe de dbadmin e readonly user.	<ul style="list-style-type: none"> <li>• Contacte o Suporte da Cisco para mais informações.</li> </ul>

## Resolução de problemas do Script `install_SDBN_initial.py`

O script de inicialização `install_SDBN_initial.py` Data Store regista mensagens em ficheiros de registo em `/lancope/var/database/logs/db_initial_install_[datestamp].log`. Consulte para informações adicionais.

## Pré-requisitos não totalmente satisfeitos durante a configuração (SO) local para `verify-[data-node-ip-address].xml`

Quando inicializar o Data Store na [Inicialização e configuração do Data Store](#) executando o script `python install_SDBN_initial.py`, pode verificar que a consola indica `Prerequisites not fully met during local (OS) configuration for verify-[data-node-ip-address].xml`, seguido de uma série de mensagens de registo. Estas mensagens de registo são antecipadas e não indicam uma falha na inicialização do Data Store. Não tem de realizar qualquer ação em relação a estas mensagens de registo.

A tabela seguinte descreve cada mensagem.

Nível de registo e Código de erro	Descrição	Explicação
FAIL (s0180)	Insufficient swap size. Need 2.00 GB, have 1.50 GB	O espaço atribuído para a partição de troca não cumpre as recomendações. <b>Não</b> modifique a atribuição de espaço de troca. A Cisco configurou o seu Data Store com a atribuição de espaço de troca correta.
FAIL (s0311)	root account is not in /etc/sudoers	O instalador não localizou a conta root na lista de permissões de superutilizador /etc/sudoers e recomenda que atualize o Vertica para resolver o problema. <b>Não</b> atualize o Vertica. Esta configuração é intencional para fins de segurança.
HINT (S0040)	Could not find the following tools normally provided by the pstack or gstack package: pstack/gstack	O instalador não consegue encontrar os pacotes <code>pstack</code> ou <code>gstack</code> para registar rastreios de pilha. Estes não são necessários para o seu Data Store.
HINT (S0041)	Could not find the following tools normally provided by the mcelog package: mcelog	O instalador não consegue encontrar o pacote <code>mcelog</code> para registar verificações de máquina. Isto não é necessário para o seu Data Store.
HINT (S0305)	TZ is unset for dbadmin. Consider updating .profile or .bashrc	O instalador não encontrou uma variável de ambiente <code>TZ</code> para a conta de utilizador <code>dbadmin</code> utilizada para fusos horários. Isto não é necessário para o seu Data Store quando configura servidores NTP para a sua implementação de Stealthwatch.

WARN (N0010)	Linux iptables (firewall) has some non-trivial rules in tables: filter	As iptables do Nós de dados contêm regras pré-existent. O sistema regista um aviso se as iptables contiverem regras, mas não verifica se existem colisões com as portas de comunicação necessárias. Isto é esperado e não deve provocar problemas com a sua implementação de Data Node.
-----------------	--	---

## Parâmetro SSLCA config não definido; os certificados de cliente não serão pedidos ou verificados

Quando inicializar o Data Store na [Inicialização e configuração do Data Store](#) executando o script `python install_SDBN_initial.py`, pode verificar que a consola indica `Enable SSL/TLS for remote connections`, seguido de `INFO 6403: SSLCA config parameter is not set; client certificates will not be requested or verified` uma vez por cada Nós de dados que está a inicializar. Esta mensagem de registo é antecipada e não indica uma falha no estabelecimento de ligações seguras com o Data Store. Não tem de realizar qualquer ação em relação a estas mensagens de registo.

O Data Store é configurado no Modo de Servidor TLS, o que requer que, quando os dispositivos estabelecem uma ligação segura ao Data Store, verifiquem também o certificado do servidor da base de dados. Contraste isto com a configuração do Modo Mútuo TLS, que requer que, quando os dispositivos estabelecem uma ligação segura com o Data Store, os dispositivos verifiquem o certificado do servidor da base de dados e que a base de dados verifique os certificados de cliente dos dispositivos. O Modo Mútuo TLS requer a configuração do parâmetro `SSLCA` com o ficheiro `root.crt` que contém a Autoridade de Certificação (CA) ou cadeia de confiança CA utilizada para assinar os certificados de cliente. Como o Modo Mútuo não está ativado, `SSLCA` não é configurado e o Data Store não verifica os certificados de cliente quando estabelece uma ligação segura. No entanto, a ligação entre os dispositivos e o Data Store no Modo de Servidor TLS continua a ser uma ligação segura através de TLS.

## Mensagens gerais de erro `install_SDBN_initial.py`

A tabela seguinte apresenta mensagens de erro que podem ser exibidas se ocorrer um erro com o script `install_SDBN_initial.py`, assim como soluções possíveis para o problema.

Mensagem de Erro	Descrição	Soluções possíveis
<p>Ficheiro Config não encontrado ou nenhuma secção válida</p>	<p>O script <code>install_SDBN_initial.py</code> não consegue localizar o ficheiro de configuração <code>install_SDBN.cfg</code> ou os dados no ficheiro de configuração não têm um formato que seja esperado.</p>	<ul style="list-style-type: none"> <li>• Assegure que tem uma cópia de <code>install_SDBN_example.cfg</code> guardada em <code>/lancope/database/install_SDBN.cfg</code> neste Nós de dados.</li> <li>• Assegure que a formatação de <code>install_SDBN.cfg</code> corresponde à formatação de <code>install_SDBN_example.cfg</code>, que atribui um nome a cada secção de nó no formato <code>node#</code>, que definiu um endereço IP privado e público para cada secção de configuração do Nós de dados e que tem uma subrede definida na secção comum.</li> </ul>
<p>Não foi possível encontrar o ficheiro <code>jar</code> esperado para obter palavras-passe de utilizador DB. Certifique-se de que está a executar uma imagem que contém este suporte</p>	<p>O script <code>install_SDBN_initial.py</code> não consegue localizar o ficheiro <code>sw-datastore-admin.jar</code> que contém as palavras-passe de <code>dbadmin</code> e <code>readonlyuser</code>.</p>	<ul style="list-style-type: none"> <li>• Assegure que o seu dispositivo tem a versão 7.3+.</li> <li>• Execute o script <code>setup-sw-datastore-secure-connectivity</code> em <code>/lancope/admin/cds</code> e selecione a opção <b>1. Distribua a palavra-passe do SW DataStore pelos dispositivos</b> para distribuir as palavras-passe de <code>dbadmin</code> e <code>readonlyuser</code>. Após concluir este passo, se ainda não o tiver feito, execute também a opção <b>2. Distribua os Certificados para Ligação DB Segura</b>.</li> <li>• Contacte o Suporte da Cisco se o erro persistir.</li> </ul>

<p>cada nó tem de ter uma entrada de endereço público e privado</p>	<p>O ficheiro de configuração <code>install_SDBN.cfg</code> tem uma ou mais entradas de nó que não têm um endereço IP privado e público definido.</p>	<ul style="list-style-type: none"> <li>• Assegure que definiu um endereço IP privado e público para cada secção de configuração do Nós de dados em <code>/lancope/database/install_SDBN.cfg</code>.</li> </ul>
<p>O ficheiro de armazenamento secreto não existe OU a palavra-passe não existe no ficheiro. Inicie a sessão no SMC e execute o script apropriado para definir e distribuir as palavras-passe DB.</p>	<p>Ocorreu um erro com o script <code>install_SDBN_initial.py</code> ao tentar obter as palavras-passe de <code>dbadmin</code> e <code>readonlyuser</code>.</p>	<ul style="list-style-type: none"> <li>• A partir do SMC CLI, execute o script <code>setup-sw-datastore-secure-connectivity</code> em <code>/lancope/admin/cds</code> e selecione a opção <b>1. Distribua a palavra-passe do SW DataStore pelos dispositivos</b> para distribuir as palavras-passe de <code>dbadmin</code> e <code>readonlyuser</code>. Após concluir este passo, se ainda não o tiver feito, execute também a opção <b>2. Distribua os Certificados para Ligação DB Segura</b>.</li> </ul>
<p>Falhou a obtenção das palavras-passe da base de dados</p>	<p>Ocorreu um erro com o script <code>install_SDBN_initial.py</code> ao tentar obter as palavras-passe de <code>dbadmin</code> e <code>readonlyuser</code>.</p>	<ul style="list-style-type: none"> <li>• A partir do SMC CLI, execute o script <code>setup-sw-datastore-secure-connectivity</code> em <code>/lancope/admin/cds</code> e selecione a opção <b>1. Distribua a palavra-passe do SW DataStore pelos dispositivos</b> para distribuir as palavras-passe de <code>dbadmin</code> e <code>readonlyuser</code>. Após concluir este passo, se ainda não o tiver feito, execute também a opção <b>2. Distribua os Certificados para Ligação DB Segura</b>.</li> </ul>



