Cisco StealthWatch

Guía de instalación y configuración del hardware del almacén de datos

Índice

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Introducción a la instalación y configuración del hardware del almacén de datos

Descripción general

Esta guía explica cómo instalar Stealthwatch Almacén de datos como parte de la implementación de un sistema de Stealthwatch. Describe los componentes del sistema de Stealthwatch y cómo se colocan en el sistema, especialmente en relación con el Almacén de datos.

Este capítulo incluye los siguientes temas:

Público

Esta guía está diseñada para la persona responsable de la instalación del hardware del sistema de Stealthwatch. Damos por sentado que ya dispone de ciertos conocimientos generales sobre la instalación de equipos de red (recopilador de flujo y consola de gestión de Stealthwatch).

Para obtener información sobre la configuración de los productos del sistema de Stealthwatch, consulte la *Guía de configuración del sistema Stealthwatch*.

Utilización de esta guía

Además de esta introducción, hemos dividido esta guía en los siguientes capítulos:

Capítulo	Descripción
Arquitectura y conceptos del almacén de datos	Describe los conceptos básicos que sustentan la base de datos del Almacén de datos y la arquitectura básica relacionada con la implementación del Almacén de datos en relación con una SMC y con recopiladores de flujo.
Requisitos previos y recomendaciones de la	Describe el hardware de Stealthwatch compatible con el Almacén de datos y

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Capítulo	Descripción
implementación del almacén de datos	proporciona los requisitos y recomendaciones para la implementación del Almacén de datos, incluidos los puertos de comunicación que deben abrirse.
Stealthwatch Descripción general de la implementación del almacén de datos	Proporciona una descripción general de alto nivel de la implementación de appliances de Stealthwatch para su uso con un Almacén de datos.
Instalación del hardware del almacén de datos	Proporciona una descripción general integral de la implementación de appliances de Stealthwatch para su uso con un Almacén de datos y las instrucciones de configuración para inicializar la base de datos del Almacén de datos.
Configuración de conservación del almacén de datos	Proporciona información sobre la configuración del período de conservación de datos del Almacén de datos.
Pasos siguientes para la instalación del almacén de datos	Describe los pasos que debe seguir cuando termine de implementar y configurar su Almacén de datos.
Mantenimiento del almacén de datos	Describe las tareas de mantenimiento del Almacén de datos.
Resolución de problemas de implementación del almacén de datos	Describe los problemas comunes que se han detectado durante el proceso de instalación del Almacén de datos y las soluciones sugeridas.
Apéndice A. Preparación para la instalación	Proporciona advertencias para la instalación del hardware.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Capítulo	Descripción
Apéndice B. Instalación del hardware de Stealthwatch	Proporciona una descripción general de la instalación de appliances de Stealthwatch y la realización de la configuración inicial para asignar una dirección IP y otra información de gestión relacionada.
Apéndice C. Configuración de los appliances	Proporciona una descripción general del uso de la herramienta de configuración de appliances para configurar los appliances de Stealthwatch.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Arquitectura y conceptos del almacén de datos

> **No** instale a por su cuenta un Stealthwatch Almacén de datos. Si tiene previsto comprar un StealthwatchAlmacén de datos, póngase en contacto con los servicios profesionales de Cisco para obtener ayuda con la ubicación, la implementación y la configuración dentro y como parte de su implementación general de Stealthwatch.

El Stealthwatch Almacén de datos proporciona un repositorio central para almacenar la telemetría de su red, recopilada por los Stealthwatch recopiladores de flujo. El Almacén de datos se compone de un clúster de Nodo de datos, cada uno con una parte de sus datos, y una copia de seguridad de los datos de un Nodo de datos independiente. Debido a que todos sus datos se encuentran en una base de datos centralizada, en lugar de extenderse a través de varios recopiladores de flujo, su consola de administración de Stealthwatch puede recuperar los resultados de las consultas de Almacén de datos de manera más rápida que si consultara a todos los recopiladores de flujo por separado. El clúster Almacén de datos proporciona una tolerancia a errores mejorada, una respuesta de consulta mejorada y una población de gráficos y gráficos más rápida.

Almacenamiento del Almacén de datos y tolerancia a fallas

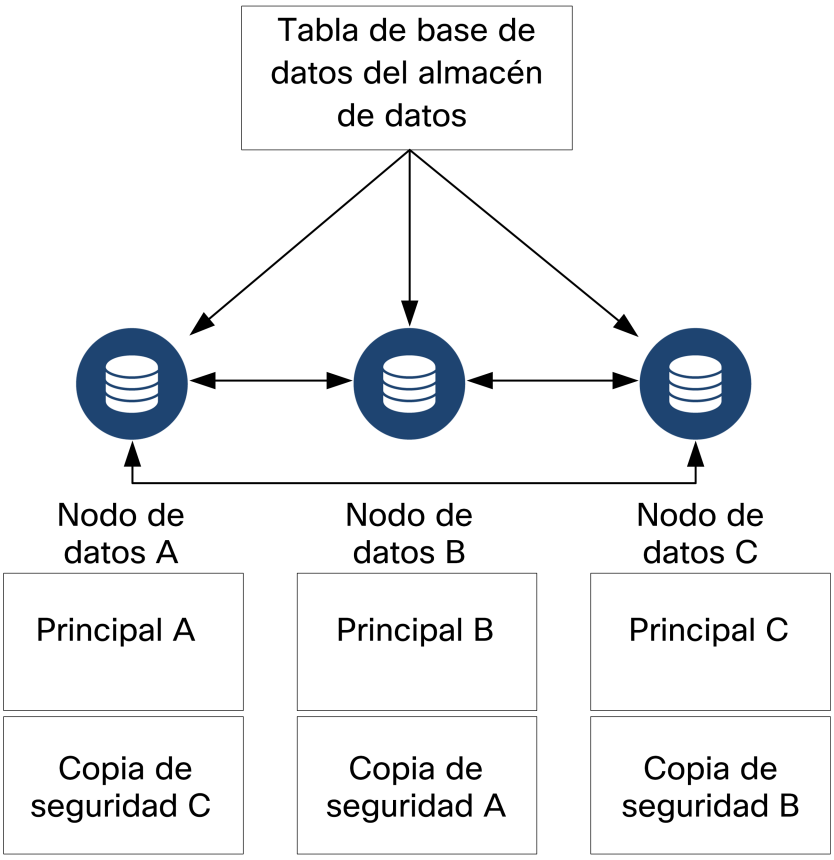
El Almacén de datos recopila datos de los recopiladores de flujo y los distribuye de manera equitativa entre los Nodos de datos en el clúster. Cada Nodo de datos, además de almacenar una parte de su telemetría general, también almacena una copia de seguridad de la telemetría de otro Nodo de datos. Almacenar datos de esta manera:

- ayuda con el equilibrio de carga
- distribuye el procesamiento entre cada nodo
- garantiza que todos los datos introducidos en el Almacén de datos tienen una copia de seguridad de tolerancia a errores
- permite aumentar el número de Nodos de datos para mejorar el almacenamiento general y el rendimiento de las consultas

Si un nodo se cae, mientras el nodo que contiene su copia de seguridad todavía esté disponible, y al menos la mitad de su número total de Nodos de datos todavía esté activo, el Almacén de datos en conjunto permanece activo. Esto le permite tiempo para reparar la conexión inactiva o el hardware defectuoso; después de sustituir el Nodo de datos defectuoso, el Almacén de Datos restaura los datos de ese nodo de la copia de seguridad existente almacenada en el Nodo de datos adyacente y crea una copia de

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

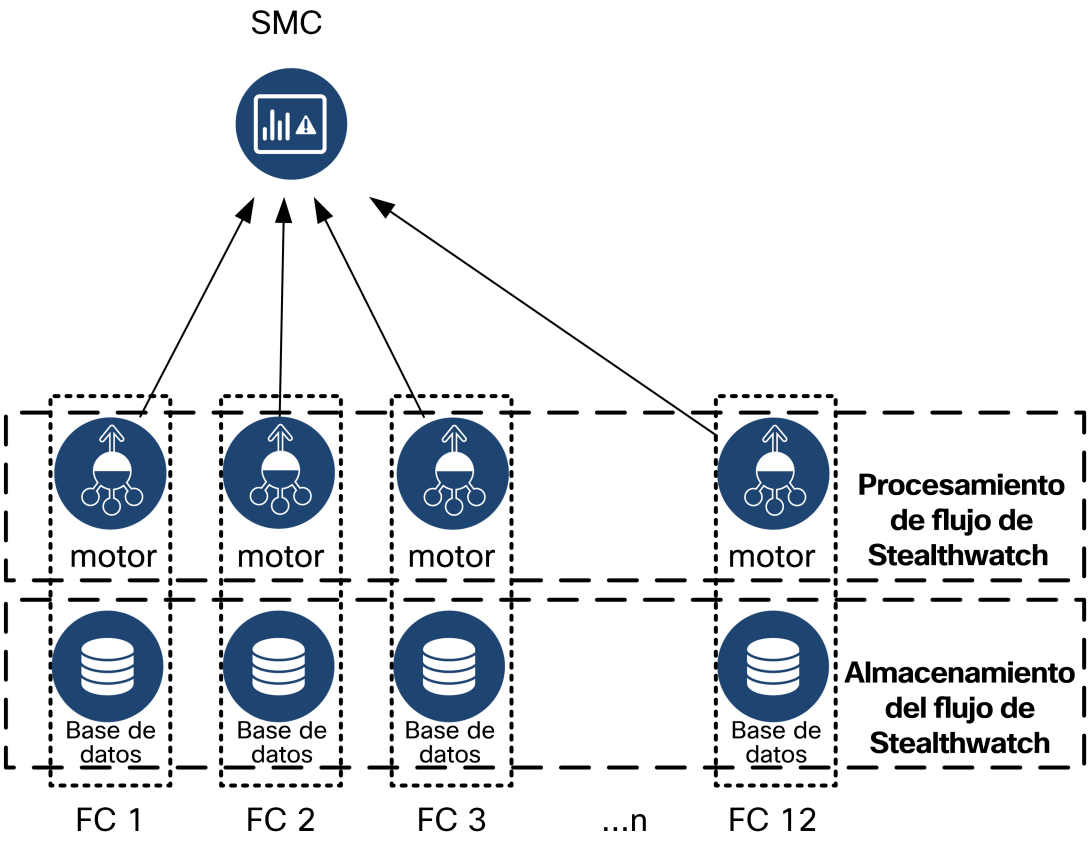
seguridad de los datos en ese Nodo de datos. Consulte el siguiente diagrama para ver un ejemplo de cómo los nodos de datos almacenan la telemetría:



Arquitectura de implementación del Almacén de Datos de Stealthwatch

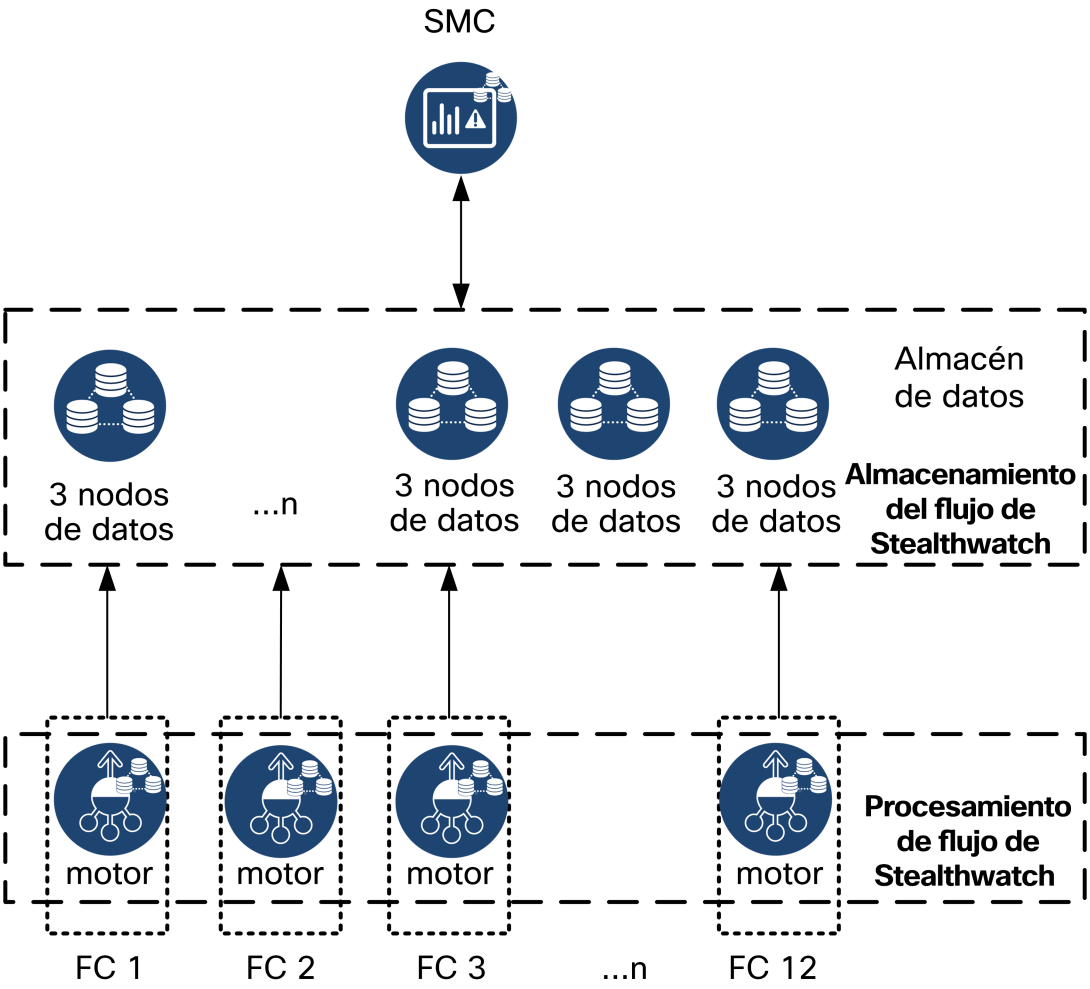
En una implementación de Stealthwatch tradicional sin un Almacén de datos, uno o más recopiladores de flujo ingieren y deduplican datos, realizan análisis y notifican datos y resultados directamente al SMC. Para resolver las consultas enviadas por el usuario, incluidos los gráficos y las tablas, SMC consulta todos los recopiladores de flujos gestionados. Cada Flow Collector devuelve resultados coincidentes al SMC. El SMC recopila la información de los diferentes conjuntos de resultados y, a continuación, genera un gráfico o un gráfico que muestra los resultados. En esta implementación, cada Flow Collector almacena datos en una base de datos local. Consulte el siguiente diagrama para ver un ejemplo.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.



En una implementación de Stealthwatch con una Almacén de datos, el clúster de Almacén de datos se sitúa entre la SMC y los recopiladores de flujo. Uno o más recopiladores de flujo procesa y deduplica los flujos, realiza análisis e informa de los datos y resultados directamente al Almacén de datos, distribuyéndolos aproximadamente por igual a todos los Nodo de datos. El Almacén de datos facilita el almacenamiento de datos, mantiene todo su tráfico en dicha ubicación centralizada en lugar de repartirlo entre varios recopiladores de flujo y ofrece una mayor capacidad de almacenamiento que varios recopiladores de flujo. Vea el siguiente diagrama de ejemplo.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.