Exceção E/S ao tentar ler o ficheiro	Ocorreu um erro com o script <code>install_SDBN_initial.py</code> ao tentar obter as palavras-passe de <code>dbadmin</code> e <code>readonlyuser</code> .	<ul style="list-style-type: none"> <li>• Contacte o Suporte da Cisco e indique a mensagem de erro.</li> </ul>
Uma das duas palavras-passe não existe no ficheiro. Inicie a sessão no SMC e execute o script apropriado para definir e distribuir as palavras-passe DB.	Ocorreu um erro com o script <code>install_SDBN_initial.py</code> ao tentar obter as palavras-passe de <code>dbadmin</code> e <code>readonlyuser</code> .	<ul style="list-style-type: none"> <li>• A partir do SMC CLI, execute o script <code>setup-sw-datastore-secure-connectivity</code> em <code>/lancope/admin/cds</code> e selecione a opção <b>1. Distribua a palavra-passe do SW DataStore pelos dispositivos</b> para distribuir as palavras-passe de <code>dbadmin</code> e <code>readonlyuser</code>. Após concluir este passo, se ainda não o tiver feito, execute também a opção <b>2. Distribua os Certificados para Ligação DB Segura</b>.</li> </ul>
privateAddrs tem de ser especificado	O ficheiro de configuração <code>install_SDBN.cfg</code> tem uma ou mais entradas de nó que não têm um endereço IP privado definido.	<ul style="list-style-type: none"> <li>• Assegure que definiu um endereço IP privado para cada secção de configuração do Nós de dados em <code>/lancope/database/install_SDBN.cfg</code>. Note que o Nós de dados utiliza este endereço IP não encaminhável no <code>eth2</code> para comunicar com outros Nós de dados como parte do Data Store.</li> </ul>
publicAddrs tem de ser especificado	O ficheiro de configuração <code>install_SDBN.cfg</code> tem uma ou mais	<ul style="list-style-type: none"> <li>• Assegure que definiu um endereço IP público para cada secção de configuração do Nós de dados em <code>/lancope/database/install_SDBN.cfg</code>. Note que o Nós de dados</li> </ul>

	entradas de nó que não têm um endereço IP público definido.	utiliza este endereço IP encaminhável no <code>eth0</code> para comunicar com outros dispositivos Stealthwatch como parte da sua implementação de Stealthwatch.
publicSubnet tem de ser especificado	O ficheiro de configuração <code>install_SDBN.cfg</code> tem uma ou mais entradas de nó que não têm uma subrede definida.	<ul style="list-style-type: none"> <li>Assegure que tem uma subrede definida na secção de configuração comum em <code>/lancope/database/install_SDBN.cfg</code>. Note que este subconjunto está associado aos endereços IP encaminháveis no <code>eth0</code> que os Nós de dados utilizam para comunicar com outros dispositivos Stealthwatch como parte da sua implementação Stealthwatch.</li> </ul>
Exceção inesperada durante a leitura dos segredos	Ocorreu um erro com o script <code>install_SDBN_initial.py</code> ao tentar obter as palavras-passe de <code>dbadmin</code> e <code>readonlyuser</code> .	<ul style="list-style-type: none"> <li>Execute o script <code>setup-sw-datastore-secure-connectivity</code> em <code>/lancope/admin/cds</code> e selecione a opção <b>1. Distribua a palavra-passe do SW DataStore pelos dispositivos</b> para distribuir as palavras-passe de <code>dbadmin</code> e <code>readonlyuser</code>. Após concluir este passo, se ainda não o tiver feito, execute também a opção <b>2. Distribua os Certificados para Ligação DB Segura</b>.</li> <li>Contacte o Suporte da Cisco se o erro persistir.</li> </ul>
Valor devolvido inesperado	O script <code>install_SDBN_initial.py</code> recebeu um valor e	<ul style="list-style-type: none"> <li>Contacte o Suporte da Cisco e indique a mensagem de erro.</li> </ul>

	parou porque não podia continuar.	
--	-----------------------------------	--

## Atualize as palavras-passe de dbadmin e readonlyuser do Data Store após a inicialização:

Se já tiver inicializado o Data Store, conforme descrito na [Inicialização e configuração do Data Store](#) e desejar alterar as palavras-passe de dbadmin e readonlyuser, execute o script bash de conectividade segura `setup-sw-datastore-secure-connectivity`. Após indicar a palavra-passe de dbadmin atual, pode atribuir novas palavras-passe para dbadmin e readonlyuser. O script distribui as credenciais atualizadas pelos seus dispositivos através de SSH e atualiza as credenciais de conta de utilizador dbadmin e readonlyuser.



Se tiver perdido a palavra-passe dbadmin, contacte o Suporte da Cisco para obter ajuda na sua recuperação.

Cada palavra-passe tem de cumprir os seguintes requisitos:

- no mínimo, 1 número
- no mínimo, 1 carácter de minúsculas
- no mínimo, 1 carácter de maiúsculas
- no mínimo, 1 carácter especial da lista seguinte: `<> . , ? / ' " | : ; ` ~ ! @ # $ % ^ & * ( ) - _ + = { } [ ]`
- no mínimo, 8 caracteres, sem comprimento máximo
- apenas caracteres com codificação ASCII

Note que utilizará esta opção se já tiver inicializado o Data Store. Se estiver a realizar uma implementação e configuração inicial do Data Store, consulte [Distribuir palavras-passe do Data Store pelo seu SMC, Nós de dados e Coletores de fluxo](#) para atribuir palavras-passe para dbadmin e readonlyuser e configurar as definições de ligação segura com a base de dados do Data Store.

Se tiver efetuado uma cópia de segurança da sua base de dados do Data Store e tiver alterado a palavra-passe de dbadmin, atualize o ficheiro de palavra-passe de cópia de segurança `pw.ini` com a nova palavra-passe de dbadmin. Consulte [Criar uma cópia de segurança do Data Store](#) para obter mais informações.

### Antes de começar

- Efetue uma compilação de uma lista de palavras-passe root para o seu SMC, Nós de dados, Coletores de fluxo e um SMC secundário se tiver implementado um.
- Ative o acesso SSH e acesso root SSH no seu SMC, Nós de dados e Coletores de fluxo.



Quando o SSH está ativado, o risco de comprometer o sistema aumenta. É importante ativar o SSH apenas quando necessita do mesmo. Quando parar de utilizar o SSH, desative-o.

- Inicie a sessão no seu SMC CLI como utilizador root.

## Procedimento

1. A partir da linha de comandos, introduza `cd /lancope/admin/cds` e prima Enter para alterar os diretórios.
2. Introduza `./setup-sw-datastore-secure-connectivity` e prima Enter para executar o script bash de conectividade segura do Data Store.
3. A partir do menu principal do script, seleccione **3. Atualize a palavra-passe do SW DataStore nos dispositivos**.
4. Introduza a palavra-passe atual de **dbadmin** e seleccione **OK**.
5. Na linha de comandos, quando lhe for solicitada a palavra-passe raiz para cada dispositivo, introduza a palavra-passe e prima Enter.



Uma vez que introduz múltiplas palavras-passe, certifique-se de que introduz a palavra-passe correta para o respetivo dispositivo.

Após introduzir todas as palavras-passe root dos dispositivos, o script pede-lhe as palavras-passe de `dbadmin` e `readonlyuser`.

6. Introduza a nova palavra-passe de **dbadmin**.
7. Introduza a mesma palavra-passe de `dbadmin` no campo **dbadmin (confirmação)**.
8. Introduza a nova palavra-passe de **readonlyuser**.
9. Introduza a mesma palavra-passe de `readonlyuser` no campo **readonlyuser (confirmação)**.

**i** Não introduza a mesma palavra-passe para `dbadmin` e `readonlyuser`. A atribuição da mesma palavra-passe provoca uma falha do script e a não atribuição de palavra-passe a qualquer uma das contas de utilizador.

10. Selecione **OK**.

O script distribui estas palavras-passe de forma segura pelos seus dispositivos. Quando termina, apresenta uma lista dos dispositivos atualizados.

11. Selecione **OK** para regressar ao menu principal do script.

### O que fazer a seguir

- Inicie a sessão no VMC como `dbadmin`. É-lhe solicitada a atualização da sua palavra-passe.

**i** Se não atualizar a palavra-passe de forma a corresponder à nova palavra-passe de `dbadmin`, o VMC não envia notificações de alerta de estado de funcionamento, nem monitoriza devidamente o seu Data Store.

## Resolução de problemas do Script `update_SDBN.py`

O script `update_SDBN_initial.py` Nós de dados regista mensagens em ficheiros de registo em `/lancope/var/database/logs/db_update_[datestamp].log`. Consulte para informações adicionais.

## Mensagens gerais de erro `update_SDBN_initial.py`

A tabela seguinte apresenta mensagens de erro que podem ser exibidas se ocorrer um erro com o script `update_SDBN_initial.py`, assim como soluções possíveis para o problema.

Mensagem de Erro	Descrição	Soluções possíveis
Ficheiro Config não encontrado ou nenhuma secção válida	O script <code>update_SDBN.py</code> não consegue localizar o ficheiro de configuração <code>update_</code>	<ul style="list-style-type: none"> <li>• Assegure que tem uma cópia de <code>update_SDBN.cfg</code> guardada em <code>/lancope/database/update_SDBN.cfg</code> neste Nós de dados.</li> <li>• Assegure que a formatação de <code>update_SDBN.cfg</code> corresponde à formatação de</li> </ul>

	SDBN.cfg ou os dados no ficheiro de configuração não têm um formato que seja esperado.	update_SDBN_example.cfg, que atribui um nome a cada secção de nó no formato node#, que definiu um endereço IP privado e público para cada secção de configuração do Nós de dados, que tem uma subrede definida na secção comum e que definiu o primeiro nó como mais um do que o número total de nós que já existem no seu Data Store.
cada nó tem de ter uma entrada de endereço público e privado	O ficheiro de configuração update_SDBN.cfg tem uma ou mais entradas de nó que não têm um endereço IP privado e público definido.	<ul style="list-style-type: none"> <li>• Assegure que definiu um endereço IP privado e público para cada secção de configuração do Nós de dados em /lancope/database/update_SDBN.cfg.</li> </ul>
Falhou a obtenção da palavra-passe de dbadmin da base de dados	O script update_SDBN.py não consegue localizar a palavra-passe de dbadmin.	<ul style="list-style-type: none"> <li>• Assegure que o seu dispositivo tem a versão 7.3+.</li> <li>• Execute o script setup-sw-datastore-secure-connectivity em /lancope/admin/cds e selecione a opção <b>3. Atualize a palavra-passe do SW DataStore nos dispositivos</b> para definir as palavras-passe de dbadmin e readonlyuser.</li> <li>• Contacte o Suporte da Cisco se o erro persistir.</li> </ul>
firstNode tem de ser especificado	O ficheiro de configuração update_SDBN.cfg não tem um valor	<ul style="list-style-type: none"> <li>• Assegure que definiu um valor firstNode na secção de configuração comum em /lancope/database/update_SDBN.cfg.</li> </ul>