Para resolver consultas enviadas por el usuario, incluidos gráficos y tablas, SMC consulta el Almacén de datos. El Almacén de datos encuentra resultados coincidentes en las columnas relevantes para la consulta, luego recupera las filas coincidentes y devuelve los resultados de la consulta al SMC. SMC genera el gráfico o la tabla sin necesidad de recopilar varios conjuntos de resultados de varios recopiladores de flujo. Esto reduce el coste de las consultas, en comparación con las consultas de varios recopiladores de flujo, y mejora el rendimiento de las consultas.

Debido a la arquitectura del Almacén de datos, el SMC y todos los recopiladores de flujo deben comunicarse con el Almacén de datos y deben configurarse durante la implementación para funcionar con el Almacén de datos. No puede tener un entorno "combinado" en el que algunos recopiladores de flujos notifiquen directamente a SMC y otros recopilen informes al Almacén de datos.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Arquitectura del almacén de datos Stealthwatch

Cada Almacén de datos se compone de 3 o más Nodos de datos. Cada Nodo de datos es su propio chasis de hardware. Cuando compra un Almacén de datos, recibe varios chasis de hardware de Nodo de datos, correspondientes a la cantidad de nodos indicados por ese modelo de Almacén de datos. Por ejemplo, un Almacén de datos DS 6200 proporciona 3 chasis de hardware de Nodo de datos.

Puede comprar más de un Almacén de datos para su implementación. Los Nodo de datos se pueden agrupar como parte de su Almacén de datos en múltiplos de 3, desde un mínimo de 3 hasta un máximo de 36.

> Cisco recomienda que configure sus Nodos de datos para que los Nodos de datos de números adyacentes se alimenten con fuentes de alimentación redundantes e independientes. Esta configuración mejora la redundancia de datos y el tiempo de actividad general del Almacén de datos. Consulte Requisitos y consideraciones sobre la implementación del almacén de datos para obtener más información.

Para implementar un Almacén de datos, debe asignar lo siguiente para cada Nodo de datos:

- una dirección IP enrutable para la administración, ingesta y comunicación de consultas con sus dispositivos Stealthwatch
- una dirección IP no enrutable (bloque CIDR `169.254.42.0/24`) en una LAN o VLAN aislada para las comunicaciones entre los Nodos de datos como parte del clúster del Almacén de datos
- dos conexiones 10G, una para las comunicaciones de gestión, ingesta y consulta, una para las comunicaciones entre Nodos de datos
- opcionalmente, para la redundancia de red y la importancia de las comunicaciones entre Nodos de datos, una conexión 10G adicional y un switch adicional para establecer un canal de puerto en el Nodo de datos

Consulte Requisitos y recomendaciones de la implementación del almacén de datos para obtener información más detallada sobre la implementación y los requisitos previos de la misma.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Requisitos previos y recomendaciones de la implementación del almacén de datos

A continuación se describe la información sobre los requisitos previos y las recomendaciones para la implementación de Almacén de datos.

> Si tiene previsto comprar un Stealthwatch Almacén de datos, póngase en contacto con los servicios profesionales de Cisco para obtener ayuda con la ubicación, la implementación y la configuración dentro y como parte de su implementación general de Stealthwatch.

Stealthwatch Compatibilidad de las versiones

Al implementar un Almacén de datos, todos los appliances de Stealthwatch deben estar en la misma versión (versión 7.3+).

Stealthwatch Opciones de licencia

La implementación de Stealthwatch requiere una licencia inteligente de tasa de flujo (FPS); el propio Almacén de datos no requiere una licencia adicional.

Stealthwatch Compatibilidad de hardware y requisitos de red

La siguiente tabla proporciona una descripción general del hardware necesario para implementar un Almacén de datos.

Componente de hardware	**Capacidad admitida**
Almacén de datos	• Mínimo de 3 nodos de datos (DS 6200) • Conjuntos adicionales de 3 Nodos de datos para ampliar el Almacén de datos, máximo de 36 Nodos de datos
Consola de gestión de Stealthwatch	• Mínimo de 1 consola de gestión de Stealthwatch
Recopilador de flujo	• Mínimo de 1 recopilador de flujo

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Tenga en cuenta que debe obtener una licencia inteligente de tasa de flujo (FPS) para la implementación general de Stealthwatch.

> ⚠ No actualice la BIOS del appliance, ya que puede provocar problemas con la funcionalidad del appliance.

Si desea implementar un Almacén de datos, debe tener al menos 3 Nodos de datos. Un Almacén de datos 6200 con 3 Nodos de datos puede gestionar aproximadamente 500 000 flujos por segundo y conservar esos datos durante aproximadamente 90 días. Puede ampliar su Almacén de datos con Nodos de datos adicionales en múltiplos de 3, hasta un máximo de 36 Nodos de datos.

> ⓘ Estas recomendaciones solo tienen en cuenta la telemetría. Su rendimiento puede variar en función de otros factores, como el recuento de hosts, el uso del sensor de flujo, los perfiles de tráfico y otras características de la red. Póngase en contacto con el soporte de Cisco para obtener ayuda con el tamaño.

> ⓘ Actualmente, el Almacén de datos no admite la implementación de Nodos de datos de repuesto como reemplazos automáticos si un Nodo de datos principal deja de funcionar. Póngase en contacto con el soporte de Cisco para obtener asesoramiento.

Debe implementar una SMC con su Almacén de datos y configurarla para su uso con un Almacén de datos. Si desea alta disponibilidad para su SMC, también puede implementar una SMC de conmutación por error.

Además, debe implementar al menos 1 recopilador de flujo con su Almacén de datos y configurar los recopiladores de flujo para su uso con un Almacén de datos.

Por cada SMC y recopilador de flujo que implemente, debe asignar una dirección IP pública enrutable al puerto de gestión `eth0`. Al implementar un Almacén de datos, puede configurar el uso de un puerto de 1 G/10 G de cobre BASE-T o un puerto de 10 G de cable twinaxial SFP+ para el puerto de gestión `eth0` de la SMC y el recopilador de flujo. Cisco requiere un rendimiento de 10 G en el puerto de cobre BASE-T para el uso de Almacén de datos. Los usuarios que no implementan un Almacén de datos solo pueden configurar la interfaz de cobre de 100 Mbps/1 Gbps/10 Gbps como `eth0`.

También puede implementar recopiladores de flujo y UDP Directors para la implementación de Stealthwatch. Dado que estos appliances no se comunican directamente con el Almacén de datos, no es necesario configurarlos para su uso con un Almacén de datos.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Consulte las hojas de especificaciones correspondientes para obtener más información sobre las plataformas compatibles. Consulte la Matriz de compatibilidad de versiones de hardware y software de Stealthwatch para obtener más información sobre la compatibilidad de versiones.

Stealthwatch Consideraciones sobre la implementación empresarial

Tenga en cuenta lo siguiente:

- Si configura un recopilador de flujo para que sea compatible con el almacén de datos, la interfaz de administración de appliances (administrador de appliances) oculta determinadas funciones. Utilice la administración central para realizar la configuración del recopilador de flujo y otras tareas relacionadas. Si desea supervisar las estadísticas de almacenamiento, descargue la aplicación Creador de informes en su SMC.
- Utilice la aplicación web de Stealthwatch para supervisar y configurar su instalación de Stealthwatch si implementa un almacén de datos. El cliente de escritorio de Stealthwatch no es compatible con un almacén de datos.
- Si configura su SMC para utilizarla con un Almacén de datos, no puede utilizar las aplicaciones Auditoría criptográfica de ETA o Clasificador de host.

Almacén de datos Credenciales necesarias para la implementación

Prepare las contraseñas para las siguientes cuentas de usuario:

- `root` y `sysadmin` para cada SMC, Nodo de datos y recopilador de flujo. Se asignan durante la configuración inicial del sistema.
- `admin` para cada SMC, Nodo de datos y recopilador de flujo. Se asignan mediante la herramienta de configuración de appliances.
- `dbadmin` y `readonlyuser` para el almacén de datos. Se asignan al inicializar el Almacén de datos.

Consideraciones de red y switching del almacén de datos

La tabla siguiente proporciona una descripción general de las consideraciones de red y switching al implementar un Almacén de datos.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Consideraciones sobre la red	Descripción
Credenciales necesarias	Para cada Nodo de datos, consola de gestión de Stealthwatch y recopilador de flujo: • Configurado durante la configuración del sistema inicial: `root`, `sysadmin` • Configurado con la herramienta de configuración de appliances: `admin` • Configurado durante la inicialización de Almacén de datos: `dbadmin`, `readonlyuser`
Comunicaciones entre Nodo de datos	• Establezca una latencia de tiempo de ida y vuelta (RTT) recomendada inferior a 200 microsegundos entre Nodos de datos. • Mantenga una diferencia del reloj de 1 segundo o menos entre sus Nodos de datos. • Establezca un rendimiento recomendado de 6,4 Gbps o mayor (conexión conmutada de dúplex completo a 10 Gbps) entre sus Nodos de datos.
Nodo de datos Alimentación de hardware	• Si el hardware Nodo de datos pierde la alimentación inesperadamente, los datos pueden dañarse. Utilice ambas fuentes de alimentación en circuitos separados de fuentes de alimentación ininterrumpidas. • Cuando inicialice el clúster de Almacén de datos (consulte Inicialización y configuración del almacén de datos para obtener más información), alterne la configuración de Nodo de datos según las fuentes de alimentación que utiliza cada Nodo de datos. Esto puede optimizar la tolerancia a fallos minimizando el número de Nodos de datos que se caen si se pierde la alimentación.
Nodo de datos Uso de switches	• Los Nodos de datos necesitan sus propias VLAN de capa 2 para permitir la comunicación entre Nodos de datos. Los Nodos de datos del hardware se pueden conectar a un switch 10G compartido o específico.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

	• Cisco recomienda que los Nodos de datos del hardware se conecten a 2 switches para garantizar una conectividad constante durante las interrupciones de alimentación y actualizaciones del switch. Debido a la baja latencia necesaria para la comunicación entre Nodos de datos, Cisco recomienda un par de switches redundantes, en el que los 2 switches estén interconectados y transporten la VLAN de capa 2 a través de ambos switches.
Stealthwatch Comunicaciones de appliances	• Se requiere SSH y acceso raíz SSH para SMC, nodos de datos y recopiladores de flujo y que se configuren desde el SMC • El SMC y los recopiladores de flujo deben poder alcanzar todos los Nodos de datos • Nodo de datos debe poder alcanzar el SMC, todos los recopiladores de flujo y cada Nodo de datos

Debe asignar las siguientes direcciones IP a cada una Nodo de datos:

- una dirección IP enrutable para la comunicación con sus appliances de Stealthwatch (`eth0`). Conecte el puerto Nodo de datos `eth0` a su red para permitir la comunicación con la SMC y los recopiladores de flujo. Puede configurar el uso de un puerto de 1 G/10 G de cobre BASE-T o un puerto de 10 G de cable twinaxial SFP+ para el puerto de gestión Nodo de datos `eth0`.

  Durante la implementación y la configuración del Almacén de datos, asigne las direcciones IP de Nodo de datos `eth0` al nombre de Almacén de datos para permitir una distribución más uniforme del almacenamiento de telemetría y la solicitud y respuesta de consultas. Consulte Inicialización y configuración de la base de datos del almacén de datos para obtener más información.

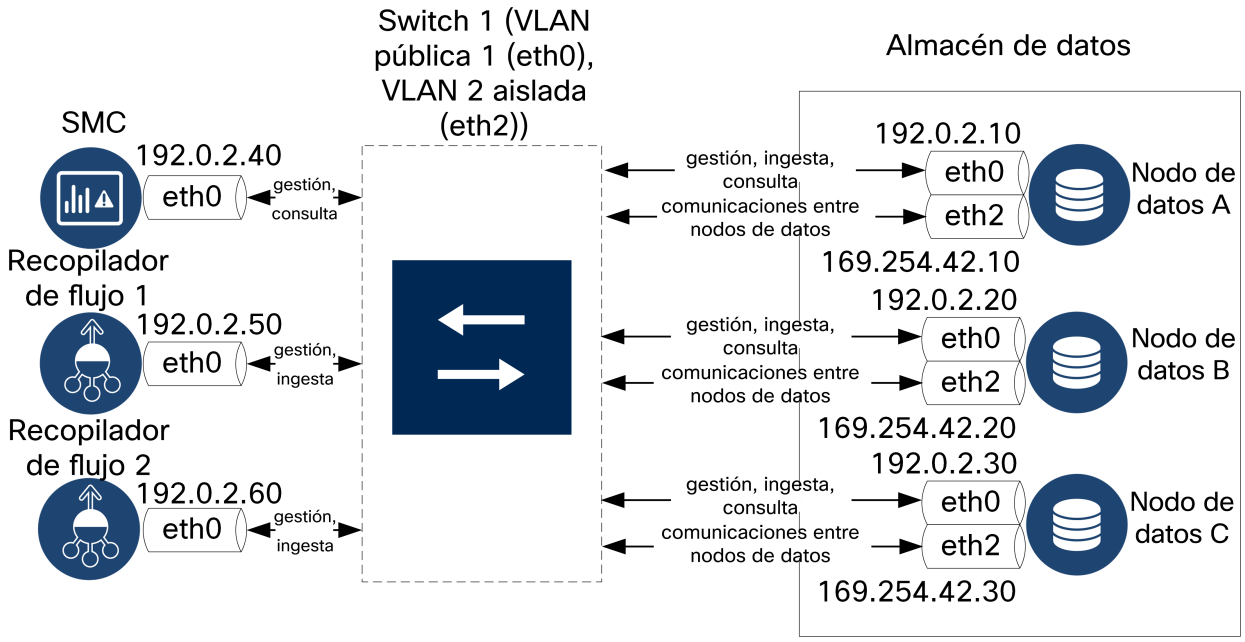
- una dirección IP no enrutable dentro de una LAN o VLAN privada, que se utilizará para la intercomunicación entre Nodo de datos (`eth2` o canal de puerto que contenga `eth2` y `eth3` para mejorar el rendimiento). Como parte del Almacén de datos, sus Nodo de datos se comunican entre sí. Conecte el puerto Nodo de datos `eth2` o el canal de puerto que contenga `eth2` y `eth3` a los switches para la comunicación entre los Nodo de datos.