	<code>firstNode</code> definido.	
<code>privateAddr</code> tem de ser especificado	O ficheiro de configuração <code>update_SDBN.cfg</code> tem uma ou mais entradas de nó que não têm um endereço IP privado definido.	<ul style="list-style-type: none"> <li>Assegure que definiu um endereço IP privado para cada secção de configuração do Nós de dados em <code>/lancope/database/update_SDBN.cfg</code>. Note que o Nós de dados utiliza este endereço IP não encaminhável no <code>eth2</code> para comunicar com outros Nós de dados como parte da base de dados do Data Store.</li> </ul>
<code>publicAddr</code> tem de ser especificado	O ficheiro de configuração <code>update_SDBN.cfg</code> tem uma ou mais entradas de nó que não têm um endereço IP público definido.	<ul style="list-style-type: none"> <li>Assegure que definiu um endereço IP para cada secção de configuração do Nós de dados em <code>/lancope/database/update_SDBN.cfg</code>. Note que o Nós de dados utiliza este endereço IP encaminhável no <code>eth0</code> para comunicar com outros dispositivos Stealthwatch como parte da sua implementação de Stealthwatch.</li> </ul>
<code>publicSubnet</code> tem de ser especificado	O ficheiro de configuração <code>update_SDBN.cfg</code> tem uma ou mais entradas de nó que não tem uma subrede definida.	<ul style="list-style-type: none"> <li>Assegure que tem uma subrede definida na secção de configuração comum em <code>/lancope/database/update_SDBN.cfg</code>. Note que este subconjunto está associado aos endereços IP encaminháveis no <code>eth0</code> que os Nós de dados utilizam para comunicar com outros dispositivos Stealthwatch como parte da sua implementação Stealthwatch.</li> </ul>

## Resolução de problemas com a Consola de Gestão Vertical

Se a sua instância do VMC não se atualizar automaticamente no seu web browser, pode ter de atualizá-la manualmente para ver as alterações no seu Data Store ou alterações de configuração.

---

## Resolução de problemas do Data Store

Note que o Data Store reserva até 40% do espaço de armazenamento disponível para manutenção do Data Store. No mínimo, está disponível 60% do espaço total para armazenamento de fluxo.

### A Plataforma de Análise Vertical não reinicia automaticamente após ocorrer uma falha de energia num Nó de dados e este reiniciar

Se ocorrer uma falha de energia inesperada num Nós de dados e o utilizador reiniciar o dispositivo, a instância da Plataforma de Análise Vertical (Vertica) nesse Nós de dados pode não reiniciar automaticamente devido a possíveis dados corrompidos. Se ainda existirem Nós de dados a funcionar que permitam que o Data Store continue a funcionar, o Data Store continua a ingerir dados dos Coletores de fluxo. No entanto, tem de reiniciar o Nós de dados logo que possível, para permitir que se junte novamente ao Data Store, obtenha dados perdidos de Nós de dados adjacentes e acompanhe o resto dos Nós de dados.

Nesta situação, inicie a sessão no Nós de dados e force um reinício manual do Vertica, o que elimina os dados corrompidos e permite um reinício correto do Vertica.

Adicionalmente, pode ter de atualizar a política de restabelecimento de energia do Nós de dados antes de reiniciar. Se a política de restabelecimento de energia estiver definida para Energia desligada, tem de reiniciar manualmente o Nós de dados após a falha de energia. Consulte o [Guia de configuração da GUI UCS C-Series](#) para mais informações sobre a configuração da política de restabelecimento de energia no CIMC.

#### Antes de começar

- Inicie a sessão no CLI do Nós de dados como root.

#### Procedimento

1. Copie o comando seguinte e cole-o num editor de texto:

```
tail /lancope/var/database/dbs/sw/v_sw_[node_name]_
catalog/ErrorReport.txt
```

2. Substitua `[node_name]` pelo nome do seu Nós de dados (por exemplo, `node0001`).
3. Copie o comando atualizado e cole-o no CLI e, em seguida, prima Enter para rever as entradas mais recentes no ficheiro de erro `ErrorReport.txt`. Se a



mensagem de erro indicar possíveis problemas de consistência e corrupção de dados, avance para o passo seguinte para forçar um reinício do Vertica.

4. Copie o comando seguinte e cole-o num editor de texto:

```
admintools -t restart_node --hosts=[data-node-ip-address]  
--database='sw-datastore' --password="[dbadmin-password]"  
--force
```

5. Substitua `[data-node-ip-address]` pelo endereço IP do seu Nós de dados afetado .
6. Substitua `[dbadmin-password]` pela sua palavra-passe de Data Store `dbadmin`.
7. Copie o comando atualizado e cole-o no CLI e, em seguida, prima Enter para forçar um reinício do Vertica no seu Nós de dados afetado. O Vertica elimina quaisquer dados corrompidos e recupera esses dados de Nós de dados adjacentes.
8. Se o sistema lhe perguntar `Do you want to continue waiting?` `(yes/no) [yes]`, introduza `yes` (sim) e prima Enter para continuar a aguardar. Como o Vertica restaura a informação do Nós de dados afetado de Nós de dados adjacentes, se estes Nós de dados tiverem ingerido uma grande quantidade de tráfego de fluxo, enquanto o Nós de dados esteve inativo, pode ser necessário algum tempo até o Nós de dados recuperar.

## O que fazer a seguir

- Reveja as recomendações da Cisco sobre o fornecimento de alimentação aos seus Nós de dados em [Requisitos e considerações sobre a implementação do Data Store](#).

# Anexo A. Preparação da instalação


## Avisos relativos à instalação

Leia o documento [Informações de segurança e conformidade regulamentar](#) antes de instalar os dispositivos Data Store Stealthwatch.

Tome nota dos seguintes avisos:


### Declaração 1071—Definição de aviso

#### INSTRUÇÕES DE SEGURANÇA IMPORTANTES

 Este símbolo de aviso significa perigo. Está numa situação que poderá causar lesão corporal. Antes de trabalhar em qualquer equipamento, tenha em atenção os perigos inerentes aos circuitos elétricos e familiarize-se com as práticas padrão para prevenção de acidentes. Utilize o número de declaração fornecido no final de cada aviso para localizar a respetiva tradução, nos avisos de segurança traduzidos que acompanham este dispositivo.

#### GUARDE ESTAS INSTRUÇÕES


### Declaração 1005—Disjuntor

 Este produto confia na instalação elétrica do edifício no que respeita à proteção contra curto-circuito (sobretensão). Certifique-se de que a tensão nominal do dispositivo de proteção não é superior a: EUA: 120 V, 15 A (UE: 250 V, 16 A)

### Declaração 1004—Instruções de instalação

 Leia as instruções de instalação antes da utilização, instalação ou ligação do sistema à fonte de energia.

### Declaração 12—Aviso de desconexão da fonte de alimentação

 Antes de realizar trabalhos num chassi ou próximo de fontes de alimentação, desligue o cabo de alimentação nas unidades AC; desligue a alimentação no disjuntor nas unidades DC.

#### Declaração 43–Aviso de remoção de joias



Antes de trabalhar em equipamento ligado à eletricidade, retire todas as joias que estiver a usar (incluindo anéis, colares e relógios). Os objetos metálicos aquecem quando ligados à eletricidade e à terra e podem provocar queimaduras graves ou soldar o metal aos terminais.

#### Declaração 94–Aviso de pulseira antiestática



Durante este procedimento, utilize pulseiras de ligação à terra para evitar danos ESD na placa. Não toque diretamente no barramento com a mão ou qualquer ferramenta metálica, pois pode apanhar um choque.

#### Declaração 1045–Proteção contra curto-circuito



Este produto necessita de proteção contra curto-circuito (sobretensão), a ser fornecida como parte da instalação do edifício. Instale apenas de acordo com os regulamentos de ligação nacionais e locais.

#### Declaração 1021–Circuito SELV



Para evitar choques elétricos, não ligue circuitos de tensão de segurança extra baixa (SELV) a circuitos de tensão da rede telefónica (TNV). As portas LAN contêm circuitos SELV e as portas WAN contêm circuitos TNV. Algumas portas LAN e WAN utilizam conectores RJ-45. Tenha cuidado ao ligar cabos.

#### Declaração 1024–Condutor de terra



Este equipamento tem de ser ligado à terra. Nunca elimine o condutor de terra nem opere o equipamento sem o condutor de terra devidamente instalado. Contacte a autoridade de inspeção elétrica adequada ou um electricista se tiver dúvidas sobre a existência de uma ligação à terra correta.

#### Declaração 1040–Eliminação do produto



A eliminação final deste produto deve ser realizada em conformidade com todas as leis e regulamentos nacionais.

Declaração 1074—Em conformidade com os códigos elétricos locais e nacionais



A instalação do equipamento deve respeitar os códigos elétricos locais e nacionais.

Declaração 19—Aviso de energia TN



O dispositivo destina-se a funcionar com sistemas de alimentação TN.

## Orientações de instalação

Tome nota dos seguintes avisos:

Declaração 1047—Proteção contra Sobreaquecimento



Para evitar o sobreaquecimento do sistema não o opere em áreas cuja temperatura ambiente seja superior à máxima recomendada de: 5 a 35 °C.

Declaração 1019—Dispositivo de desconexão principal



A combinação ficha-tomada tem de estar sempre acessível, pois funciona como dispositivo de desconexão principal.