  > Debe asignar las direcciones IP no enrutables del puerto `eth2` o el canal de puerto `eth2/eth3` desde el bloque CIDR `169.254.42.0/24`.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

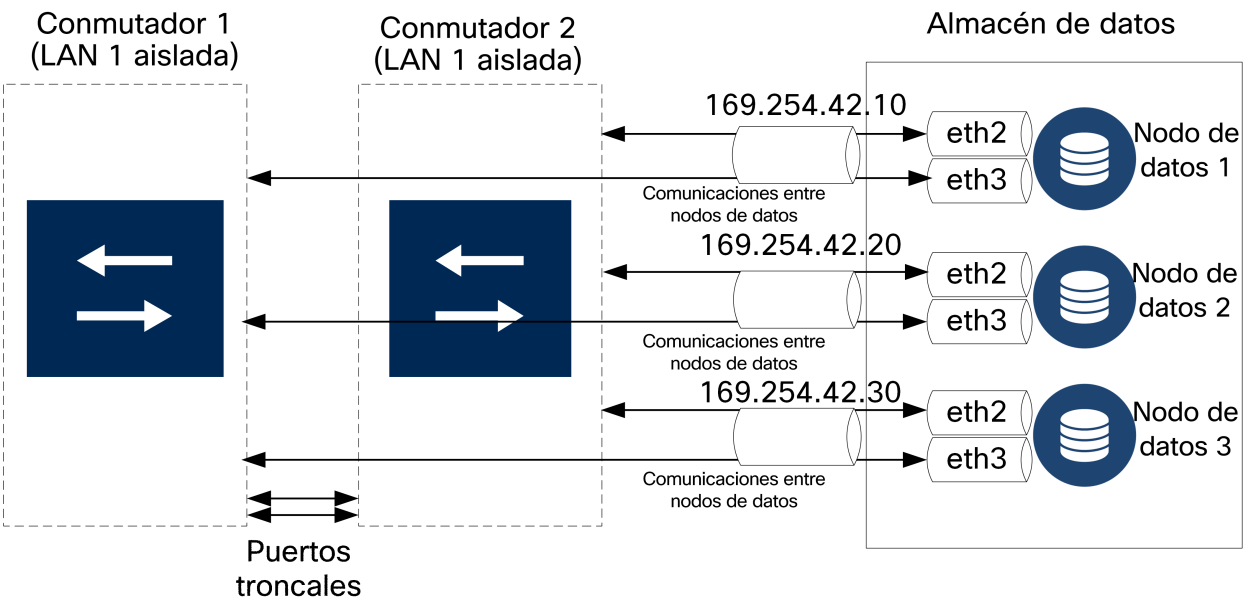
Configurar un puerto `eth2` para un rendimiento de 10 G es suficiente para una comunicación normal entre los Nodo de datos. La creación de un canal de puerto `eth2/eth3` para un rendimiento de hasta 20 G permite una comunicación más rápida entre los Nodo de datos y una adición o sustitución más rápida de los Nodo de datos en el Almacén de datos, ya que cada nuevo Nodo de datos recibe tráfico de los Nodo de datos adyacentes para rellenar sus datos.

Para activar las comunicaciones entre Nodo de datos a través de `eth2` o el canal de puerto `eth2/eth3`, debe implementar 1 switch que admita velocidades de 10G. Configure una LAN o VLAN pública para las comunicaciones de Nodo de datos `eth0` con la SMC y los recopiladores de flujo, así como una LAN o VLAN aislada para las comunicaciones entre Nodo de datos. Puede compartir estos switches con otros appliances, pero cree LAN o VLAN independientes para el tráfico adicional del appliance. Vea el siguiente diagrama de ejemplo:



El clúster de Almacén de datos requiere un latido continuo entre los nodos dentro de la VLAN aislada. Sin este latido, los Nodos de datos podrían desconectarse, lo que aumenta el riesgo de que el Almacén de datos se desconecte. Si desea redundancia de red adicional, para planificar las actualizaciones del switch y la interrupción de alimentación planificada, Cisco recomienda que configure sus Nodos de datos con canales de puerto para una comunicación específica entre Nodos de datos. Conecte cada Nodo de datos a 2 switches, con cada puerto físico conectado a un switch diferente. Vea el siguiente diagrama de ejemplo:

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.



Póngase en contacto con los servicios profesionales de Cisco para obtener ayuda con la planificación de su implementación.

Almacén de datos Requisitos y consideraciones de la implementación

Coloque cada Nodo de datos de manera que se pueda comunicar con todos sus recopiladores de flujo, su SMC y el resto de los Nodos de datos. Para obtener el mejor rendimiento, coloque sus Nodos de datos y sus recopiladores de flujo para minimizar la latencia de comunicación, y sus Nodo de datos y su SMC para un rendimiento óptimo de las consultas. Cisco recomienda encarecidamente colocar los Nodos de datos en el firewall, como en un NOC. Tenga en cuenta lo siguiente para el rendimiento:

- Establezca una latencia de tiempo de ida y vuelta (RTT) recomendada inferior a 200 microsegundos entre los Nodos de datos al implementarlos.
- Mantenga la diferencia del reloj en 1 segundo o menos entre sus Nodos de datos.
- Establezca un rendimiento recomendado de 6,4 Gbps o mayor (conexión conmutada de dúplex completo de 10 Gbps) entre sus Nodos de datos.

Si el Almacén de datos deja de funcionar debido a una pérdida de alimentación o a un fallo de hardware, corre un mayor riesgo de daño y pérdida de los datos. Cisco recomienda instalar los Nodos de datos teniendo en cuenta el tiempo de actividad constante. Tenga en cuenta lo siguiente:

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

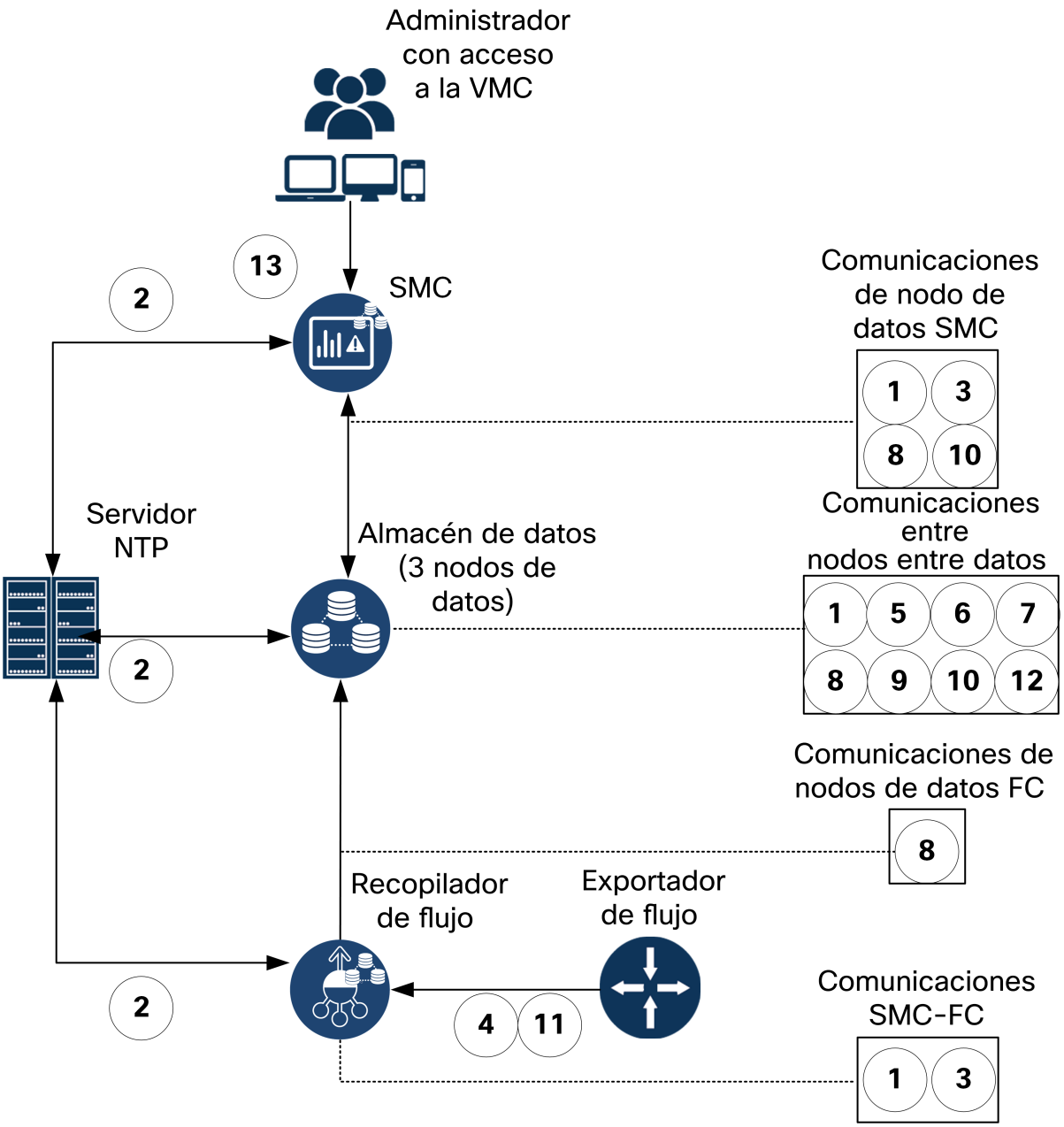
- Cisco recomienda encarecidamente instalar fuentes de alimentación redundantes o ininterrumpidas para cada Nodo de datos para ayudar a evitar la pérdida o el daño de los datos en caso de un apagón.
- Compruebe que la política de restauración de energía del Nodo de datos esté establecida en **Restaurar último estado**, que reinicia el Nodo de datos automáticamente tras la pérdida de energía e intenta restaurar los procesos en ejecución. Consulte la Guía de configuración de la GUI del UCS Serie C para obtener más información sobre la configuración de la política de restauración de energía en CIMC.
- Cuando inicialice el Almacén de datos (consulte Configuración e inicialización de la base de datos del almacén de datos para obtener más información), alterne la configuración del Nodo de datos en función de la fuente de alimentación. El Almacén de datos crea una copia de seguridad de un Nodo de datos en el siguiente Nodo de datos secuencial durante la configuración y la copia de seguridad del último Nodo de datos configurado en el primer Nodo de datos configurado. Si implementa sus Nodos de datos en dos fuentes de alimentación independientes y alterna Nodos de datos pares e impares en función de la fuente de alimentación, si una de las fuentes de alimentación deja de funcionar y tiene un número par de nodos, el Almacén de datos aún puede permanecer activo debido a que los datos o la copia de seguridad de cada Nodo de datos son accesibles desde los Nodos de datos con alimentación.

  Si un Nodo de datos pierde energía inesperadamente y reinicia el appliance, la instancia de base de datos de ese Nodo de datos no se reiniciará automáticamente. Consulte Resolución de problemas del almacén de datos para obtener información sobre el reinicio manual de la instancia de base de datos.

Almacén de datos Puertos de comunicación

El siguiente diagrama muestra un ejemplo de arquitectura de Stealthwatch con los puertos de comunicación que deben abrirse. Consulte la tabla de los puertos asociados con cada llamada.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.



A continuación se enumeran los puertos de comunicación que deben abrirse en el firewall para implementar el Almacén de datos. Consulte la Guía de configuración del sistema Stealthwatch para ver qué puertos de comunicación adicionales deben abrirse para la implementación general de Stealthwatch.

N.º	De (cliente)	A (servidor)	Puerto	Protocolo o propósito
1	SMC	Recopiladores	22/TCP	Se necesita SSH para

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

		de flujo y Nodo de datos		inicializar la base de datos Almacén de datos
1	Nodo de datoss	Todos los demás Nodo de datos	22/TCP	Se necesita SSH para inicializar la base de datos Almacén de datos y para las tareas de administración de la base de datos
2	SMC, colectores de flujo y Nodo de datos	Servidor NTP	123/UDP	Se necesita NTP para la sincronización horaria
2	Servidor NTP	SMC, colectores de flujo y Nodo de datos	123/UDP	Se necesita NTP para la sincronización horaria
3	SMC	Recopiladores de flujo y Nodo de datos	443/TCP	Se necesita HTTPS para una comunicación segura entre los dispositivos
3	Recopiladores de flujo	SMC	443/TCP	Se necesita HTTPS para una comunicación segura entre los dispositivos
3	Nodo de datoss	SMC	443/TCP	Se necesita HTTPS para una comunicación segura entre los dispositivos
4	Exportadores de NetFlow	Recopiladores de flujo: NetFlow	2055/UDP	Ingestión de NetFlow
5	Nodo de datoss	Todos los demás Nodo de datos	4803/TCP	Servicio de mensajería interna Nodo de datos

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

6	Nodo de datoss	Todos los demás Nodo de datos	4803/UDP	Servicio de mensajería interna Nodo de datos
7	Nodo de datoss	Todos los demás Nodo de datos	4804/UDP	Servicio de mensajería interna Nodo de datos
8	SMC, colectores de flujo y Nodo de datos	Nodo de datoss	5433/TCP	Conexiones de cliente de Vertica
9	Nodo de datos	Todos los demás Nodo de datos	5433/UDP	Supervisión del servicio de mensajería de Vertica
10	SMC	Nodo de datoss	5444/TCP	Comunicaciones seguras de la consola de administración de Vertica
10	Nodo de datoss	SMC y todos los demás Nodo de datos	5444/TCP	Comunicaciones seguras de la consola de administración de Vertica
11	Exportadores de sFlow	Recopiladores de flujo: sFlow	6343/UDP	Ingestión de sFlow
12	Nodo de datoss	Todos los demás Nodo de datos	6543/UDP	Servicio de mensajería interna Nodo de datos
13	Estaciones de trabajo de administrador para acceder a la consola de administración de Vertica	SMC	9450/TCP	Acceso al navegador web de la consola de administración de Vertica

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Stealthwatch Descripción general de la implementación del almacén de datos

> ⚠ Si tiene previsto comprar un Stealthwatch Almacén de datos, póngase en contacto con los servicios profesionales de Cisco para obtener ayuda con la ubicación, la implementación y la configuración dentro y como parte de su implementación general de Stealthwatch. **No** instale un almacén de datos por su cuenta.

A continuación, se describen los pasos generales para la implementación de Almacén de datos con una implementación de Stealthwatch:

- Implemente sus appliances de Stealthwatch, incluidos sus Nodos de datos, y configure su SMC y sus recopiladores de flujo para utilizarlos con un Almacén de datos

  > ⓘ Asegúrese de instalar la última versión y el parche de actualización de los appliances después de implementarlos, pero antes de continuar con la inicialización y configuración de Almacén de datos.