Declaração 1005—Disjuntor



Este produto confia na instalação elétrica do edifício no que respeita à proteção contra curto-circuito (sobretensão). Certifique-se de que a tensão nominal do dispositivo de proteção não é superior a: EUA: 120 V, 15 A (UE: 250 V, 16 A)

Declaração 1074—Em conformidade com os códigos elétricos locais e nacionais



A instalação do equipamento deve respeitar os códigos elétricos locais e nacionais.

Declaração 371—Cabo elétrico e adaptador AC



Utilize os cabos de ligação/cabos elétricos/adaptadores AC/baterias fornecidos ou designados para instalar o produto. A utilização de quaisquer outros cabos/adaptadores pode provocar avarias ou incêndio. A Lei relativa à



segurança dos dispositivos e materiais elétricos proíbe a utilização de cabos com certificação UL (com as letras "UL" ou "CSA" no cabo), não regulada pela lei ao mostrar "PSE" no cabo, em qualquer outro dispositivo elétrico além dos produtos concebidos pela CISCO.



Declaração 1073—Não existem peças passíveis de assistência por parte do utilizador

Não existem peças passíveis de assistência por parte do utilizador. Não abrir.

Quando instalar um chassi, tenha em consideração as seguintes orientações:

- Certifique-se de que existe espaço suficiente em redor do chassi para poder efetuar manutenção e permitir um fluxo de ar adequado. No chassi, o fluxo de ar processa-se no sentido da parte frontal para a parte traseira.



Para garantir que o fluxo de ar se processa corretamente, tem de montar o chassi no rack com os kits de calhas. Se colocar as unidades fisicamente empilhadas umas sobre as outras sem os kits de calhas, vai bloquear os orifícios de ventilação existentes na parte superior do chassi, o que pode provocar sobreaquecimento, um aumento da velocidade das ventoinhas e um maior consumo de energia. Quando instalar o chassi no rack, recomenda-se que o monte com os kits de calhas, uma vez que estes garantem o espaçamento mínimo necessário entre o chassi e o rack. Se montar o chassi com os kits de calhas, não tem de acrescentar qualquer espaçamento adicional entre chassi e o rack.

- Certifique-se de que o ar condicionado tem capacidade para manter o chassi a uma temperatura de 5 a 35 °C.
- Certifique-se de que o armário ou o rack estão em conformidade com os requisitos de rack.
- Certifique-se de que a alimentação no local está em conformidade com os requisitos de alimentação indicados na [folha de especificações](#) do seu dispositivo. Se disponível, pode utilizar uma UPS como proteção contra falhas de alimentação.



Evite os tipos de UPS que utilizam tecnologia ferorrressonante. Estes tipos de UPS podem tornar-se instáveis com estes sistemas, que podem



ter flutuações de consumo de corrente substanciais devido a padrões de tráfego de dados irregulares.

## Recomendações de segurança

As informações a seguir ajudam a garantir a sua segurança e a proteger o chassi. Estas informações podem não abranger todas as situações potencialmente perigosas no seu ambiente de trabalho, por isso, esteja atento e avalie sempre bem cada situação.

Observe estas diretrizes de segurança:

- Mantenha a área desimpedida e sem pó antes, durante e após a instalação.
- Mantenha as ferramentas afastadas das áreas de passagem onde o utilizador ou outras pessoas possam tropeçar nas mesmas.
- Não use vestuário largo nem joias, como brincos, pulseiras ou colares que possam ficar presos no chassi.
- Use óculos de segurança se trabalhar em condições que possam ser perigosas para os olhos.
- Não realize qualquer ação que represente perigo para as pessoas ou que afete a segurança do equipamento.
- Nunca tente elevar um objeto demasiado pesado para uma só pessoa.

## Manter a segurança elétrica



Antes de realizar trabalhos num chassi, certifique-se de que o cabo de alimentação foi desligado.

Respeite estas orientações ao operar equipamento alimentado a eletricidade:

- Não trabalhe sozinho quando existam condições perigosas no seu espaço de trabalho.
- Nunca presuma que a eletricidade está desligada; verifique sempre.
- Observe bem a sua área de trabalho para detetar eventuais perigos, como pisos húmidos, cabos de extensões elétricas sem ligação à terra, cabos elétricos desgastados e ausência de ligações à terra de segurança.
- Se ocorrer um acidente elétrico:
  - Tenha cuidado para não se magoar.
  - Desligue a alimentação do sistema.

- Se possível, peça a outra pessoa para chamar assistência médica. Caso contrário, avalie o estado da vítima e, em seguida, solicite socorro.
- Determine se a pessoa precisa de respiração cardiopulmonar ou de compressões torácicas e atue em conformidade.
- Utilize o chassi de acordo com as especificações elétricas assinaladas e as instruções de utilização do produto.

## Prevenção de danos resultantes de descarga eletrostática (ESD)

As descargas eletrostáticas (ESD) ocorrem quando os componentes eletrônicos são manuseados incorretamente e podem danificar o equipamento, bem como afetar os circuitos elétricos, o que pode provocar avarias intermitentes ou a avaria total do seu equipamento.

Siga sempre os procedimentos de prevenção de ESD quando remover e substituir componentes. Assegure-se de que o chassi está eletricamente ligado à terra. Use uma pulseira anti-ESD e certifique-se de que esta está sempre em contacto com a pele. Prenda a presilha de ligação à terra numa superfície não pintada da frame do chassi para encaminhar tensões de ESD de forma segura para a terra. Para prevenir devidamente danos e choques decorrentes de ESD, a pulseira e o cabo têm de funcionar eficazmente. Caso não disponha de uma pulseira, proteja-se tocando numa parte metálica do chassi.

Por motivos de segurança, verifique periodicamente o valor de resistência da pulseira antiestática, que deve situar-se entre um e 10 megohms.

## Ambiente do local

Para evitar avarias no equipamento e reduzir a possibilidade de encerramentos provocados pelas condições do ambiente, planeie cuidadosamente a configuração do local e a localização do equipamento. Se verificar que estão a ocorrer encerramentos frequentes ou se existirem taxas de erro invulgarmente elevadas no seu equipamento, pode ser útil isolar a causa dessas falhas e evitar problemas futuros.

## Considerações sobre a fonte de alimentação

Quando instalar o chassi, considere o seguinte:

- Assegure a existência de alimentação no local antes de instalar o chassi para garantir que está livre de picos e ruído. Se necessário, instale um condicionador de potência, para assegurar as tensões corretas e níveis de potência corretos na

tensão de entrada do dispositivo.

- Instale uma ligação à terra correta para evitar danos provocados por relâmpagos e picos de corrente no local.
- O chassi não tem um intervalo de operação selecionável pelo utilizador. Consulte a identificação no chassi relativa ao requisito de potência de entrada correta do dispositivo.
- Estão disponíveis vários tipos de cabos de alimentação CA para o dispositivo; certifique-se de que possui o tipo adequado ao seu local.
- Se estiver a utilizar fontes de alimentação redundantes duplas (1+1), recomendamos que utilize circuitos elétricos independentes para cada fonte de alimentação.
- Instale uma fonte de alimentação ininterrupta no seu local, se possível.

## Considerações relativas à configuração do rack

Considere o seguinte quando planear uma configuração de bastidor:

- Assegure-se de que a frame do bastidor não bloqueia as portas de admissão e de exaustão se estiver a montar um chassi num bastidor aberto.
- Assegure que os bastidores fechados possuem uma ventilação adequada. Certifique-se de que o bastidor não está demasiado congestionado, já que cada chassi produz calor. Os bastidores fechados devem ter laterais em persiana e uma ventoinha para fornecer ar de ventilação.
- Num bastidor fechado com uma ventoinha de ventilação na parte superior, o calor produzido pelo equipamento próximo da parte inferior do bastidor pode ser puxado para cima e para dentro das portas de admissão do equipamento que se encontra por cima, no bastidor. Assegure uma ventilação adequada no equipamento na parte inferior do bastidor.
- A utilização de defletores pode ajudar a isolar o ar de exaustão do ar de admissão, ajudando também a captar o ar de ventilação através do chassi. O melhor posicionamento dos defletores depende dos padrões de fluxo de ar do bastidor. Experimente diferentes disposições para posicionar os defletores da forma mais eficaz.



# Anexo B. Instalação de hardware Stealthwatch

Esta secção aborda a instalação dos dispositivos no seu ambiente. Inclui:

- **Montagem do dispositivo**
- **Ligação do dispositivo à rede**
- **Ligação do dispositivo**
- **Configurar as definições de rede utilizando a Configuração inicial**

## Montagem do dispositivo

Pode montar os dispositivos Stealthwatch diretamente num rack ou armário padrão de 19", em qualquer outro armário adequado ou sobre uma superfície plana. Quando montar um dispositivo num rack ou num armário, siga as instruções incluídas nos kits de calhas de montagem. Quando determinar o local onde o equipamento ficará montado, certifique-se de que deixa uma folga nos painéis frontal e traseiro para que:

- Os indicadores do painel frontal sejam fáceis de ler
- O espaço de acesso às portas do painel traseiro seja suficiente para não limitar a cablagem
- A tomada de alimentação do painel traseiro fique perto de uma fonte de alimentação AC condicionada
- O fluxo de ar em torno do dispositivo e no interior das condutas não apresente restrições.

## Hardware incluído com o dispositivo

Os dispositivos Stealthwatch incluem o seguinte hardware:

- Cabo de alimentação CA
- Chaves de acesso (para a superfície frontal da placa)
- Kit de calhas para montagem em rack ou abas de montagem para dispositivos mais pequenos
- Para o Coletor de fluxo 5210, um cabo de SFP de 10 GB

## Hardware adicional necessário

Tem de fornecer o seguinte hardware adicional necessário:

- Parafuso de montagem para um rack padrão de 19"
- Uma fonte de alimentação ininterrupta (UPS) para cada dispositivo que instalar
- Para efetuar a configuração local (opcional), recorra a um dos seguintes métodos:
  - Computador portátil com um cabo de vídeo e um cabo USB (para o teclado)
  - Monitor de vídeo com um cabo de vídeo e um teclado com um cabo USB

## Ligação do dispositivo à rede

Utilize o mesmo procedimento para ligar todos os dispositivos à rede. Em termos de ligação, a única diferença consiste no tipo de dispositivo que tem.



Não atualize o dispositivo BIOS, pois pode provocar problemas na funcionalidade do dispositivo.

Para obter informações detalhadas relativas às especificações, consulte as [Folhas de especificações Stealthwatch](#).



Todo o hardware Cisco x2xx utiliza a mesma plataforma UCS, a UCSC-C220-M5SX, exceto o Coletor de fluxo 5210 DB, que utiliza a UCSC-C240-M5SX. As diferenças entre dispositivos estão nas placas NIC, no processador, na memória, no armazenamento e no RAID.



O Coletor de fluxo 5210 é composto por dois servidores ligados (motor e base de dados) e funciona como um único dispositivo. Devido a isso, a instalação é ligeiramente diferente da de outros dispositivos. Primeiro, ligue os servidores entre si através de um cabo 10G SFP+ DA Cross Connect. Em seguida, ligue-os à sua rede.

Para ligar o dispositivo à rede:

1. Ligue um cabo Ethernet à porta de gestão, situada na parte traseira do dispositivo.
2. Ligue, pelo menos, uma porta de monitorização para os Sensores de fluxo e para os Encaminhadores de UDP.

No caso do Encaminhador de UDP HA, ligue os Encaminhadores de UDP através de cabos crossover. Ligue a porta eth2 de um Encaminhador de UDP à porta eth2 do segundo Encaminhador de UDP. Da mesma forma, ligue a porta eth3 de cada Encaminhador de UDP com um segundo cabo crossover. O cabo pode ser de fibra ótica ou em cobre.

Certifique-se de que toma nota da etiqueta Ethernet (eth2, eth3, etc.) de cada porta. Estas etiquetas correspondem às interfaces de rede (eth2, eth3, etc.) que são apresentadas e podem ser configuradas na página Inicial da interface de administrador do dispositivo.

3. Ligue a outra extremidade dos cabos Ethernet ao switch da sua rede.
4. Ligue os cabos de alimentação à fonte de alimentação. Alguns dispositivos têm duas ligações de alimentação: Power Supply 1 e Power Supply 2.

## Ligação do dispositivo

Esta secção descreve como ligar o dispositivo de forma a alterar as palavras-passe de utilizador predefinidas.

Pode ligar o dispositivo através uma das seguintes formas:

- com um teclado e um monitor
- com um computador portátil (e um emulador de terminal)


No caso de dispositivos novos, o SSH está desativado. Tem de iniciar sessão na interface da Web de administrador do dispositivo para o ativar.

## Ligação com um teclado e um monitor

Para configurar localmente o endereço IP, siga os passos abaixo:

1. Ligue o cabo de alimentação ao dispositivo.
2. Prima o botão Power para ligar o dispositivo. Aguarde até concluir totalmente o arranque. Não interrompa o processo de arranque.

Pode ter de remover o painel frontal para ligar a alimentação.

Enquanto o sistema não arranca, as ventoinhas da fonte de alimentação de alguns modelos ligam-se. Verifique se o indicador LED no painel  frontal está ativo.

Certifique-se de que liga o dispositivo a uma fonte de alimentação ininterrupta (UPS). A fonte de alimentação tem de estar ligada à energia, caso contrário, o sistema apresenta um erro.

3. Ligar o teclado:

- Se tiver um teclado padrão, ligue-o ao conector de teclado padrão.
  - Se tiver um teclado USB, ligue-o a um conector USB.
4. Ligue o cabo de vídeo ao conector de vídeo. É apresentada a linha de comandos de início de sessão.
  5. Continue para a secção **Configurar as definições de rede utilizando a Configuração inicial**.

## Ligação com um computador portátil

Também pode ligar o dispositivo a um computador portátil que tenha um emulador de terminal.

Para ligar um dispositivo com um computador portátil:

1. Ligue o computador portátil ao dispositivo através de um dos seguintes métodos:
  - Ligue um cabo RS232 do conector de porta de série (DB9) do seu portátil à porta Console do dispositivo.
  - Ligue um cabo crossover da porta Ethernet do portátil à porta Management do dispositivo.
2. Ligue o cabo de alimentação ao dispositivo.
3. Prima o botão Power para ligar o dispositivo. Aguarde até concluir totalmente o arranque. Não interrompa o processo de arranque.

Pode ter de remover o painel frontal para ligar a alimentação.



Enquanto o sistema não arranca, as ventoinhas da fonte de alimentação de alguns modelos ligam-se. Verifique se o indicador LED no painel frontal está ativo. Certifique-se de que liga o dispositivo a uma fonte de alimentação ininterrupta (UPS). A fonte de alimentação tem de estar ligada à energia, caso contrário, o sistema apresenta um erro.

4. No computador portátil, estabeleça ligação ao dispositivo.

Pode utilizar qualquer emulador de terminal que tiver disponível para comunicar com o dispositivo.

5. Aplique as seguintes definições:

- BPS: 115200
- Bits de dados: 8
- Bit de paragem: 1
- Paridade: Nenhuma
- Controlo do fluxo: Nenhum

São apresentados o ecrã e a linha de comandos de início de sessão.

6. Continue para a secção seguinte, **Configurar as definições de rede utilizando a Configuração inicial**.

## Configurar as definições de rede utilizando a Configuração inicial

Após se ligar ao dispositivo, utilize a Configuração inicial para configurar as definições de rede, incluindo endereços IP. Lembre-se do seguinte:

- Se implementar um SMC 2210 ou Coletor de fluxo 4210 com um Data Store, além de configurar os endereços IP, pode também configurar o SMC ou Coletor de fluxo para utilização de Data Store e o tipo de porta física que utiliza para a porta de gestão `eth0`.



Se optar por configurar o seu SMC ou Coletor de fluxo para utilização com um Data Store, não pode atualizar a configuração do dispositivo para alterar esta configuração. Tem de submeter o dispositivo a RFD se seleccionar a opção errada. Ative esta opção apenas se planear implementar um Data Store na sua rede.

- Se o seu dispositivo for um Nós de dados, pode configurar o tipo de porta física que este utiliza para a porta de gestão `eth0` e o endereço IP e informação relacionada para o canal de porta `eth2` ou `eth2/eth3` para comunicações Nós de dados.

Consulte o [Guia de instalação e configuração do hardware de cluster do Data Store](#) para mais informações sobre a instalação dos dispositivos SMC 2210, FC 4210 e Nós de dados.

Após configurar os endereços IP e portas, altere as palavras-passe de utilizador.



Na primeira vez que entrar na Configuração do sistema, o assistente de Configuração inicial abre-se e guia-o ao longo da configuração inicial do



dispositivo. Se sair da Configuração inicial antes de concluir o assistente, na próxima vez que entrar na Configuração inicial, o assistente de Configuração inicial abre-se novamente.

Com base no seu dispositivo, acesse à secção seguinte:

- [Dispositivos compatíveis com Data Store \(SMC 2210, FC 4210\)](#)
- [Configuração geral de dispositivo Stealthwatch](#)
- [Configuração de Nó de dados](#)

## Configuração geral de dispositivo Stealthwatch

Para todos os dispositivos exceto Nós de dados, SMC 2210 e FC 4210, a Configuração inicial apresenta a seguinte configuração:

- [Configure o endereço IP e a informação de gestão do dispositivo](#)

## Configure o endereço IP e a informação de gestão do dispositivo:

Na Configuração inicial, pode configurar o endereço IP de gestão eth0 e informação relacionada do dispositivo. Para a maior parte dos dispositivos, esta é a primeira configuração na Configuração inicial.

### Antes de começar

- Se estiver a configurar um Nós de dados, acesse a [Configuração de Nó de dados](#).
- Se estiver a configurar um SMC ou Coletor de fluxo compatível com Data Store, acesse a [Dispositivos compatíveis com Data Store \(SMC 2210, FC 4210\)](#).
- Se estiver a configurar qualquer outro dispositivo Stealthwatch, comece pelo passo 1.

### Procedimento

1. Inicie sessão no programa de Configuração do sistema:
  - Se estiver a configurar um dispositivo compatível com Nós de dados ou Data Store, digite `root` e prima **Enter**. Se estiver a configurar qualquer outro dispositivo, digite `sysadmin` e prima **Enter**.



São necessárias permissões de `root` para configurar corretamente o Data Store e a compatibilidade do Data Store.

- Quando for apresentada linha de comandos para introduzir a palavra-passe, introduza **lan1cope** e, em seguida, prima **Enter**.
  - Na linha de comandos seguinte, introduza **SystemConfig** e, em seguida, prima **Enter**.
2. Se é a primeira vez que entra na Configuração do sistema neste dispositivo, é aberta a Configuração inicial.

Caso contrário, abre-se o menu da Configuração do sistema. Selecione **Management** (Gestão) e, em seguida, prima **Enter**.

3. Introduza um **endereço IP** para este dispositivo.
4. Introduza a **máscara de sub-rede** da rede.
5. Introduza um endereço de **Gateway** para o endereço IP deste dispositivo.
6. Introduza um endereço de **Difusão** para o dispositivo.
7. Introduza um **Nome de anfitrião** para o seu dispositivo.
8. Introduza um **Domínio** para o seu dispositivo.
9. Selecione **Selecionar** e, em seguida, selecione **Sim** para confirmar as suas entradas.