- Prepare la implementación de Stealthwatch para utilizar el Almacén de datos mediante la distribución de contraseñas de usuario y certificados de identidad
- Inicialice el Almacén de datos
- Configure la consola de administración de Vertica (VMC) en su SMC y active las notificaciones y los umbrales de alerta
- Configure los ajustes de conservación de Almacén de datos a través de la API REST
- Instale las aplicaciones de Stealthwatch en su SMC para obtener funciones adicionales relacionadas con Almacén de datos

Revise estas tareas antes de iniciar la implementación.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Componente y tarea necesarios	Pasos
Instalación y configuración de la SMC	Consulte Configuración de la SMC para su uso con un almacén de datos para obtener más información. 1. Implemente la SMC en su red. 2. Con el CIMC o conectándose directamente al appliance, inicie sesión en la consola de SMC como `root`. Ejecute el script de configuración del sistema `systemconfig` y utilice el asistente de primera configuración para configurar la información de administración básica, incluida la dirección IP del appliance, el uso con un Almacén de datos y la configuración del puerto físico `eth0`. 3. Desde un navegador web, vaya a la dirección IP `eth0` de la SMC para acceder a la herramienta de configuración de appliances. Utilice la herramienta de configuración de appliances para configurar las contraseñas de administrador, el dominio de Stealthwatch y los servidores DNS y NTP, y para instalar la administración central. 4. Desde un navegador web, vaya a la dirección IP de la SMC después de configurar el appliance mediante la herramienta de configuración de appliances para acceder a la aplicación web de Stealthwatch. En Administración central, active el acceso SSH y el acceso raíz SSH a la SMC. 5. Actualice su SMC a la última versión y parche. Consulte las guías de actualización para obtener más información sobre la actualización a la versión actual y los readme de parches para obtener más información sobre las actualizaciones de parches.
Nodo de datos instalación y configuración	Consulte Implementación inicial y configuración del hardware del almacén de datos para obtener más información. 1. Implemente sus Nodos de datos en su red. 2. Con el CIMC o conectándose directamente al appliance, inicie sesión en la consola de cada Nodo de datos como `root`.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

	Ejecute el script de configuración del sistema `systemconfig` y utilice el asistente de primera configuración para configurar la información de administración básica, incluida la dirección IP de administración del appliance y la dirección IP no enrutable de comunicación entre Nodos de datos (con configuración de canal de puerto opcional). Asigne una dirección IP no enrutable a `eth2` o al canal de puerto `eth2/eth3` desde el bloque CIDR `169.254.42.0/24`. 3. En cada Nodo de datos, desde un navegador web, vaya a la dirección IP enrutable `eth0` de Nodo de datos para acceder a la herramienta de configuración de appliances. Utilice la herramienta de configuración de appliances de cada Nodo de datos para configurar las contraseñas de administrador, el dominio de Stealthwatch y los servidores DNS y NTP, y para que la administración central administre el Nodo de datos. 4. Desde la aplicación web de Stealthwatch, vaya a Administración central y active el acceso SSH y el acceso raíz SSH a cada Nodo de datos. 5. Actualice sus Nodos de datos a la última versión y parche. Consulte las guías de actualización para obtener más información sobre la actualización a la versión actual y los readme de parches para obtener más información sobre las actualizaciones de parches. **i** Revise las guías de actualización correspondientes y la documentación de los readme de parches antes de continuar. El proceso de actualización de Nodo de datos requiere pasos adicionales en comparación con otros appliances de Stealthwatch.
Instalación y configuración del recopilador de flujo	Consulte Configuración del recopilador de flujo para su uso con un almacén de datos para obtener más información. 1. Implemente sus recopiladores de flujo en su red. 2. Con el CIMC o conectándose directamente al appliance, inicie sesión en la consola de cada recopilador de flujo como `root`. Ejecute el script de configuración del sistema `systemconfig`

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

	y utilice el asistente de primera configuración para configurar la información de administración básica, incluida la dirección IP del appliance, el uso con un Almacén de datos y la configuración del puerto físico eth0. 3. En cada recopilador de flujo, desde un navegador web, vaya a la dirección IP `eth0` del recopilador de flujo para acceder a la herramienta de configuración de appliances. Utilice la herramienta de configuración de appliances de cada recopilador de flujo para configurar las contraseñas de administrador, el dominio de Stealthwatch, los servidores DNS y NTP y el número de puerto de recopilación de flujos (`2055` para NetFlow o `6343` para sFlow), y para que la administración central administre el recopilador de flujo. 4. Desde la aplicación web de Stealthwatch, vaya a Administración central y active el acceso SSH y el acceso raíz SSH a cada recopilador de flujo. 5. Actualice sus Recopilador de flujo a la última versión y parche. Consulte las guías de actualización para obtener más información sobre la actualización a la versión actual y los readme de parches para obtener más información sobre las actualizaciones de parches.
Almacén de datos inicialización y configuración	Consulte Inicialización y configuración de la base de datos del almacén de datos para obtener más información. 1. Desde la aplicación web de Stealthwatch, vaya a Administración central y asegúrese de que todos los recopiladores de flujo y Nodo de datos se administren en Administración central, de que la conexión esté activa y de que tanto el acceso SSH como el acceso raíz SSH estén activados. 2. Inicie sesión en la consola de SMC principal como `sysadmin`. Mediante el script de conectividad segura de la base de datos `setup-sw-datastore-secure-connectivity`, distribuya las contraseñas `dbadmin` y `readonlyuser` de la base de datos y los certificados de identidad a su SMC, Nodo de datos y recopiladores de flujo.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

	3. En función de los resultados del script de conectividad segura `setup-sw-datastore-secure-connectivity`, inicie sesión en la consola de Nodo de datos especificada como `root`. Copie el archivo de configuración de inicialización de la base de datos de ejemplo `install_SDBN_example.cfg` como `install_SDBN.cfg` y actualícelo con sus direcciones IP y su subred de Nodo de datos. Ejecute el script de inicialización, haciendo referencia al archivo de configuración de inicialización (`python install_SDBN_initial.py -i install_SDBN.cfg`). 4. Desde el Nodo de datos donde ejecutó el script de inicialización, recupere la cadena de clave API de `/opt/vertica/config/apikey.dat`. Utilizará esta clave API para establecer una conexión entre la base de datos de Almacén de datos y la VMC en un paso posterior. 5. Desde la aplicación web de Stealthwatch, vaya a Administración central y, en la SMC y todos los recopiladores de flujo, utilice la resolución local para asignar el nombre de la base de datos de Almacén de datos (`sw-datastore`) a cada dirección IP enrutable de Nodo de datos. Para un rendimiento óptimo, asigne las direcciones IP de Nodo de datos `eth0` en el mismo orden para cada appliance.
Instalación y configuración de la consola de administración de Vertica (VMC) en la SMC	Consulte Configuración de la consola de administración de Vertica para obtener más información. 1. Copie el certificado de servidor `/lancope/var/admin/cds/ server.crt` de su SMC en su estación de trabajo local. 2. Desde un navegador web de su estación de trabajo local, vaya a `[smc-ipv4-address]:9450/webui/login` para acceder a la VMC. Realice el aprovisionamiento y la configuración inicial de la VMC. Desactive las conexiones que utilicen versiones menos seguras de TLS. Utilice la cadena de clave API y el archivo de certificado `server.crt` para establecer una conexión con el Almacén de datos. Configure umbrales de alerta y notificaciones de alerta para recibir alertas de estado de Almacén de datos.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Almacén de datos conservación de datos	Consulte Configuración de conservación del almacén de datos para obtener más información. • Utilice la API REST para configurar el período de conservación de Almacén de datos.
Revise los siguientes pasos tras completar la implementación de Almacén de datos	Revise los pasos siguientes para la instalación del almacén de datos: 1. Instale la aplicación Creador de informes de Stealthwatch en su SMC para ejecutar informes en su implementación de Stealthwatch y ver las estadísticas de almacenamiento de Almacén de datos. Consulte las notas de versión para obtener más información. 2. Revise la ayuda en línea de la aplicación web de Stealthwatch para obtener más información sobre cómo utilizar Stealthwatch.

De forma opcional, también puede hacer lo siguiente:

Componente y tarea opcionales	**Pasos**
Instalación y configuración de UDP Director	• Implemente UDP Director como se describe en la Guía de instalación del hardware de la serie x2xx de Stealthwatch y la Guía de configuración del sistema Stealthwatch. Actualice su UDP Director a la última versión y parche. Consulte las guías de actualización para obtener más información sobre la actualización a la versión actual y los readme de parches para obtener más información sobre las actualizaciones de parches.
Sensor de flujo	• Implemente el sensor de flujo como se describe en la Guía de instalación del hardware de la serie x2xx de Stealthwatch y la Guía de configuración del sistema Stealthwatch. Actualice su sensor de flujo a la última versión y parche. Consulte las guías de actualización para obtener más información sobre la actualización a la versión actual y los readme de parches para obtener más información sobre las actualizaciones de parches.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Instalación y configuración de la SMC de conmutación por error	• Implemente la SMC de conmutación por error como se describe en la Guía de instalación del hardware de la serie x2xx de Stealthwatch, la Guía de configuración del sistema Stealthwatch y la Guía de configuración de conmutación por error de Stealthwatch. Actualice su SMC a la última versión y parche. Consulte las guías de actualización para obtener más información sobre la actualización a la versión actual y los readme de parches para obtener más información sobre las actualizaciones de parches.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Instalación del hardware del almacén de datos

> Si tiene previsto comprar un Stealthwatch Almacén de datos, póngase en contacto con los servicios profesionales de Cisco para obtener ayuda con la ubicación, la implementación y la configuración dentro y como parte de su implementación general de Stealthwatch.

Stealthwatch Implementación del hardware y consideraciones

Implemente y configure sus appliances de Stealthwatch de la SMC, el Nodo de datos y el recopilador de flujo en función de las siguientes instrucciones e instale switches para el Almacén de datos en su red. Al implementar sus Nodos de datos y conectarlos a su red, revise Requisitos y consideraciones sobre la implementación del almacén de datos. Asegúrese de que sus SMC, Nodo de datos y recopiladores de flujo tengan la misma versión (más de 7.3). Consulte la Guía de instalación del hardware de la serie x210 de Stealthwatch o el **Apéndice A. Preparación para la instalación** y el **Apéndice B. Instalación del hardware de Stealthwatch** para obtener más información sobre la instalación y configuración inicial del appliance.

> Si desea implementar un almacén de datos en su red como parte de una implementación existente de Stealthwatch, colabore con los servicios profesionales de Cisco para integrar el almacén de datos. Póngase en contacto con el soporte de Cisco para obtener más información.

> Utilice la aplicación web de Stealthwatch para supervisar y configurar su instalación de Stealthwatch si implementa un almacén de datos. El cliente de escritorio de Stealthwatch no es compatible con un almacén de datos.

Configuración de la SMC para su uso con un almacén de datos

Implemente y configure su SMC para su uso con un Almacén de datos y para administrar sus Nodos de datos y recopiladores de flujo.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

> Si tiene una SMC secundaria, configúrela primero para que la SMC principal pueda comunicarse con ella. Consulte la Guía de configuración del sistema Stealthwatch para obtener más información sobre el establecimiento de un par de conmutación por error de la SMC. Consulte **Implementación de la consola de administración de Stealthwatch de conmutación por error** para obtener más contexto sobre la implementación y la configuración de una SMC secundaria para que funcione con un Almacén de datos.

Realice lo siguiente:

1. Primero, implemente la SMC en su red. A continuación, conéctese a su appliance con CIMC, un teclado y un monitor o un ordenador portátil e inicie sesión en la consola como `root`. Ejecute `systemconfig` y utilice el asistente de primera configuración para actualizar la configuración del puerto de administración y utilizarlo con un Almacén de datos y las contraseñas de usuario `root` y `sysadmin`. Consulte la Guía de instalación del hardware de la serie x210 de Stealthwatch o el **Apéndice A. Preparación para la instalación** y el **Apéndice B. Instalación del hardware de Stealthwatch** para obtener más información.

   > Solo la primera vez que acceda a la configuración del sistema, el sistema le llevará al asistente de primera configuración, que le guiará automáticamente a través del proceso de configuración inicial del appliance.

   > Después de elegir configurar SMC o Recopilador de flujo para usarlo con un Almacén de datos, no puede actualizar la configuración del appliance para cambiar esto. Debe seleccionar el appliance con RFD si selecciona una opción incorrecta. Active esta opción solo si tiene previsto implementar un Almacén de datos en la red.

2. A continuación, en un navegador web, vaya a la dirección IP que asignó al puerto de administración. Utilice la herramienta de configuración de appliances para realizar una configuración adicional, incluida la asignación de la contraseña de usuario `admin` (y las contraseñas de usuario `root` y `sysadmin` si no las asignó durante la configuración del sistema), la configuración del dominio de Stealthwatch, otra configuración de red, la configuración de DNS y NTP y la instalación de la administración central en la SMC. Consulte la Guía de configuración del sistema Stealthwatch o el **Apéndice C. Configuración de los appliances** para obtener más información.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

3. A continuación, active el acceso SSH y el acceso raíz SSH en su SMC. Para inicializar el Almacén de datos, como se describe en **Inicialización y configuración del almacén de datos**, debe ejecutar un script que se base en el acceso SSH a cada appliance.

> ⚠ Cuando SSH está activado, aumenta el riesgo de compromiso del sistema. Es importante activar SSH solo cuando sea necesario. Cuando haya terminado de utilizar SSH, desactívelo.

Actualice el permiso de acceso SSH de la SMC:

Antes de comenzar

- Inicie sesión en la aplicación web de la SMC como administrador del sistema.

Procedimiento

1. Acceda al panel del administrador de appliances. Tiene las siguientes opciones:
   - La herramienta de configuración de appliances se abre en el panel del administrador de appliances si ha completado la configuración del appliance.
   - Haga clic en el icono **Configuración global**. Seleccione **Administración central**. Aparecerá el panel del administrador de appliances.
2. Para la entrada del elemento de línea de la SMC, haga clic en el menú Acciones y, a continuación, seleccione **Editar configuración del appliance**.
3. Seleccione la pestaña Appliance.
4. En el panel SSH, seleccione **Activar SSH**.
5. Seleccione **Activar acceso raíz SSH**.
6. Haga clic en **Aplicar configuración**.

Siguientes pasos

- Actualice su SMC a la última versión y parche, como se describe en el siguiente paso.

1. Por último, actualice su SMC a la última versión y parche. Consulte las guías de actualización para obtener más información sobre la actualización a la versión actual y los readme de parches para obtener más información sobre las actualizaciones de parches.

   Después de actualizar su SMC, tiene las siguientes opciones:

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

- Vuelva a Stealthwatch Descripción general de la implementación del almacén de datos para revisar el proceso de implementación.
- Implemente y configure sus Nodos de datos como se describe en la siguiente sección.

Almacén de datos Implementación inicial y configuración del hardware

Después de implementar su SMC, implemente y configure sus appliances de Nodo de datos. Al implementar sus Nodos de datos y conectarlos a su red, revise Requisitos y consideraciones sobre la implementación del almacén de datos.

En cada Nodo de datos, realice lo siguiente:

1. En primer lugar, implemente el Nodo de datos en la red. A continuación, conéctese al appliance de Nodo de datos con CIMC, un teclado y un monitor o un ordenador portátil e inicie sesión en la consola como `root`. Ejecute `systemconfig` y utilice el asistente de primera configuración para actualizar la configuración del puerto de administración, la configuración del puerto de comunicación entre Nodo de datos y las contraseñas de usuario `root` y `sysadmin`. Consulte la Guía de instalación del hardware de la serie x210 de Stealthwatch o el **Apéndice A. Preparación para la instalación** y el **Apéndice B. Instalación del hardware de Stealthwatch** para obtener más información.

   > Solo la primera vez que acceda a la configuración del sistema, el sistema le llevará al asistente de primera configuración, que le guiará automáticamente a través del proceso de configuración inicial del appliance.

2. A continuación, en un navegador web, vaya a la dirección IP que asignó al puerto de administración. Utilice la herramienta de configuración de appliances para realizar una configuración adicional, incluida la asignación de la contraseña de usuario `admin` (y las contraseñas de usuario `root` y `sysadmin` si no las asignó durante la configuración del sistema), la configuración del dominio de Stealthwatch, otra configuración de red, la configuración de DNS y NTP y permitir que el Nodo de datos sea administrable por la administración central. Consulte la Guía de configuración del sistema Stealthwatch o el **Apéndice C. Configuración de los appliances** para obtener más información.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

3. Por último, active el acceso SSH y el acceso raíz SSH en su Nodo de datos. Para inicializar el Almacén de datos, como se describe en **Inicialización y configuración del almacén de datos**, debe ejecutar un script que se base en el acceso SSH a cada appliance.

> ⚠ Cuando SSH está activado, aumenta el riesgo de compromiso del sistema. Es importante activar SSH solo cuando sea necesario. Cuando haya terminado de utilizar SSH, desactívelo.

Actualice el permiso de acceso SSH de un Nodo de datos:

Antes de comenzar

- Inicie sesión en la aplicación web de la SMC como administrador del sistema.

Procedimiento

1. Acceda al panel del administrador de appliances. Tiene las siguientes opciones:
   - La herramienta de configuración de appliances se abre en el panel del administrador de appliances si ha completado la configuración del appliance.
   - Haga clic en el icono **Configuración global**. Seleccione **Administración central**. Aparecerá el panel del administrador de appliances.