Esta é a última opção de configuração na Configuração inicial. O seu dispositivo reinicia e implementa as alterações. Depois de reiniciar, abre-se a página Login (Início de sessão).

### O que fazer a seguir

- Altere as palavras-passe de utilizador. Consulte [Alteração da palavra-passe do utilizador Sysadmin](#) para obter mais informações.

### Dispositivos compatíveis com Data Store (SMC 2210, FC 4210)

Para o SMC 2210 e FC 4210, a Configuração inicial apresenta a seguinte configuração:

1. [Configure a porta física de gestão eth0](#)
2. [Configure o endereço IP e a informação de gestão do dispositivo](#)
3. [Configure a compatibilidade do Data Store](#)

## Configure a porta física de gestão eth0

Se configurar um SMC ou Coletor de fluxo compatível com Data Store e implementar um Data Store, pode, opcionalmente, configurar `eth0` como uma porta SFP+ DAC em vez da porta de cobre BASE-T predefinida. Para estes dispositivos, esta é a primeira configuração na Configuração inicial.

### Antes de começar

- Se estiver a configurar um Nós de dados ou um SMC ou Coletor de fluxo compatível com Data Store, consulte a [folha de especificações do Stealthwatch relativa ao seu dispositivo](#) para informações sobre as portas SFP+ e BASE-T suportadas.
- Se estiver a configurar um Nós de dados, aceda a [Configuração de Nó de dados](#).
- Se estiver a configurar qualquer outro dispositivo Stealthwatch além de dispositivos compatíveis com Data Store, consulte [Configuração geral de dispositivo Stealthwatch](#).

### Procedimento

1. Inicie sessão no programa de Configuração do sistema:

- Digite **root** e, em seguida, prima **Enter**.



São necessárias permissões de `root` para configurar corretamente a compatibilidade do Data Store.

- Quando for apresentada linha de comandos para introduzir a palavra-passe, introduza **lan1cope** e, em seguida, prima **Enter**.
  - Na linha de comandos seguinte, introduza **SystemConfig** e, em seguida, prima **Enter**.
2. Se é a primeira vez que entra na Configuração do sistema neste dispositivo, é aberta a Configuração inicial e apresentada a configuração de Ordem de portas Avance para o passo 5.

Caso contrário, abre-se o menu da Configuração do sistema. Selecione **Management** (Gestão) e, em seguida, prima **Enter**.

3. A partir do menu Configuração do sistema, selecione **Rede** e, em seguida, prima **Enter**.
4. Selecione **Ordem de portas** e prima **Enter**.
5. Tem as seguintes opções:



- Selecione **LOM** para configurar o seu dispositivo para utilizar uma porta de cobre BASE-T para eth0.
  - Selecione **SFP+** para configurar o seu dispositivo para utilizar uma porta de fibra SFP+ para eth0.
6. Selecione **OK** para confirmar a sua seleção.

### O que fazer a seguir

- Configure o endereço IP e a informação de gestão da porta de gestão eth0. Consulte o procedimento seguinte.

## Configurar o endereço IP e a informação de gestão do dispositivo:


Na Configuração inicial, pode configurar o endereço IP de gestão eth0 e informação relacionada do dispositivo. Para dispositivos compatíveis com Data Store, esta configuração ocorre após configurar a porta de gestão física eth0.

### Antes de começar

- Se estiver a configurar um SMC ou Coletor de fluxo compatível com Data Store, após configurar a Ordem de portas, o assistente de Configuração inicial apresenta a configuração de gestão eth0. Avance para o passo 3.

### Procedimento

1. Inicie sessão no programa de Configuração do sistema:
  - Se estiver a configurar um dispositivo compatível com Data Store, digite `root` e prima **Enter**.

 São necessárias permissões de `root` para configurar corretamente o Data Store e a compatibilidade do Data Store.

  - Quando for apresentada linha de comandos para introduzir a palavra-passe, introduza **lan1cope** e, em seguida, prima **Enter**.
  - Na linha de comandos seguinte, introduza **SystemConfig** e, em seguida, prima **Enter**.
2. Se é a primeira vez que entra na Configuração do sistema neste dispositivo, é aberta a Configuração inicial.

Caso contrário, abre-se o menu da Configuração do sistema. Selecione **Management** (Gestão) e, em seguida, prima **Enter**.

3. Introduza um **endereço IP** para este dispositivo.
4. Introduza a **máscara de sub-rede** da rede.
5. Introduza um endereço de **Gateway** para o endereço IP deste dispositivo.
6. Introduza um endereço de **Difusão** para o dispositivo.
7. Introduza um **Nome de anfitrião** para o seu dispositivo.
8. Introduza um **Domínio** para o seu dispositivo.
9. Selecione **Selecionar** e, em seguida, selecione **Sim** para confirmar as suas entradas.

### O que fazer a seguir

- Configure o dispositivo para utilização sem um Data Store. Consulte o procedimento seguinte para obter mais informações.

## Configure a utilização do Data Store

Configure o seu SMC 2210 ou FC 4210 para funcionar com um Data Store. Os seus Coletores de fluxo serão ligados ao Data Store e o seu SMC consultará o Data Store.



Se optar por configurar o seu SMC ou Coletor de fluxo para utilização com um Data Store, não pode atualizar a configuração do dispositivo para alterar esta configuração. Tem de submeter o dispositivo a RFD se selecionar a opção errada. Ative esta opção **apenas se** planear implementar um Data Store na sua rede.



Tem de configurar todos os seus SMCs e Coletores de fluxo para utilização com um Data Store se implementar um Data Store. Não pode configurar alguns dos seus Coletores de fluxo para ligação ao Data Store e outros para ligação direta ao SMC.

### Antes de começar

- Se estiver na Configuração inicial, a Configuração do sistema apresenta a configuração do Data Store após terminar a configuração do endereço IP do dispositivo. Avance para o passo 3.

### Procedimento

1. A partir do menu de Configuração do Sistema. Selecione **Avançadas** e prima **Enter**.
2. Selecione **Data Store** e prima Enter.
3. Selecione **Sim** para configurar o seu dispositivo para compatibilidade com um Data Store.



Se optar por configurar o seu SMC ou Coletor de fluxo para utilização com um Data Store, não pode atualizar a configuração do dispositivo para alterar esta configuração. Tem de submeter o dispositivo a RFD se selecionar a opção errada. Ative esta opção **apenas se** planear implementar um Data Store na sua rede.

4. Selecione **OK** para confirmar a sua seleção.

Esta é a última opção de configuração na Configuração inicial. O seu dispositivo reinicia e implementa as alterações. Depois de reiniciar, abre-se a página Login (Início de sessão).

### O que fazer a seguir

- Altere as palavras-passe de utilizador. Consulte [Alteração da palavra-passe do utilizador Sysadmin](#) para obter mais informações.

## Configuração de Nó de dados

Para Nós de dados, a Configuração inicial apresenta a seguinte configuração:

1. [Configure a porta física de gestão eth0](#)
2. [Configure o endereço IP e a informação de gestão do dispositivo](#)
3. [Configure eth2 e eth3 para comunicações inter-Nós de dados](#)

## Configure a porta física de gestão eth0

Se configurar um Nós de dados, opcionalmente, pode configurar `eth0` como uma porta de cobre BASE-T em vez da porta SFP+ DAC predefinida. Para estes dispositivos, esta é a primeira configuração na Configuração inicial.

### Antes de começar

- Se estiver a configurar um Nós de dados, consulte [a folha de especificações do Stealthwatch relativa ao seu dispositivo](#) para informações sobre as portas SFP+ e BASE-T suportadas.

- Se estiver a configurar um SMC ou Coletor de fluxo compatível com Data Store, aceda a [Dispositivos compatíveis com Data Store \(SMC 2210, FC 4210\)](#).
- Se estiver a configurar qualquer outro dispositivo Stealthwatch além de dispositivos compatíveis com Data Store, consulte [Configuração geral de dispositivo Stealthwatch](#).

## Procedimento

1. Inicie sessão no programa de Configuração do sistema:

- Digite **root** e, em seguida, prima **Enter**.



São necessárias permissões de `root` para configurar corretamente a compatibilidade do Data Store.

- Quando for apresentada linha de comandos para introduzir a palavra-passe, introduza **lan1cope** e, em seguida, prima **Enter**.
  - Na linha de comandos seguinte, introduza **SystemConfig** e, em seguida, prima **Enter**.
2. Se é a primeira vez que entra na Configuração do sistema neste dispositivo, é aberta a Configuração inicial e apresentada a configuração de Ordem de portas Avance para o passo 5.

Caso contrário, abre-se o menu da Configuração do sistema. Selecione **Management** (Gestão) e, em seguida, prima **Enter**.

3. A partir do menu Configuração do sistema, selecione **Rede** e, em seguida, prima **Enter**.
4. Selecione **Ordem de portas** e prima Enter.
5. Tem as seguintes opções:
- Selecione **SFP+** para configurar o seu dispositivo para utilizar uma porta de fibra SFP+ para eth0.
  - Selecione **LOM** para configurar o seu dispositivo para utilizar uma porta de cobre BASE-T para eth0.
6. Selecione **OK** para confirmar a sua seleção.

## O que fazer a seguir

- Configure o endereço IP e a informação de gestão da porta de gestão eth0. Consulte o procedimento seguinte.

## Configurar o endereço IP e a informação de gestão do

## dispositivo:

Na Configuração inicial, pode configurar o endereço IP de gestão eth0 e informação relacionada do dispositivo.

### Antes de começar

- Se estiver a configurar um Nós de dados, após configurar a Ordem de portas, o assistente de Configuração inicial apresenta a configuração de gestão eth0. Avance para o passo 3.