   Revise la lista de appliances y confirme que el Nodo de datos aparece en la lista y que el estado del appliance es **Activo**.
2. Para la entrada del elemento de línea de Nodo de datos, haga clic en el menú Acciones y, a continuación, seleccione **Editar configuración del appliance**.
3. Seleccione la pestaña Appliance.
4. En el panel SSH, seleccione **Activar SSH**.
5. Seleccione **Activar acceso raíz SSH**.
6. Haga clic en **Aplicar configuración**.

Siguientes pasos

- Actualice su Nodo de datos a la última versión y parche, como se describe en el siguiente paso.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

1. Por último, actualice su nodo de datos a la última versión y parche. Consulte las guías de actualización para obtener más información sobre la actualización a la versión actual y los readme de parches para obtener más información sobre las actualizaciones de parches.

   > Revise las guías de actualización correspondientes y la documentación de los readme de parches antes de continuar. El proceso de actualización de Nodo de datos requiere pasos adicionales en comparación con otros appliances de Stealthwatch.

   Después de actualizar el Nodo de datos, tiene las siguientes opciones:

   - Vuelva a Stealthwatch Descripción general de la implementación del almacén de datos para revisar el proceso de implementación.
   - Vuelva a **Almacén de datos Implementación inicial y configuración del hardware** y repita este proceso de instalación y configuración inicial de Nodo de datos, configuración de la herramienta de configuración de appliances y configuración de la administración central para el resto de Nodo de datos.

2. Después de implementar y configurar todos sus Nodo de datos, tiene las siguientes opciones:

   - Configure su UDP Director, si tiene uno, como se describe en la siguiente sección.
   - Configure los recopiladores de flujo si no tiene un UDP Director, como se describe en **Configuración del recopilador de flujo para su uso con un almacén de datos**.

Implementación de UDP Director

Si desea implementar un UDP Director, siga las instrucciones de la Guía de instalación del hardware de la serie x210 de Stealthwatch y la Guía de configuración del sistema Stealthwatch. Tenga en cuenta que el proceso de instalación del UDP Director no cambia, tanto si implementa un Almacén de datos como si no. No tiene que configurar un UDP Director para utilizarlo con un Almacén de datos.

Después de implementar su UDP Director, tiene las siguientes opciones.

- Vuelva a Stealthwatch Descripción general de la implementación del almacén de datos para revisar el proceso de implementación.
- Implemente y configure sus recopiladores de flujo como se describe en la siguiente sección.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Configuración del recopilador de flujo para su uso con un almacén de datos

Después de configurar sus Nodo de datos y sus UDP Director, si los ha implementado, implemente y configure los recopiladores de flujo.

En cada recopilador de flujo, realice lo siguiente:

1. En primer lugar, implemente el recopilador de flujo en su red. A continuación, conéctese al recopilador de flujo con CIMC, un teclado y un monitor o un ordenador portátil e inicie sesión en la consola como `root`. Ejecute `systemconfig` y utilice el asistente de primera configuración para actualizar la configuración del puerto de administración y utilizarlo con un Almacén de datos y las contraseñas de usuario `root` y `sysadmin`. Consulte la Guía de instalación del hardware de la serie x210 de Stealthwatch o el **Apéndice A. Preparación para la instalación** y el **Apéndice B. Instalación del hardware de Stealthwatch** para obtener más información.

   > Solo la primera vez que acceda a la configuración del sistema, el sistema le llevará al asistente de primera configuración, que le guiará automáticamente a través del proceso de configuración inicial del appliance.

   > Después de elegir configurar SMC o Recopilador de flujo para usarlo con un Almacén de datos, no puede actualizar la configuración del appliance para cambiar esto. Debe seleccionar el appliance con RFD si selecciona una opción incorrecta. Active esta opción solo si tiene previsto implementar un Almacén de datos en la red.

2. A continuación, en un navegador web, vaya a la dirección IP que asignó al puerto de administración. Utilice la herramienta de configuración de appliances para realizar una configuración adicional, incluida la asignación de la contraseña de usuario `admin` (y las contraseñas de usuario `root` y `sysadmin` si no las asignó durante la configuración del sistema), la selección del dominio de Stealthwatch, otra configuración de red, la configuración de DNS y NTP, el número de puerto de recopilación de flujos (`2055` para NetFlow o `6343` para sFlow), y para permitir que la administración central administre el recopilador de flujo. Consulte la Guía de configuración del sistema Stealthwatch o el **Apéndice C. Configuración de los appliances** para obtener más información.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

> Si configura un recopilador de flujo para su uso con un Almacén de datos, la interfaz de administración de appliances (administrador de appliances) oculta determinadas funciones. Utilice la administración central para realizar la configuración del recopilador de flujo y otras tareas relacionadas. Si desea supervisar las estadísticas de almacenamiento, descargue la aplicación de estadísticas de almacenamiento de Almacén de datos en su SMC.

3. Por último, active el acceso SSH y el acceso raíz SSH en los recopiladores de flujo. Para inicializar el Almacén de datos, como se describe en **Inicialización y configuración del almacén de datos**, debe ejecutar un script que se base en el acceso SSH a cada appliance.

> Cuando SSH está activado, aumenta el riesgo de compromiso del sistema. Es importante activar SSH solo cuando sea necesario. Cuando haya terminado de utilizar SSH, desactívelo.

Actualice el permiso de acceso SSH de un recopilador de flujo:

Antes de comenzar

- Inicie sesión en la aplicación web de la SMC como administrador del sistema si no está utilizando la herramienta de configuración de appliances.

Procedimiento

1. Acceda al panel del administrador de appliances. Tiene las siguientes opciones:
   - La herramienta de configuración de appliances se abre en el panel del administrador de appliances si ha completado la configuración del appliance.
   - Haga clic en el icono **Configuración global**. Seleccione **Administración central**. Aparecerá el panel del administrador de appliances.

   Revise la lista de appliances y confirme que el recopilador de flujo aparece en la lista y que el estado del appliance es **Activo**.
2. Para la entrada del elemento de línea del recopilador de flujo, haga clic en el menú Acciones y, a continuación, seleccione **Editar configuración del appliance**.
3. Seleccione la pestaña Appliance.
4. En el panel SSH, seleccione **Activar SSH**.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

5. Seleccione **Activar acceso raíz SSH**.
6. Haga clic en **Aplicar configuración**.

Siguientes pasos

- Actualice su Recopilador de flujo a la última versión y parche, como se describe en el siguiente paso.

1. Por último, actualice su Recopilador de flujo a la última versión y parche. Consulte las guías de actualización para obtener más información sobre la actualización a la versión actual y los readme de parches para obtener más información sobre las actualizaciones de parches.

   Después de actualizar el Recopilador de flujo, tiene las siguientes opciones:

   - Vuelva a Stealthwatch Descripción general de la implementación del almacén de datos para revisar el proceso de implementación.
   - En cada uno de los recopiladores de flujo, repita el proceso descrito en **Configuración del recopilador de flujo para su uso con un almacén de datos** de instalación y configuración inicial del recopilador de flujo, configuración a través de la herramienta de configuración de appliances y configuración de la administración central para los recopiladores de flujo restantes.
2. Después de implementar y configurar todos sus Recopilador de flujo, tiene las siguientes opciones:
   - Configure su sensor de flujo, si tiene uno, como se describe en la siguiente sección.
   - Configure su SMC secundaria, si tiene una, como se describe en **Implementación de la consola de administración de Stealthwatch de conmutación por error**.
   - Si no tiene un sensor de flujo o una SMC secundaria, inicialice y configure el Almacén de datos, como se describe en **Inicialización y configuración del almacén de datos**.

Implementación del sensor de flujo

Si desea implementar un sensor de flujo, siga las instrucciones de la Guía de instalación del hardware de la serie x210 de Stealthwatch y la Guía de configuración del sistema Stealthwatch. Tenga en cuenta que el proceso de instalación del sensor de flujo es el mismo, tanto si implementa un Almacén de datos como si no. No tiene que configurar un sensor de flujo para utilizarlo con un Almacén de datos.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Después de implementar y configurar el sensor de flujo, tiene las siguientes opciones:

- Vuelva a Stealthwatch Descripción general de la implementación del almacén de datos para revisar el proceso de implementación.
- Configure su SMC secundaria como una SMC de conmutación por error, si tiene una, como se describe en la siguiente sección.
- Si no tiene una SMC secundaria, inicialice el Almacén de datos como se describe en **Inicialización y configuración del almacén de datos**.

Implementación de la consola de administración de Stealthwatch de conmutación por error

Si tiene una SMC secundaria que desea configurar como SMC de conmutación por error, siga las instrucciones de la Guía de instalación del hardware de la serie x210 de Stealthwatch, la Guía de configuración del sistema Stealthwatch y la Guía de configuración de conmutación por error de Stealthwatch.

Cuando termine de configurar la SMC secundaria y la SMC principal se administre a través de la administración central, tiene las siguientes opciones:

- Vuelva a Stealthwatch Descripción general de la implementación del almacén de datos para revisar el proceso de implementación.
- Si tiene una SMC secundaria y convierte su SMC secundaria en la SMC principal, se requiere una configuración adicional antes de volver a utilizar el script `setup-sw-datastore-secure-connectivity`. Consulte Copiar información de confianza del almacén de datos en una SMC de conmutación por error para obtener más información.
- Inicialice y configure el Almacén de datos como se describe en **Inicialización y configuración del almacén de datos**.

Inicialización y configuración del almacén de datos

Después de implementar y configurar su SMC, sus Nodo de datos y sus recopiladores de flujo, inicialice y configure el Almacén de datos. Asegúrese de que todos los SMC, Nodos de datos y Recopiladores de flujo estén actualizados a la última versión y parche antes de continuar.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

> Si tiene una SMC secundaria y convierte su SMC secundaria en la SMC principal, se requiere una configuración adicional antes de volver a utilizar el script `setup-sw-datastore-secure-connectivity`. Consulte Copiar información de confianza del almacén de datos en una SMC de conmutación por error para obtener más información.

Realice lo siguiente:

1. En primer lugar, asegúrese de que todos los Nodo de datos y los recopiladores de flujo, así como la SMC secundaria, si ha implementado una, se administren a través de la administración central y de que todos tengan el SSH y el acceso raíz SSH activados.
2. A continuación, desde la SMC, ejecute un script para distribuir contraseñas Almacén de datos `dbadmin` y `readonlyuser` y certificados de identidad para establecer comunicaciones de Almacén de datos seguras con sus appliances de Stealthwatch.
3. A continuación, en el Nodo de datos especificado durante el paso anterior, ejecute un script para inicializar el Almacén de datos y establecer conexiones seguras entre los Nodo de datos y sus appliances de Stealthwatch.
4. Por último, en Administración central, asigne un nombre de Almacén de datos interno (`sw-datastore`) a las direcciones IP de Nodo de datos en la SMC y en los recopiladores de flujo para mejorar la distribución de la carga y el rendimiento de las consultas de Nodo de datos.

Compruebe que sus Nodo de datos y sus recopiladores de flujo se administren a través de la administración central:

Antes de comenzar

- Haga una lista de todas las direcciones IP y nombres de host de Nodo de datos y de los recopiladores de flujo que prevé administrar en la administración central.
- Inicie sesión en la aplicación web de la SMC como administrador del sistema y vaya a Administración central.

Procedimiento

1. En el inventario de appliances, compare la lista de Nodo de datos y recopiladores de flujo, así como la SMC secundaria, si ha implementado una, con la lista del

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

inventario y asegúrese de que el **estado del appliance** de cada uno sea **Activo**. **No** siga con la inicialización de Almacén de datos hasta que se hayan administrado todos los appliances previstos y el **estado del appliance** sea **Activo**.

Si el estado de un appliance es **Inactivo**, revise la configuración del appliance y la conexión entre la SMC y dicho appliance.

Si un appliance no aparece en el inventario, agréguelo.

2. En cada appliance, haga clic en el menú Acciones y, a continuación, seleccione **Editar configuración del appliance**.
3. Seleccione la pestaña Appliance. Asegúrese de que **Activar SSH** y **Activar acceso raíz SSH** estén seleccionados. **No** siga con la inicialización de Almacén de datos hasta que todos los appliances previstos tengan el acceso SSH y el acceso raíz SSH activados.

   Si ninguno de los dos está seleccionado, seleccione la opción y haga clic en **Aplicar configuración**.

Distribuya contraseñas de Almacén de datos a su SMC, sus Nodos de datos y sus recopiladores de flujo:

Desde la interfaz de línea de comandos de la SMC, puede ejecutar un script que prepare su implementación de Stealthwatch para la inicialización de Almacén de datos mediante la distribución de la información necesaria para establecer conexiones de Almacén de datos seguras. La primera opción del script le permite crear contraseñas para las cuentas de usuario `dbadmin` y `readonlyuser` y las distribuye de forma segura a la SMC, los Nodo de datos y los recopiladores de flujo. Cada contraseña debe cumplir los siguientes requisitos:

- al menos 1 número
- al menos 1 minúscula
- al menos 1 mayúscula
- al menos 1 carácter especial de la siguiente lista: `<>.,?/'"|:;` `~!@#$%^&*()-_+={}[]`
- al menos 8 caracteres, no hay longitud máxima
- solo caracteres con codificación ASCII

Cuando ejecuta un script para inicializar el Almacén de datos, el script utiliza esta información para establecer las credenciales de la cuenta de usuario `dbadmin` y

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

`readonlyuser`, y establecer conexiones seguras entre cada appliance y el Almacén de datos.

> Si establece estas contraseñas y luego las pierde, póngase en contacto con el soporte de Cisco para obtener ayuda para recuperarlas.

Tenga en cuenta que utiliza esta opción cuando implementa por primera vez el Almacén de datos. Si ya ha inicializado el Almacén de datos y desea actualizar estas contraseñas, consulte Actualizar las contraseñas dbadmin y readonlyuser del almacén de datos para obtener más información.

Antes de comenzar

- Compile una lista de contraseñas raíz para la SMC, los Nodos de datos, los recopiladores de flujo y la SMC secundaria, si ha implementado una.
- Inicie sesión en la consola SMC como `root`.

Procedimiento

1. Desde la línea de comandos, introduzca `cd /lancope/admin/cds` y pulse Entrar para cambiar los directorios.
2. Introduzca `./setup-sw-datastore-secure-connectivity` y pulse Entrar para ejecutar el script de bash de conectividad segura de Almacén de datos.
3. En el menú principal del script, seleccione **1. Distribuir la contraseña de SW DataStore a los appliances**.

   El script muestra una lista de la SMC, los Nodo de datos administrados por la SMC, los recopiladores de flujo compatibles con el almacén de datos administrados por la SMC y cualquier SMC secundaria compatible con Almacén de datos administrada por la SMC principal.
4. Confirme la lista de appliances y seleccione **Aceptar**. La primera vez que ejecuta este script cuando configura la implementación de Stealthwatch para el uso de Almacén de datos, se seleccionan todos los appliances.
5. En la línea de comandos, cuando se le solicite la contraseña `root` para cada appliance, introduzca la contraseña y pulse Entrar.

   > Dado que introduce varias contraseñas, asegúrese de introducir la contraseña correcta para dicho appliance.

   Después de introducir las contraseñas `root` de todos los appliances, el script le pide las contraseñas `dbadmin` y `readonlyuser`.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

6. Introduzca la contraseña **dbadmin**.
7. Introduzca la misma contraseña `dbadmin` en el campo **dbadmin (confirmación)**.
8. Introduzca la contraseña **readonlyuser**.
9. Introduzca la misma contraseña `readonlyuser` en el campo **readonlyuser (confirmación)**.

   > No introduzca la misma contraseña para `dbadmin` y `readonlyuser`. Asignar la misma contraseña provoca que el script falle y que no se asignen contraseñas a ninguna de las cuentas de usuario.

10. Seleccione **Aceptar**.

    El script distribuye estas contraseñas de forma segura a los appliances seleccionados. Cuando finalice, mostrará una lista de los appliances actualizados.
11. Seleccione **Aceptar** para volver al menú principal del script.

Siguientes pasos

- Distribuya certificados de identidad de Almacén de datos para comunicaciones seguras, como se describe en el siguiente procedimiento.

Distribuir certificados de identidad para comunicaciones seguras de Almacén de datos a sus appliances

En el script para establecer conexiones de Almacén de datos seguras, la segunda opción le permite generar un certificado de identidad y distribuirlo a la SMC, los Nodo de datos y los recopiladores de flujo. Cuando ejecuta un script para inicializar el Almacén de datos, el script utiliza este certificado de identidad para establecer conexiones seguras entre sus appliances y el Almacén de datos.

El certificado de identidad está autofirmado, es válido durante 5 años y se ha emitido con el nombre común `sw-datastore.stealthwatch.cisco.com`.

Antes de comenzar

- Desde la línea de comandos de la SMC, ejecute el script `setup-sw-datastore-secure-connectivity`.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Procedimiento

1. En el menú principal del script, seleccione **2. Distribuir certificados para la conexión de base de datos segura**.
2. El script muestra una lista de la SMC, los Nodo de datos administrados por la SMC, los recopiladores de flujo administrados por la SMC y cualquier SMC secundaria administrada por la SMC principal.

   Si ya ha confirmado la lista de appliances después de seleccionar **1. Distribuir la contraseña de SW DataStore a los appliances**, es posible que el script no muestre esta lista de appliances. Vaya al paso 4.
3. Confirme la lista de appliances y seleccione **Aceptar**. La primera vez que ejecuta este script cuando configura la implementación de Stealthwatch para el uso de Almacén de datos, se seleccionan todos los appliances.

   El script genera un certificado de identidad, que se utiliza para las comunicaciones seguras, y la clave privada vinculada.
4. En la línea de comandos, cuando se le solicite la contraseña `root` para cada appliance, introduzca la contraseña y pulse Entrar.

   > Dado que introduce varias contraseñas, asegúrese de introducir la contraseña correcta para dicho appliance.
5. Una vez que el script se ha realizado correctamente, muestra un mensaje de éxito y una dirección IP de Nodo de datos. En el siguiente procedimiento, iniciará sesión en la consola de Nodo de datos utilizando el SSH para ejecutar el script de inicialización de Almacén de datos.

   > Registre esta dirección IP antes de salir de este mensaje. No podrá recuperarla después de salir del mensaje.

Siguientes pasos

- Inicialice el Almacén de datos como se describe en el siguiente procedimiento.

Ejecutar un script para inicializar el Almacén de datos y aplicar conexiones seguras

Después de distribuir las contraseñas de usuario `dbadmin` y `readonlyuser` y el certificado de identidad a sus appliances, inicie sesión en el Nodo de datos, como se especifica en el procedimiento anterior, modifique el archivo de configuración

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

`install_SDBN.cfg` y ejecute el script de inicialización `install_SDBN.initial.py`. Este script inicializa el Almacén de datos conectando sus Nodos de datos, establece las credenciales `dbadmin` y `readonlyuser` proporcionadas y aplica el requisito de conexiones seguras entre sus appliances de Stealthwatch y el Almacén de datos.

Después de inicializar el Almacén de datos, copie la clave API maestra de Almacén de datos de este Nodo de datos. Utilice esta información en **Configuración de la consola de administración de Vertica** para instalar la consola de administración de Vertica (VMC) en su SMC.

Antes de comenzar

- Compile una lista de todas sus direcciones IP públicas Nodo de datos `eth0` y direcciones IP privadas de canal de puerto `eth2` o `eth2/eth3`.
- Como `root`, inicie sesión en la consola del Nodo de datos cuya dirección IP se haya mostrado después de distribuir los certificados de identidad mediante el script de conexión segura de Almacén de datos, como se describe en **Distribuir certificados de identidad para comunicaciones seguras de Almacén de datos a sus appliances**.

Procedimiento

1. Desde la línea de comandos, introduzca `cd /lancope/database` y pulse Entrar para cambiar los directorios.
2. Introduzca `cp install_SDBN_example.cfg install_SDBN.cfg` y pulse Entrar para realizar una copia del archivo de configuración de ejemplo.
3. Introduzca `vi install_SDBN.cfg` y pulse Entrar para modificar el archivo de configuración en un editor de texto.
4. Cree secciones `[nodeN]` numeradas consecutivamente para que coincidan con el número de Nodos de datos que ha implementado. Por ejemplo, si ha implementado 6 Nodos de datos, el archivo contendrá lo siguiente:

```
[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
```

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

```
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. Comenzando por la sección `[node1]`, introduzca las direcciones IP privadas (canal de puerto `eth2` o `eth2/eth3`) y públicas (`eth0`) en cada Nodo de datos. Tenga en cuenta lo siguiente:
   - Este script asigna los Nodos de datos al Almacén de datos en el orden en que aparecen en la lista. Si ha implementado sus Nodos de datos con varias fuentes de alimentación redundantes, alterne la asignación de nodos en función de la fuente de alimentación para maximizar el tiempo de actividad general de Almacén de datos y la redundancia de datos.
   - Las direcciones IP privadas no deben ser enrutables, en una LAN o VLAN privada. Debe asignar direcciones IP en el bloque CIDR `169.254.42.0/24`.
   - No superponga las direcciones IP entre Nodos de datos.
   - Solo agregue los Nodos de datos que desee que formen parte del Almacén de datos.
6. En la sección `[common]`, actualice la `subred` para que sea la dirección IP más baja del bloque CIDR de direcciones IP públicas.
7. Pulse Esc, introduzca `:wq` y pulse Entrar para guardar los cambios y salir del editor de texto.
8. Desde la línea de comandos, introduzca `python install_SDBN_initial.py -i install_SDBN.cfg` y pulse Entrar para ejecutar el script de python de inicialización de Almacén de datos. Este script utiliza el archivo de configuración `install_SDBN.cfg` para inicializar los Nodos de datos en el orden especificado.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Cuando finalice el script, revise los mensajes de estado de la CLI para asegurarse de que el script se ha realizado correctamente.

> En cada Nodo de datos, la consola muestra `Requisitos previos que no se cumplen por completo durante la configuración local (SO)` y enumera una serie de mensajes de registro: `SUGERENCIA (S0305)`, `SUGERENCIA (S0041)`, `SUGERENCIA (S0040)`, `ADVERTENCIA (N0010)`, `ERROR (s0180)`, y `ERROR (s0311)`. Estos mensajes de registro son previsibles y no indican un error al inicializar el Almacén de datos. Consulte **Resolución de problemas de implementación del almacén de datos** para obtener más información sobre estos mensajes.

> En cada Nodo de datos, la consola muestra `INFO 6403: El parámetro de configuración SSLCA no está establecido; no se solicitarán ni verificarán los certificados de cliente`. Estos mensajes de registro son previsibles y no indican un error al establecer conexiones seguras con el Almacén de datos. Consulte **Resolución de problemas de implementación del almacén de datos** para obtener más información sobre estos mensajes.

9. Introduzca `cd /opt/vertica/config` para cambiar los directorios.
10. Introduzca `cat apikeys.dat` para mostrar la cadena de clave API en la consola.
11. Copie la cadena de clave API y péguela en un editor de texto sin formato. Utilice esta clave API en **Configuración de la consola de administración de Vertica** para configurar la VMC en su SMC.
12. Anote la dirección IP de este nodo de datos. Utilice esta dirección IP en **Configuración de la consola de administración de Vertica** para configurar la VMC en su SMC.

Siguientes pasos

- Utilice la resolución local en la administración central para asignar las direcciones IP de Nodo de datos al nombre de Almacén de datos, como se describe en el siguiente procedimiento.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Asignar el nombre de Almacén de datos a sus Nodos de datos mediante la resolución local

Después de inicializar el Almacén de datos, utilice la administración central para asignar el nombre de Almacén de datos (`sw-datastore`) a todas las direcciones IP de Nodo de datos en su SMC y sus recopiladores de flujo. Dado que el Almacén de datos contiene varios Nodos de datos, esta asignación de resolución local ayuda a distribuir el almacenamiento de flujo y las solicitudes de consulta de manera más uniforme entre los Nodos de datos, lo que mejora el rendimiento y la respuesta.

> Para un rendimiento óptimo, asigne las direcciones IP de Nodo de datos `eth0` en el **mismo orden** en cada appliance.

Antes de comenzar

- Compile una lista de todas sus direcciones IP públicas de Nodo de datos.
- Compile una lista de los recopiladores de flujo administrados en Administración central.
- Inicie sesión en la aplicación web de la SMC como administrador y vaya a Administración central.

Procedimiento

1. Comenzando por la SMC, haga clic en el menú Acciones y, a continuación, seleccione **Editar configuración del appliance**.
2. Seleccione la pestaña Servicios de red.
3. En la sección Resolución local, haga clic en **Agregar nueva**.
4. Introduzca `sw-datastore` en el campo **Nombre de host**.
5. Introduzca la primera dirección IP pública de Nodo de datos de su lista.
6. Haga clic en **Agregar**.
7. Repita los tres pasos anteriores en el resto de Nodo de datos utilizando la lista de direcciones IP públicas de Nodos de datos.
8. Haga clic en **Aplicar configuración** y, a continuación, confirme los cambios.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

9. Repita este procedimiento en todos los recopiladores de flujo de su lista y en su SMC secundaria, si ha implementado una.

> Para un rendimiento óptimo, asigne las direcciones IP de Nodo de datos `eth0` en el **mismo orden** en cada appliance.

Siguientes pasos

- Vuelva a Stealthwatch Descripción general de la implementación del almacén de datos para revisar el proceso de implementación.
- Configure la consola de administración de Vertica (VMC) en su SMC. Consulte la siguiente sección para obtener más información.

Configuración de la consola de administración de Vertica

Después de inicializar y configurar el Almacén de datos, configure la consola de administración de Vertica (VMC) en su SMC para conectarse al Almacén de datos. Puede utilizar la VMC para supervisar el estado de Almacén de datos y recibir notificaciones basadas en umbrales configurables. Realice lo siguiente:

1. Desde un navegador web de su estación de trabajo local, realice la configuración inicial de la VMC, incluida la configuración de la VMC para que no permita el uso de TLS 1.0 y 1.1 tanto para el acceso al navegador web como para las notificaciones por correo electrónico.
2. En la VMC, configure una conexión segura con su Almacén de datos.
3. En la VMC, configure las notificaciones automáticas (como el correo electrónico) y los umbrales de notificación.

> Si utiliza la opción **3. Actualizar la contraseña de SW DataStore en los appliances** en `setup-sw-datastore-secure-connectivity` para actualizar la contraseña `dbadmin` después de configurarla inicialmente, debe iniciar sesión en la VMC como `dbadmin` para actualizar la contraseña manualmente. Consulte Actualizar las contraseñas dbadmin y readonlyuser del almacén de datos después de la inicialización para obtener más información.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Realizar la configuración inicial de la VMC

Realice la configuración inicial de la VMC la primera vez que acceda a la VMC.

De forma predeterminada, la VMC permite las conexiones TLS 1.0 y TLS 1.1 en un navegador web. Dado que estas versiones anteriores de TLS son menos seguras que TLS 1.2 en adelante, configure la VMC para no permitir conexiones a través de TLS 1.0 y TLS 1.1.

Antes de comenzar

- Anote la dirección IPv4 de su SMC.
- Asegúrese de que el puerto de comunicación `9450/TCP` esté abierto entre la estación de trabajo y la SMC.

Procedimiento

1. En su estación de trabajo, abra un navegador web e introduzca `https://[`*`smc-ipv4-address`*`]:9450/webui/login` en la barra de direcciones. Sustituya `[`*`smc-ipv4-address`*`]` por la dirección IPv4 de su SMC. Acceda a dicha URL.
2. Acepte la licencia de Vertica y, a continuación, haga clic en **Siguiente**.
3. Introduzca la contraseña **`dbadmin`** e introdúzcala en **Confirmar contraseña**.

   > Esta cuenta de usuario `dbadmin` es la cuenta de usuario de la VMC que se asignará más adelante a su cuenta de usuario Almacén de datos `dbadmin`. Puede asignar una contraseña diferente a esta cuenta que la que asignó a su cuenta de usuario Almacén de datos `dbadmin`.

4. Introduzca `dbadmin` como **nombre de grupo Unix**.
5. No cambie las rutas de archivo predeterminadas (`/home/dbadmin`) ni el puerto predeterminado (`5450`); a continuación, haga clic en **Siguiente**.

   Aparecerán las opciones de almacenamiento.
6. Haga clic en **Siguiente**.

   Aparecerán las opciones de autorización de la consola de administración.
7. Haga clic en **Siguiente**. Espere a que se reinicie el servicio de Vertica.

   Esto puede tardar 20 minutos o más. Si la ventana del navegador no se actualiza automáticamente, actualice manualmente la página.
8. Introduzca sus credenciales `dbadmin` y haga clic en **Iniciar sesión** para iniciar sesión en la VMC.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

9. En la página principal de la VMC, haga clic en **Configuración de MC**.
10. Haga clic en la pestaña Configuración.
11. Seleccione **Desactivar las conexiones TLS 1.0 y 1.1 desde el navegador** y, a continuación, guarde el cambio.

Configurar una conexión segura de la VMC para el Almacén de datos

Antes de empezar a configurar esta conexión segura, copie el archivo `/lancope/var/admin/cds/server.crt` de su SMC en su estación de trabajo local. Utilice este archivo para establecer una conexión segura entre la VMC y el Almacén de datos.

Antes de comenzar

- Copie el archivo `/lancope/var/admin/cds/server.crt` de su SMC en su estación de trabajo local.
- Tenga una copia de su clave API maestra de Almacén de datos disponible, como se describe en **Ejecutar un script para inicializar el Almacén de datos y aplicar conexiones seguras**.
- Anote la dirección IP del Nodo de datos desde la que ha copiado la clave API, como se describe en **Ejecutar un script para inicializar el Almacén de datos y aplicar conexiones seguras**.

Procedimiento

1. En la página principal de la VMC, haga clic en **Importar un clúster de base de datos de Vertica**.
2. Introduzca la **dirección IP** de la dirección IP Nodo de datos `eth0` desde la que ha copiado la clave API y, a continuación, haga clic en **Siguiente**.
3. Si lo desea, cambie el **nombre del clúster**.
4. Introduzca la **clave API** maestra de Almacén de datos y, a continuación, haga clic en **Continuar**.

   La VMC localiza el Almacén de datos.
5. Introduzca `dbadmin` como **nombre de usuario** y la **contraseña** `dbadmin`.
6. Seleccione **Usar TLS**.
7. Haga clic en **Configurar TLS e importar base de datos**.

   Aparecerá la ventana Configurar certificados de conexión TLS.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

8. Haga clic en **Configurar conexión TLS**.
9. Seleccione **Cargar un nuevo certificado de CA** y haga clic en **Siguiente**.
10. Haga clic en **Explorar** y, a continuación, seleccione el archivo `server.crt` que guardó en su estación de trabajo local desde la SMC.
11. Introduzca `sw-datastore-cert` como **alias del certificado de CA** y, a continuación, haga clic en **Siguiente**.
12. Haga clic en **Revisar**.
13. Haga clic en **Configurar TLS para la base de datos**.

    La VMC configura conexiones seguras para el Almacén de datos.
14. Haga clic en **Cerrar**.

> Es posible que vea el mensaje "Error al importar la base de datos en MC. no definido". Este mensaje es previsible y no indica un error al establecer una conexión segura con el Almacén de datos.

Configurar notificaciones de alerta de la VMC por correo electrónico

Puede configurar la VMC para enviar notificaciones de alerta por correo electrónico.

Antes de comenzar

- Inicie sesión en la VMC como `dbadmin`.

Procedimiento

1. En la página Configuración de MC, haga clic en la pestaña Gateway de correo electrónico.
2. Introduzca un **servidor SMTP (Nombre de host)**. Puede introducir un nombre de hasta 255 caracteres o una dirección IP.
3. Introduzca un **puerto de servidor SMTP**.
4. Seleccione **Usar TLS** en **Tipo de sesión (SSL o TLS)**.
5. Introduzca un **nombre de usuario SMTP**.
6. Introduzca una **contraseña SMTP**.
7. Introduzca un **alias de correo electrónico de origen**, desde el cual la VMC enviará las alertas por correo electrónico.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

8. Haga clic en **Probar** para probar la configuración.

   Actualice la configuración si no recibe un correo electrónico de prueba.

9. Haga clic en **Aplicar**.

Configurar umbrales de alerta de la VMC

Puede configurar varios umbrales mínimos y máximos a partir de los que la VMC generará una alerta si el Almacén de datos supera un valor de umbral.

Antes de comenzar

- Inicie sesión en la VMC como `dbadmin`.

Procedimiento

1. Seleccione **Configuración > Umbrales**.
2. Marque la casilla de verificación del elemento de línea del umbral de notificación de alerta para activarlo o desmarque la casilla de verificación para desactivarlo. Cisco recomienda activar la notificación de `cambio de estado del nodo` para recibir notificaciones cuando un Nodo de datos se desactive.

   > Al configurar umbrales mínimos, puede dar lugar a excesivas notificaciones de falsos positivos. Por ejemplo, si establece un umbral mínimo de CPU de nodo, este puede activarse con frecuencia, ya que el uso de la CPU fluctúa.

3. Seleccione *Prioridad 1* en cada umbral de notificación del que desee recibir correos electrónicos.
4. Si selecciona *Prioridad 1*, haga clic en el icono de exploración que hay junto a **Destino de correo electrónico**.
5. Introduzca una dirección de correo electrónico en **Introducir campo nuevo** y, a continuación, haga clic en el icono **+**.
6. Haga clic en **OK**.
7. Seleccione un **intervalo de correo electrónico** para determinar la frecuencia de los correos electrónicos cuando Almacén de datos supere un umbral.
8. Haga clic en **Aplicar**.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Siguientes pasos

- Vuelva a Stealthwatch Descripción general de la implementación del almacén de datos para revisar el proceso de implementación.
- Configure la conservación de datos de Almacén de datos como se describe en la siguiente sección.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Configuración de conservación del almacén de datos

De forma predeterminada, el Almacén de datos conserva los datos durante un máximo de siete (7) días antes de eliminarlos automáticamente. Con la API REST de Stealthwatch, puede cambiar este período de conservación:

- a un número de días diferente, hasta 3000, o
- almacenar los datos el mayor tiempo posible, hasta que el Almacén de datos alcance la capacidad máxima.

Tenga en cuenta lo siguiente sobre la conservación del Almacén de datos:

- Después de actualizar la configuración de conservación de datos, no es necesario que reinicie ningún appliance de Stealthwatch o el Almacén de datos. La configuración surte efecto después de unos minutos.
- Cuando cambia la conservación a un período más largo, debe esperar a que caduque la diferencia de tiempo antes de que los datos almacenados se correspondan exactamente con la configuración de conservación. Hasta ese momento, los datos se muestran utilizando la resolución más reducida (es decir, la más general) disponible. Por ejemplo, si cambia la conservación de 3 días a 10 días, debe esperar 7 días antes de que los datos almacenados se correspondan exactamente con la configuración de conservación.
- Es posible que sus datos se eliminen antes del período de conservación que seleccione debido al recorte crítico de los datos según el uso de disco. Si decide almacenar los datos el mayor tiempo posible, cuando el Almacén de datos alcance la capacidad máxima, el sistema comenzará a eliminar los datos más antiguos.
- Si no desea almacenar datos, puede acceder a la interfaz de usuario de administración de cada uno de los recopiladores de flujo y seleccione **Soporte > Ajustes avanzados**. Para cada recopilador de flujo, cambie la entrada “interface_retention_days” de la columna Etiqueta de opciones a 0 (cero) y reinicie el recopilador de flujo (o el motor del recopilador de flujo, si es posible).

Para actualizar esta configuración, utilice la API REST para realizar lo siguiente:

Autenticar contra la API REST de la SMC

Recursos de información de la solicitud

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Recurso	Descripción
URI	`https://[smc-eth0-ip]/token/v2/authenticate`
Descripción	Autenticar contra la API REST de la SMC.
Parámetro URI	• *[smc-eth0-ip]* : dirección IP de gestión de eth0 de la SMC
Método HTTP	POST
Tipo MIME del texto de la solicitud	application/x-www-form-urlencoded
Texto de la solicitud	`username=[username]&password=[password]`
Parámetros del texto de la solicitud	• *[username]* : usuario de administración de la SMC (OBLIGATORIO) • *[password]* : contraseña (OBLIGATORIA) para la cuenta de usuario de administración de la SMC

Código de respuesta y definición de éxito

Respuesta	Descripción
Código de respuesta	200: Éxito
Texto de la respuesta	El texto de la respuesta contiene información de cookies, que debe pasar a las siguientes llamadas a la API REST de esta sesión. Su sesión es válida durante 20 minutos.

Recuperar la configuración de conservación de datos del Almacén de datos actual

Información del recurso de la solicitud

Recurso	Descripción
URI	`https://[smc-eth0-ip]/smc-`

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Recurso	Descripción
	`configuration/rest/v1/cds/retentionsettings`
Descripción	Recuperar la configuración de conservación de datos del Almacén de datos actual.
Parámetro URI	• *`[smc-eth0-ip]`* : dirección IP de gestión de eth0 management de la SMC
Método HTTP	GET
Tipo MIME del cuerpo de la solicitud	n/d
Texto de la solicitud	n/d
Parámetros del texto de la solicitud	n/d

Información y código de respuesta de éxito

Recurso	Descripción
Código de respuesta	200: Éxito
Texto de la respuesta	El texto de la respuesta contiene la configuración actual de conservación de datos del almacén de datos. Si no la ha cambiado anteriormente, el valor predeterminado es de 7 días.

Actualizar la configuración de conservación de datos del Almacén de datos

Información de recursos de la solicitud

Recurso	Descripción
URI	`https://`*`[smc-eth0-ip]`*`/smc-configuration/rest/v1/cds/retentionsettings`

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Recurso	Descripción
Descripción	Actualice la configuración actual de conservación de datos del Almacén de datos.
Parámetro URI	• *[smc-eth0-ip]* : dirección IP de gestión de eth0 de la SMC
Método HTTP	PUT
Tipo MIME del texto de la solicitud	application/json

Texto de la solicitud	`{`
	`"interfaceRetentionType":"`*[type]*`",`
	`"interfaceRetentionAmount":"`*[#]*`"`
	`}`

Parámetros del texto de la solicitud	• *[type]* : (OBLIGATORIO) El tipo de conservación de datos, establecido en uno de los siguientes valores de cadena:
	  • `AMOUNT`: almacene datos durante hasta el número de días definidos en interfaceRetentionAmount antes de eliminarlos
	  • `FOREVER`: guarde los datos el mayor tiempo posible, hasta que se alcance la capacidad máxima del Almacén de datos, antes de eliminarlo
	• *[#]* : (OBLIGATORIO) El número máximo de días que el Almacén de datos retiene los datos antes de eliminarlos, se establece en un número entero entre `1-3000`.
	  Aunque establezca `interfaceRetentionType` en `FOREVER`, debe pasar una `interfaceRetentionAmount` que el sistema ignora. Almacena este valor internamente como `7` como valor predeterminado, independientemente de qué `interfaceRetentionAmount` pase en esta situación.

Información y código de respuesta de éxito

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Recurso	Descripción
Código de respuesta	204 - Correcto (sin contenido)
Texto de la respuesta	El cuerpo de la respuesta no contiene contenido.

Consulte la Stealthwatch documentación de la API REST de Enterprise para obtener más información sobre la API REST.

El siguiente procedimiento proporciona la sintaxis de curl para actualizar el período de conservación de datos del Almacén de datos:

Actualice el período de conservación del Almacén de datos:

Antes de comenzar

- Inicie sesión en la consola de un appliance basado en Linux con curl instalado.

Procedimiento

1. Copie el siguiente comando y péguelo en un editor de texto sin formato:

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

2. Sustituya *[username]* por un nombre de usuario de administración de SMC.
3. Sustituya *[password]* por la contraseña de administrador de SMC.
4. Sustituya *[smc-eth0-ip]* por la dirección IP `eth0` de SMC.
5. Copie el comando actualizado, péguelo en la línea de comandos y pulse Entrar para autenticarse en el SMC para usar la API REST.

   Su sesión es válida durante 20 minutos.

6. Copie el siguiente comando y péguelo en un editor de texto sin formato:

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

7. Sustituya *[smc-eth0-ip]* por la dirección IP `eth0` de SMC.
8. Copie el comando actualizado, péguelo en la línea de comando y pulse Intro para recuperar la configuración de conservación actual del Almacén de datos.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Si es la primera vez que realiza una comprobación, el Almacén de datos se configura con un período de conservación de 7 días predeterminado.

9. Copie el siguiente comando y péguelo en un editor de texto sin formato:

```
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. Sustituya *[type]* por uno de los siguientes:
    - `AMOUNT` si desea establecer un número de días para la conservación.
    - `FOREVER` si desea almacenar datos el mayor tiempo posible.
11. Sustituya *[#]* por un número entero entre `1 y 3000` de la cantidad de días para la conservación.

    Debe definir esto incluso si establece *[type]*=`FOREVER`. En este caso, el sistema ignora este valor y lo establece como `7` internamente.
12. Sustituya *[smc-eth0-ip]* por la dirección IP `eth0` de SMC.
13. Copie el comando actualizado, péguelo en la línea de comando y pulse Intro para actualizar la configuración de conservación.

> Después de actualizar la configuración de conservación, no es necesario que reinicie ningún appliance de Stealthwatch o el Almacén de datos. La configuración surte efecto después de unos minutos. Sin embargo, cuando cambia la conservación a un período más largo, debe esperar a que caduque la diferencia de tiempo antes de que los datos almacenados se correspondan exactamente con la configuración de conservación.

Siguientes pasos

- Vuelva a Stealthwatch Descripción general de la implementación del almacén de datos para revisar el proceso de implementación.
- Revise los siguientes pasos, como se describe en la siguiente sección.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Pasos siguientes para la instalación del almacén de datos

Después de implementar y configurar su implementación de Stealthwatch para usarla con un Almacén de datos:

- Instale la aplicación Creador de informes de Stealthwatch en su SMC para ejecutar informes en su implementación de Stealthwatch y ver las estadísticas de almacenamiento de Almacén de datos. Consulte las notas de versión para obtener más información.
- Revise la ayuda en línea de la aplicación web de Stealthwatch para obtener más información sobre cómo utilizar Stealthwatch.
- Vuelva a Stealthwatch Descripción general de la implementación del almacén de datos para revisar el proceso de implementación.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Mantenimiento del almacén de datos

A continuación, se describen las tareas de mantenimiento relacionadas con Almacén de datos y Almacén de datos, entre las que se incluyen:

- reiniciar un Nodo de datos y el Almacén de datos
- copia de seguridad y restauración del Almacén de datos
- agregar, eliminar y sustituir Nodos de datos
- copiar información de confianza en una SMC de conmutación por error antes de subirla de nivel a una SMC principal

> Póngase en contacto con los servicios profesionales de Cisco para obtener ayuda con la planificación e implementación de estas tareas.

Reiniciar un Nodo de datos

> Póngase en contacto con los servicios profesionales de Cisco para obtener ayuda con la planificación e implementación de estas tareas.

Si tiene que reiniciar un Nodo de datos, emita el comando para detenerlo y, a continuación, emita el comando para reiniciarlo.

Detener y reiniciar el Nodo de datos

Antes de comenzar

- Inicie sesión en la consola de un Nodo de datos como `root`.

Procedimiento

1. Introduzca `su - dbadmin` y pulse Entrar para ejecutar los siguientes comandos como usuario `dbadmin`.
2. Copie el siguiente comando y péguelo en un editor de texto sin formato:

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

3. Sustituya `[data-node-hostname]` por el nombre de host del Nodo de datos que desee detener antes de reiniciarlo.
4. Copie el comando actualizado, péguelo en el símbolo del sistema y pulse Entrar para detener el Nodo de datos.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

5. Copie el siguiente comando y péguelo en un editor de texto sin formato:

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

6. Sustituya `[data-node-hostname]` por el nombre de host del Nodo de datos que desee reiniciar.
7. Copie el comando actualizado, péguelo en el símbolo del sistema y pulse Entrar para reiniciar el Nodo de datos.

Reiniciar el Almacén de datos

> Póngase en contacto con los servicios profesionales de Cisco para obtener ayuda con la planificación e implementación de estas tareas.

Para reiniciar el Almacén de datos, emita el comando para detenerlo y, a continuación, emita el comando para reiniciarlo.

Detener y reiniciar el Almacén de datos

Antes de comenzar

- Asegúrese de que los recopiladores de flujo no estén conectados al Almacén de datos ni transmitiendo datos.
- Asegúrese de que su SMC no esté conectada al Almacén de datos ni consultando o actualizando el Almacén de datos.
- Inicie sesión en la consola de un Nodo de datos como `root`.

Procedimiento

1. Introduzca `su - dbadmin` y pulse Entrar para ejecutar los siguientes comandos como usuario `dbadmin`.
2. Tiene las siguientes opciones:
   - Desde el símbolo del sistema, introduzca `/opt/vertica/bin/admintools -t stop_db -d sw` y pulse Entrar para detener el Almacén de datos.
   - Desde el símbolo del sistema, introduzca `/opt/vertica/bin/admintools -t stop_db -d sw -F` y pulse Entrar para detener el Almacén de datos, anulando cualquier recopilador de flujo o conexión SMC.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

3. Desde el símbolo del sistema, introduzca `/opt/vertica/bin/admintools -t start_db -d sw` y pulse Entrar para reiniciar el Almacén de datos.

Crear una copia de seguridad del Almacén de datos

> Póngase en contacto con los servicios profesionales de Cisco para obtener ayuda con la planificación e implementación de estas tareas.

Para realizar una copia de seguridad del Almacén de datos, debe hacer lo siguiente:

- Estimar el tamaño de la copia de seguridad
- Preparar un host de copia de seguridad con el doble de capacidad de almacenamiento que el tamaño de la copia de seguridad

  > Utilice un host basado en Linux independiente de sus appliances de Stealthwatch.

- Instalar Python 3.7 y rsync 3.0.5 en el host de copia de seguridad
- Asegurarse de que todos los Nodo de datos puedan acceder al host de copia de seguridad mediante acceso SSH sin contraseña
- Inicializar el directorio de copia de seguridad en el host de copia de seguridad
- Realizar una copia de seguridad del Almacén de datos

Calcular los requisitos de almacenamiento del host de copia de seguridad

Antes de comenzar

- Inicie sesión en la consola de un Nodo de datos como `root`.