### Procedimento

1. Inicie sessão no programa de Configuração do sistema:

- Se estiver a configurar um Nós de dados, digite `root` e prima **Enter**.



São necessárias permissões de `root` para configurar corretamente o Data Store e a compatibilidade do Data Store.

- Quando for apresentada linha de comandos para introduzir a palavra-passe, introduza **lan1cope** e, em seguida, prima **Enter**.
  - Na linha de comandos seguinte, introduza **SystemConfig** e, em seguida, prima **Enter**.
2. Se é a primeira vez que entra na Configuração do sistema neste dispositivo, é aberta a Configuração inicial.

Caso contrário, abre-se o menu da Configuração do sistema. Selecione **Management** (Gestão) e, em seguida, prima **Enter**.

3. Introduza um **endereço IP** para este dispositivo.
4. Introduza a **máscara de sub-rede** da rede.
5. Introduza um endereço de **Gateway** para o endereço IP deste dispositivo.
6. Introduza um endereço de **Difusão** para o dispositivo.
7. Introduza um **Nome de anfitrião** para o seu dispositivo.
8. Introduza um **Domínio** para o seu dispositivo.
9. Selecione **Selecionar** e, em seguida, selecione **Sim** para confirmar as suas entradas.

### O que fazer a seguir

- Configure a informação de gestão da porta de comunicação do Nós de dados. Consulte [Configure eth2 e eth3 para comunicações inter-Nós de dados:](#) para mais informações.

## Configure eth2 e eth3 para comunicações inter-Nós de dados:

Quando configurar um dispositivo Nós de dados, configure a porta de comunicação inter-Nós de dados com um endereço IP não encaminhável. Pode configurar uma das seguintes opções:

- eth2
- canal de porta com eth2 e eth3



Tem de atribuir endereços IP não encaminháveis a partir do bloco 169.254.42.0/24 CIDR .

### Antes de começar

- Consulte [a folha de especificações do Stealthwatch para o seu dispositivo](#) para informação sobre as portas eth2 e eth3 SFP+ . Note que eth2 e eth3 dependem da forma como configura eth0.
- Se estiver na Configuração inicial, a Configuração do sistema apresenta a configuração de canal de porta eth2 ou eth2/eth3 após terminar a configuração da informação de gestão eth0 do dispositivo. Avance para o passo 3.

### Procedimento

1. A partir do menu Configuração do sistema, selecione **Rede** e, em seguida, prima **Enter**.
2. Selecione **Comunicações de nó** e prima Enter.
3. Selecione a configuração de porta de comunicação inter-Nós de dados. Tem as seguintes opções:
  - Selecione **Sim** para agregar eth2 e eth3 como um canal de porta para comunicações inter-Nós de dados.
  - Selecione **Não** para utilizar eth2 para comunicações inter-Nós de dados.
4. Introduza um endereço **IP não encaminhável** a partir do bloco 169.254.42.0/24 CIDR para o canal de porta eth2 ou eth2/eth3.
5. Introduza uma **Máscara de rede** de 255.255.255.0 para este endereço IP.

6. Introduza um endereço de **Gateway** para este endereço IP.
7. Introduza um endereço de **Difusão** para este endereço IP.
8. Selecione **Selecionar** e, em seguida, selecione **Sim** para confirmar as suas entradas.

Esta é a última opção de configuração na Configuração inicial. O seu dispositivo reinicia e implementa as alterações. Depois de reiniciar, abre-se a página Login (Início de sessão).

### O que fazer a seguir

- Altere as palavras-passe de utilizador. Consulte [Alteração da palavra-passe do utilizador Sysadmin](#) para obter mais informações.

### Alteração da palavra-passe do utilizador Sysadmin

Para garantir que a sua rede é segura, altere a palavra-passe predefinida para o utilizador sysadmin no dispositivos.

## Altere a palavra-passe de sysadmin:

### Antes de começar

- Inicie a sessão na consola do dispositivo como **sysadmin**.
- Entre na Configuração do sistema.

### Procedimento

1. No menu System Configuration (Configuração do sistema), selecione **Password** (Palavra-passe) e prima **Enter**.

Se alterou a lista de anfitriões fidedignos nas predefinições, certifique-se de que todos os dispositivos Stealthwatch estão incluídos nessa lista em todos os dispositivos Stealthwatch da sua implementação. Caso contrário, os dispositivos não conseguirão comunicar entre si.

Abaixo do menu, é apresentada a linha de comandos para introduzir a palavra-passe atual.

2. Introduza a palavra-passe atual e, em seguida, prima **Enter**.  
É apresentada a linha de comandos para introduzir uma palavra-passe nova.
3. Introduza a palavra-passe nova e, em seguida, prima **Enter**.

A palavra-passe tem de conter 8 a 30 caracteres alfanuméricos e não pode conter espaços. Também pode utilizar os seguintes caracteres especiais: \$ . ~ ! @ # % \_ = ? : , { } ( )

4. Volte a introduzir a palavra-passe e, em seguida, prima **Enter**.
5. Quando a palavra-passe for aceite, prima **Enter** novamente para voltar ao menu System Configuration (Configuração do sistema).
6. Continue para a próxima secção, **Alteração da palavra-passe do utilizador raiz**

## Alteração da palavra-passe do utilizador raiz

Depois de alterar a palavra-passe predefinida do utilizador sysadmin, altere a palavra-passe predefinida do utilizador raiz para proteger ainda mais a sua rede.

## Altere a palavra-passe do utilizador raiz:

### Antes de começar

- Inicie a sessão na consola do dispositivo como **sysadmin**.
- Entre na Configuração do sistema.

### Procedimento

1. Aceda à shell raiz.
2. No menu System Configuration (Configuração do sistema), selecione **Advanced** (Avançadas) e prima **Enter**. É apresentado o menu Advanced (Avançadas).
3. Selecione **RootShell** e, em seguida, prima **Enter**.  
É apresentado um pedido para introduzir uma palavra-passe do utilizador raiz.
4. Introduza a palavra-passe atual do utilizador raiz e, em seguida, prima **Enter**. É apresentada a linha de comandos da shell de raiz.
5. Introduza **SystemConfig** e, em seguida, prima **Enter**.  
Através deste comando, volta ao menu System Configuration (Configuração do sistema) para poder alterar a palavra-passe do utilizador raiz.
6. Selecione **Password** (Palavra-passe) e, em seguida, prima **Enter**. Abaixo do menu, é apresentada a linha de comandos para introduzir a palavra-passe.
7. Introduza a palavra-passe nova do utilizador raiz e, em seguida, prima **Enter**. É apresentado um segundo pedido.



8. Volte a introduzir a palavra-passe nova do utilizador raiz e, em seguida, prima **Enter**.
9. Assim que a palavra-passe for alterada com êxito, prima **Enter**. Desta forma, atualizou as palavras-passe predefinidas dos utilizadores sysadmin e raiz. Em seguida, volta ao menu da consola System Configuration (Configuração do sistema).
10. Selecione **Cancel** (Cancelar) e prima **Enter**. A consola System Configuration (Configuração do sistema) fecha-se e é apresentada a linha de comandos da shell raiz.
11. Introduza **exit** e prima **Enter**. É apresentada a linha de comandos de início de sessão.
12. Prima **Ctrl+Alt** para sair do ambiente da consola.

Agora já está tudo a postos para configurar o seu dispositivo. Para configurar o seu dispositivo, consulte o [Guia de configuração do sistema Stealthwatch](#) relativo à sua versão de software. A Série x2xx é compatível com as versões de software 7.x do Stealthwatch.

---

# Anexo C. Configurar os seus dispositivos

Quando iniciar a sessão no dispositivo pela primeira vez, utilizará a Ferramenta de configuração de dispositivo para configurar as suas definições de dispositivo.

## Requisitos da ferramenta de configuração de dispositivo

- Confirme que as suas firewalls e ACLs (Access Control List) permitirão o acesso.
- Obtenha o nome de anfitrião para o dispositivo e os endereços IP para o seguinte:
  - dispositivo
  - máscara de sub-rede
  - gateways predefinidos e de difusão
  - servidores NTP e DNS
  - endereço IP de SMC para Gestão Central

## Geridos

Como parte da Ferramenta de configuração de dispositivo, irá configurar o seu dispositivo a ser gerido pela sua Consola de Gestão Stealthwatch (SMC) principal.

Quando os seus dispositivos forem geridos pela sua Consola de Gestão Stealthwatch (SMC), pode utilizar a Gestão Central para editar as configurações de dispositivo, software de atualização, reinício, encerramento e outros.

## SMC de ativação pós-falha

Se tiver mais de uma Consola de Gestão Stealthwatch (SMC), pode configurar um par de ativação pós-falha de SMC para que uma sirva de consola de cópia de segurança para a outra.

- Utilize a Ferramenta de configuração de dispositivo para configurar cada SMC individual.
- Planeie qual o SMC que será principal e secundário.
- Após configurar cada SMC individual, utilizará o Armazenamento de Confiança de Gestão Central e o Cliente de Ambiente de Trabalho Stealthwatch para configurar a relação de ativação pós-falha de SMC.

## Boas Práticas

Para configurar o seu sistema com sucesso, certifique-se de que segue as instruções deste guia.

Recomendamos o seguinte:

- **Um de cada vez:** Configure um dispositivo de cada vez. Confirme que o dispositivo está **Ativo** antes de começar a configurar o dispositivo seguinte no seu cluster.
- **Ordem:** Siga a ordem de configuração.
- **Múltiplos Gestores Centrais:** Pode configurar mais de um Gestor Central no seu sistema. No entanto, cada dispositivo pode ser gerido por apenas um SMC principal/Gestor Central.
- **Acesso:** Tem de ter privilégios de administrador para aceder à Gestão Central.

## Ordem de configuração

Configure os seus dispositivos pela ordem seguinte e anote os dados para cada dispositivo:

Pedido	Dispositivo	Detalhes
1.	SMC principal	O seu SMC principal é o seu Gestor Central.  Certifique-se de que o SMC é apresentado como Ativo antes de começar a configurar o dispositivo seguinte no sistema.
2.	UDP Directors (também designados por Replicadores de fluxo)	
3.	Nó de dados	
4.	Base de dados do Coletor de fluxo 5000 Series	Certifique-se de que a base de dados do Coletor de fluxo 5000 series é apresentada como Ativa antes de iniciar a configuração do motor.

5.	Motor do Coletor de fluxo 5000 Series	Certifique-se de que a base de dados do Coletor de fluxo 5000 series é apresentada como Ativa antes de iniciar a configuração do motor.
6.	Todos os outros coletores de fluxo (NetFlow e sFlow)	
7.	Sensores de fluxo	Certifique-se de que o seu Coletor de fluxo é apresentado como Ativo antes de iniciar a configuração do Sensor de fluxo.
8.	Concentrador do ponto final	
9.	SMC secundário (se utilizado)	Certifique-se de que o SMC principal é apresentado como Ativo antes de iniciar a configuração do SMC secundário. O SMC secundário seleciona-se a si próprio como Gestor Central. Configure a ativação pós-falha após serem configurados todos os dispositivos.



Podem não ser apresentados aqui todos os dispositivos do seu sistema.

## 1. Iniciar sessão

Utilize as instruções seguintes para configurar cada dispositivo utilizando a Ferramenta de configuração de dispositivo.

1. No campo de endereço do seu browser, introduza **https://** seguido do endereço IP do dispositivo.
  - **SMC principal:** Configure primeiro o SMC principal.
  - **Ativo:** Confirme que cada dispositivo está Ativo antes de começar a configurar o dispositivo seguinte no seu cluster.

- **Ordem:** Certifique-se de que [configura os seus dispositivos por ordem](#) para que comuniquem corretamente.

2. Introduza as credenciais seguintes para iniciar a sessão:

- **Nome do utilizador:** admin
- **Palavra-passe:** lan411cope

## 2. Configure o dispositivo

Quando inicia a sessão no dispositivo pela primeira vez, a Ferramenta de configuração de dispositivo orienta-o ao longo de cada passo de configuração.

1. **Alterar palavra-passe predefinida:** Introduza novas palavras-passe para admin, root e sysadmin. Clique em **Seguinte** para percorrer cada utilizador.

Utilize os critérios seguintes:

- **Tamanho:** 8 a 30 caracteres
- **Alteração:** Certifique-se de que a nova palavra-passe é diferente da palavra-passe predefinida em, pelo menos, 4 caracteres.

Utilizador	Palavra-passe predefinida
admin	lan411cope
root	lan1cope
sysadmin	lan1cope



Os menus sysadmin e root estão indisponíveis se já tiver alterado as palavras-passe predefinidas durante a instalação de hardware. Consulte o [Manual de instalação de hardware Stealthwatch x210 Series](#) para obter mais detalhes.

2. **Interface de rede de gestão:** Reveja os campos do endereço IP e de interface de rede. Confirme que as predefinições estão corretas. Clique em **Next** (Seguinte).

- **Alterações:** Para alterar esta informação, consulte o seu administrador de

rede e a Resolução de problemas.

- **IPv6 (opcional):** Para ativar IPv6, clique em **IPv6**. Selecione a caixa de verificação **Enable IPv6** e preencha os campos.

3. **Nome de anfitrião e Domínios:** Introduza o nome de anfitrião e o nome do domínio de rede. Clique em **Next** (Seguinte).

- **Nome de anfitrião:** É necessário um nome de anfitrião único para cada dispositivo. Se atribuir os mesmos nomes de anfitrião aos seus dispositivos, não serão instalados com sucesso.
- **Domínio de rede:** É necessário um nome de domínio totalmente qualificado para cada dispositivo.
- **Domínio Stealthwatch (apenas SMC):** Introduza um domínio de Stealthwatch para os seus dispositivos Stealthwatch.
- **Intervalos de Endereços (apenas SMC):** Selecione o intervalo de endereços IP para a sua rede Stealthwatch.

4. **Definições DNS:** Confirme que a predefinição está correta ou introduza o endereço IP do servidor de domínio. Clique em **Next** (Seguinte).

Adicionar ou Eliminar Servidores DNS (opcional):

- **Adicionar:** Clique no ícone +.
- **Eliminar:** Clique na caixa de verificação para selecionar o servidor DNS. Clique no ícone -.

5. **Definições NTP:** Confirme que a predefinição está correta ou clique no ícone **Menu** para selecionar o seu servidor NTP (Network Time Protocol). Clique em **Next** (Seguinte).

- **Múltiplos Servidores NTP:** Recomendamos que configure múltiplos servidores NTP quanto a redundância e precisão.
- **Fonte pública:** pool.ntp.org é uma boa fonte pública para NTP.

Adicionar ou Eliminar Servidores NTP (opcional):

- **Adicionar:** Clique no ícone +.

- **Eliminar:** Clique na caixa de verificação para selecionar o servidor NTP. Clique no ícone -.
6. Se o dispositivo for um SMC, aceda a **3. Registe a Consola de Gestão Stealthwatch**.

Se o dispositivo não for um SMC, aceda a **4. Adicione dispositivos à Gestão Central**.

### 3. Registe a Consola de Gestão Stealthwatch

1. **Reveja as suas definições:** Confirme que a informação do dispositivo está correta.
2. Clique em **Aplicar** ou **Reiniciar e continuar**.

Siga as indicações do ecrã enquanto o dispositivo é reiniciado.

Aguarde alguns minutos até as novas definições do sistema terem efeito. Pode ter de atualizar a página.

3. Inicie a sessão na Consola de Gestão Stealthwatch.
4. A Ferramenta de configuração do dispositivo é novamente aberta. Clique em **Continuar**.
5. No separador Registe o seu dispositivo, consulte o endereço IP e clique em **Guardar**.
  - Isto instala a Gestão Central na Consola de Gestão Stealthwatch.
  - O endereço IP do SMC é detetado automaticamente e não pode ser alterado.
6. Quando a instalação do dispositivo estiver concluída, clique em **Ir para o painel**.
7. Clique no ícone **Definições globais**. Selecione **Gestão Central**.
8. Reveja o inventário. Confirme que o estado do dispositivo SMC é apresentado como **Ativo**.



Certifique-se de que o SMC principal e cada dispositivo é apresentado como Ativo antes de começar a configurar o dispositivo seguinte no seu cluster utilizando a [ordem e os detalhes de configuração](#).

9. Implemente e configure o seu Data Store. Regresse à [Descrição geral da implementação do Data Store Stealthwatch](#) para rever o processo de implementação.

## 4. Adicione dispositivos à Gestão Central

A Ferramenta de configuração de dispositivo continua a orientá-lo ao longo da configuração de dispositivo com a Gestão Central. Alguns passos podem variar consoante o dispositivo. Siga as indicações do ecrã.

1. No separador Gestão Central, introduza o endereço IP do seu SMC principal.

O seu SMC principal é o seu Gestor Central.

2. Clique em **Save** (Guardar).
3. Siga as indicações do ecrã para confiar no certificado de identidade do dispositivo SMC principal. Clique em **Sim** para confiar no certificado e permitir que o dispositivo comunique com o SMC.
4. Introduza as credenciais de início de sessão para o seu SMC principal.
5. Selecione o seu domínio de Stealthwatch.

- **Coletores de fluxo:** Introduza o número de porta da Coleção de fluxo.

Predefinição Netflow: 2055

Predefinição sFlow: 6343

- **Sensores de fluxo:** Selecione um Coletor de fluxo.

6. Clique em **Ir para Gestão Central**. Ir para **5. Confirme o estado do dispositivo**.

## 5. Confirme o estado do dispositivo

Após configurar um dispositivo na Ferramenta de configuração de dispositivo, confirme o estado do dispositivo na Gestão Central.

1. A Ferramenta de configuração de dispositivo é aberta no inventário da Gestão Central ou pode abri-la da seguinte forma:
  - Inicie a sessão na sua Consola de Gestão Stealthwatch principal.
  - Clique no ícone **Definições globais**.



- Selecione **Gestão Central**.
2. Reveja os dispositivos no inventário do Gestor de dispositivo.
    - Confirme que o dispositivo é apresentado no inventário.
    - Confirme que o estado do dispositivo é apresentado como Ativo.



Certifique-se de que o SMC principal e cada dispositivo é apresentado como Ativo antes de começar a configurar o dispositivo seguinte no seu cluster utilizando a [ordem e os detalhes de configuração](#).

3. Para configurar o dispositivo seguinte no seu sistema, aceda a **1. Iniciar sessão** e realize os procedimentos de **5. Confirme o estado do dispositivo**.

Se não tiver outro dispositivo a instalar, aceda ao Guia de configuração do sistema Stealthwatch para mais informações sobre a forma de realizar as configurações do dispositivo. Em alternativa, regresse à Descrição geral da implementação do Data Store [Stealthwatch](#) para rever o processo de implementação.

---

# Informação de Copyright

Cisco e o logótipo da Cisco são marcas comerciais ou marcas comerciais registadas da Cisco e/ou das respetivas empresas afiliadas nos EUA e noutros países. Para ver uma lista das marcas comerciais Cisco, aceda a este URL:

<https://www.cisco.com/go/trademarks>. As marcas comerciais de terceiros mencionadas são propriedade dos respetivos proprietários. A utilização da palavra parceiro não implica uma relação de parceria entre a Cisco e qualquer outra empresa.  
(1721R)