Procedimiento

1. Copie el siguiente comando, péguelo en el símbolo del sistema y pulse Entrar para conectarse a la base de datos mediante vsql y ejecutar la consulta. Cuando se le solicite, introduzca su contraseña. Tenga en cuenta los resultados.

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

2. Multiplique la suma por 2 para calcular la cantidad de espacio de almacenamiento que necesita el host de copia de seguridad.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Preparar un host de copia de seguridad:

Antes de comenzar

- En función de los requisitos de almacenamiento que calculó en la tarea anterior, identifique un host que ejecute Linux en su red para almacenar la copia de seguridad o implemente un host que ejecute Linux con los requisitos de almacenamiento necesarios.

  > Utilice un host basado en Linux independiente de sus appliances de Stealthwatch.

- Inicie sesión en la consola del host de copia de seguridad como `root`.

Procedimiento

1. Desde el símbolo del sistema, introduzca `python --version` y pulse Entrar para ver qué versión de Python ha instalado. Tiene las siguientes opciones:
   - Si se ha instalado Python 3.7, continúe en el paso 4.
   - De lo contrario, instale Python 3.7. Continúe en el paso 2.
2. Introduzca `sudo apt-get update` y pulse Entrar para descargar versiones actualizadas de los paquetes, incluido Python. Cuando se le solicite, introduzca su contraseña.
3. Introduzca `sudo apt-get install python3.7` y pulse Entrar para instalar Python 3.7.
4. Desde el símbolo del sistema, introduzca rsync -version y pulse Entrar para ver qué versión de rsync ha instalado. Tiene las siguientes opciones:

   Si se ha instalado rsync 3.0.5, continúe en el paso 7.

   De lo contrario, instale rsync 3.0.5. Continúe en el paso 5.
5. Introduzca `sudo apt-get update` y pulse Entrar para descargar las versiones actualizadas de los paquetes, incluido rsync. Cuando se le solicite, introduzca su contraseña.
6. Introduzca `sudo apt-get install rsync` y pulse Entrar para instalar rsync.
7. Desde el símbolo del sistema, introduzca `getent passwd | grep dbadmin` y pulse Entrar para determinar si existe una cuenta de usuario `dbadmin` en este host. Tiene las siguientes opciones:

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

- Si existe una cuenta de usuario `dbadmin`, el host de copia de seguridad está listo. Continúe **Activar el acceso SSH sin contraseña para dbadmin:**.
- De lo contrario, cree una cuenta de usuario `dbadmin` en este host. Continúe en el paso 5.

8. Desde el símbolo del sistema, introduzca `useradd dbadmin` y pulse Entrar para crear una cuenta de usuario `dbadmin`.
9. Introduzca `passwd dbadmin` y pulse Entrar para asignar una contraseña a `dbadmin`.
10. Introduzca una **nueva contraseña** y pulse Entrar para establecer la contraseña `dbadmin`. Confirme la contraseña cuando se le solicite.

Siguientes pasos

- Active el acceso SSH sin contraseña para la cuenta de usuario `dbadmin`, como se describe en la siguiente sección.

Activar el acceso SSH sin contraseña para dbadmin:

Antes de comenzar

- Abra el puerto 22/TCP entre el host de copia de seguridad y cada Nodo de datos para SSH, así como el puerto 50000/TCP entre el host de copia de seguridad y cada Nodo de datos para rsync.
- Revise la documentación de OpenSSH en `ssh-copy-id` para obtener más información.
- Inicie sesión en el primer Nodo de datos como `root`.

Procedimiento

1. Copie el siguiente comando y péguelo en un editor de texto sin formato:

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

2. Sustituya `[hostname]` por el nombre del host de copia de seguridad.
3. Copie el comando actualizado, péguelo en el símbolo del sistema y pulse Entrar para copiar la clave SSH autorizada de `dbadmin` en el host de copia de seguridad.
4. Copie el siguiente comando y péguelo en un editor de texto sin formato:

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

5. Sustituya `[hostname]` por el nombre del host de copia de seguridad.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

6. Copie el comando actualizado, péguelo en el símbolo del sistema y pulse Entrar para verificar que puede iniciar sesión en la consola del host remoto a través de SSH sin necesidad de una contraseña de este Nodo de datos.

Inicializar el directorio de copia de seguridad en el host de copia de seguridad:

Antes de comenzar

- Inicie sesión en la consola del primer Nodo de datos como root.

  Tenga en cuenta el Nodo de datos que utiliza para inicializar el directorio de copia de seguridad. Realice también la copia de seguridad desde este Nodo de datos, como se describe en Copia de seguridad del almacén de datos.

Procedimiento

1. Introduzca `su - dbadmin` y pulse Entrar para ejecutar los siguientes comandos como usuario `dbadmin`.
2. Copie el siguiente comando en un editor de texto: `ssh [backup-host-ip]`
3. Sustituya `[backup-host-ip]` por la dirección IP del host de copia de seguridad.
4. Copie el comando actualizado, péguelo en el símbolo del sistema y pulse Entrar para verificar que puede iniciar sesión en la interfaz del host de copia de seguridad como `dbadmin` sin que se le solicite una contraseña. Si el host de copia de seguridad le solicita una contraseña, compruebe su configuración.
5. Introduzca `cd /home/dbadmin` y pulse Entrar para cambiar los directorios.
6. Introduzca `mkdir backups` y pulse Entrar para crear el directorio `backups`.
7. Introduzca `exit` y pulse Entrar para volver al símbolo del sistema del Nodo de datos.
8. Introduzca `vi pw.ini` y pulse Entrar para crear el archivo de contraseña de copia de seguridad `pw.ini` y editarlo.

> Si actualiza la contraseña `dbadmin` con el script `setup-sw-datastore-secure-connectivity`, también debe actualizar la contraseña almacenada en el archivo de contraseña de copia de seguridad `pw.ini` o la copia de seguridad fallará. Consulte Actualizar las contraseñas dbadmin y readonlyuser del almacén de datos después de la inicialización para obtener más información.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

9. Copie las siguientes líneas en un editor de texto sin formato:

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

10. Actualice `[dbadmin-password]` con la contraseña Almacén de datos `dbadmin`.
11. Copie las líneas actualizadas y péguelas en el archivo de contraseña de copia de seguridad `pw.ini`.
12. Pulse Esc e introduzca `:wq`. A continuación, pulse Entrar para salir y guardar los cambios.
13. Introduzca `chmod 640 pw.ini` y pulse Entrar para cambiar los permisos del archivo `pw.ini` para permitir al usuario `dbadmin` leer y editar el archivo.
14. Introduzca `vi config.ini` y pulse Entrar para crear el archivo de configuración de copia de seguridad `config.ini` y editarlo.
15. Copie las siguientes líneas y péguelas en un editor de texto sin formato:

```
[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. Sustituya *`backup-ip-host`* por la dirección IP del host de copia de seguridad.
17. Si los nombres de host en `[Mapping]` no coinciden con sus Nodos de datos, actualice estos nombres de host.
18. Asegúrese de tener una entrada para cada Nodo de datos si ha implementado más de 3 en su entorno.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

19. Copie las líneas actualizadas y péguela en el archivo `config.ini`.
20. Pulse Esc e introduzca `:wq`. A continuación, pulse Entrar para salir y guardar los cambios.
21. Introduzca `vbr -t init -c config.ini` y pulse Entrar para inicializar el directorio `/home/dbadmin/backups` en el host de copia de seguridad para recibir copias de seguridad de Almacén de datos.

Realizar una copia de seguridad de la base de datos del almacén de datos

Antes de comenzar

- Como `root`, inicie sesión en la consola del Nodo de datos desde el que inicializó el directorio del host de copia de seguridad, como se describe en Inicializar el directorio de copia de seguridad en el host de copia de seguridad.

Procedimiento

1. Introduzca `su - dbadmin` y pulse Entrar para ejecutar los siguientes comandos como usuario `dbadmin`.
2. Introduzca `vbr -t backup -c config.ini --debug 3 --dry-run` y pulse Entrar para realizar una prueba de la copia de seguridad sin crearla. Tiene las siguientes opciones:
    - Si la prueba de copia de seguridad se resuelve correctamente, realice la copia de seguridad de Almacén de datos. Continúe en el paso 2.
    - Si la prueba de copia de seguridad no se resuelve, revise los archivos de registro de depuración en el directorio `/tmp/vbr`, resuelva el origen del problema y vuelva a probar la copia de seguridad. Póngase en contacto con el soporte de Cisco si no puede resolver el problema.
3. Introduzca `vbr -t backup -c config.ini` y pulse Entrar para hacer una copia de seguridad del Almacén de datos en el directorio `/home/dbadmin/backups` en el host de copia de seguridad.

Restaurar una copia de seguridad de Almacén de datos

> Póngase en contacto con los servicios profesionales de Cisco para obtener ayuda con la planificación e implementación de estas tareas.

Para restaurar el Almacén de datos desde una copia de seguridad, debe asegurarse de lo siguiente:

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

- El Almacén de datos está inactivo. Solo puede detener el Almacén de datos si los recopiladores de flujo y la SMC no están conectados y realizando cambios.
- La copia de seguridad y el Almacén de datos tienen nombres de nodo idénticos y el mismo número de nodos.

Detener el Almacén de datos:

Antes de comenzar

- Asegúrese de que los recopiladores de flujo no estén conectados al Almacén de datos ni transmitiendo datos.
- Asegúrese de que su SMC no esté conectada al Almacén de datos ni consultando o actualizando el Almacén de datos.
- Inicie sesión en la consola de un Nodo de datos como `root`.

Procedimiento

1. Introduzca `su - dbadmin` y pulse Entrar para ejecutar los siguientes comandos como usuario `dbadmin`.
2. Tiene las siguientes opciones:
   - Desde el símbolo del sistema, introduzca `/opt/vertica/bin/admintools -t stop_db -d sw` y pulse Entrar para detener el Almacén de datos.
   - Desde el símbolo del sistema, introduzca `/opt/vertica/bin/admintools -t stop_db -d sw -F` y pulse Entrar para detener el Almacén de datos, anulando cualquier recopilador de flujo o conexión SMC.

Restaurar el almacén de datos desde una copia de seguridad:

Antes de comenzar

- Si ha actualizado la contraseña `dbadmin` con el script `setup-sw-datastore-secure-connectivity`, también debe actualizar la contraseña almacenada en el archivo de contraseña de copia de seguridad `pw.ini` o la restauración fallará. Consulte Actualizar las contraseñas dbadmin y readonlyuser del almacén de datos después de la inicialización para obtener más información.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

- Identifique el Nodo de datos en el que almacenó el archivo de configuración de copia de seguridad `config.ini` e inicie sesión en su consola como `root`.

Procedimiento

1. Introduzca `su - dbadmin` y pulse Entrar para ejecutar los siguientes comandos como usuario `dbadmin`.
2. Desde el símbolo del sistema, introduzca `vbr --task restore --config-file config-file.ini` y pulse Entrar para restaurar el Almacén de datos desde el host de copia de seguridad.

Iniciar el Almacén de datos:

Antes de comenzar

- Inicie sesión en la consola de un Nodo de datos como `root`.

Procedimiento

1. Introduzca `su - dbadmin` y pulse Entrar para ejecutar los siguientes comandos como usuario `dbadmin`.
2. Desde el símbolo del sistema, introduzca `/opt/vertica/bin/admintools -t start_db -d sw` y pulse Entrar para iniciar el Almacén de datos.

Siguientes pasos

- Elimine la instantánea catalog, como se describe en la siguiente sección.

Eliminar la instantánea catalog:

Después de reiniciar el Almacén de datos, elimine la instantánea cuyo nombre es `catalog`. Esta instantánea no es necesaria una vez que se resuelva la restauración y evita que Vertica ejecute la gestión de retenciones.

Antes de comenzar

- Inicie sesión en la consola de un Nodo de datos como `root`.

Procedimiento

1. Introduzca `su - dbadmin` y pulse Entrar para ejecutar los siguientes comandos como usuario `dbadmin`.
2. Copie el siguiente comando y péguelo en un editor de texto sin formato:

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

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

3. Sustituya `[password]` por su contraseña `dbadmin`.
4. Copie el comando actualizado, péguelo en el símbolo del sistema y pulse Entrar para eliminar la instantánea `catalog`.

Siguientes pasos

- Vuelva a conectar los recopiladores de flujo al Almacén de datos y asegúrese de que estén transmitiendo datos.
- Vuelva a conectar su SMC al Almacén de datos.

Agregar tres Nodos de datos al Almacén de datos

> Póngase en contacto con los servicios profesionales de Cisco para obtener ayuda con la planificación e implementación de estas tareas.

Puede ampliar su Almacén de datos en incrementos de tres Nodos de datos o múltiplos de tres Nodos de datos. Si desea ampliar el número de Nodos de datos en su Almacén de datos, realice las siguientes tareas:

Preparar el Almacén de datos para agregar Nodos de datos y reequilibrar

Antes de agregar un Nodo de datos, haga lo siguiente:

- Haga una copia de seguridad del Almacén de datos. Consulte **Crear una copia de seguridad del Almacén de datos** para obtener más información.
- Asegúrese de que los recopiladores de flujo no estén conectados al Almacén de datos ni transmitiendo datos.
- Asegúrese de que su SMC no esté conectada al Almacén de datos ni consultando o actualizando el Almacén de datos.
- Elimine las particiones de datos antiguas no utilizadas. Póngase en contacto con los servicios profesionales de Cisco para obtener ayuda con la identificación de estas particiones.
- Desactive los segmentos locales. Desde vsql, emita `SELECT DISABLE_LOCAL_SEGMENTS();`
- Actualice la configuración del conjunto de recursos. Desde vsql, emita el `conjunto de recursos alternos REFRESH MAXCONCURRENCY 2 PLANNEDCONCURRENCY 2 MEMORYSIZE '40%' MAXMEMORYSIZE '70%;`

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Agregar Nodos de datos al Almacén de datos

A continuación, si aún no lo ha hecho, implemente los Nodos de datos en su red en múltiplos de 3. Realice la configuración inicial en la configuración del sistema mediante el asistente de primera configuración y la herramienta de configuración de appliances para completar la configuración inicial. Consulte el **Apéndice B. Instalación del hardware de Stealthwatch** y el **Apéndice C. Configuración de los appliances** para obtener más información.

Después de configurar los Nodos de datos, incluida la asignación de una dirección IP de administración `eth0` enrutable y una dirección IP de canal de puerto `eth2` o `eth2/eth3` no enrutable, haga lo siguiente:

- Inicie sesión en un Nodo de datos y configure el archivo de configuración `update_SDBN.cfg` para agregar sus nuevos Nodos de datos.
- Ejecute el script `update_SDBN.py` para agregar los Nodos de datos al Almacén de datos y opcionalmente agréguelos también a la base de datos de Almacén de datos

Agregar Nodos de datos al Almacén de datos:

Antes de comenzar

- Inicie sesión en la consola de un Nodo de datos como `root`.

Procedimiento

1. Introduzca `su - dbadmin` y pulse Entrar para ejecutar los siguientes comandos como usuario `dbadmin`.
2. Desde la línea de comandos, introduzca `cd /lancope/database` y pulse Entrar para cambiar los directorios.
3. Introduzca `cp update_SDBN_example.cfg update_SDBN.cfg` y pulse Entrar para realizar una copia del archivo de configuración de ejemplo de adición de Nodo de datos.
4. Introduzca `vi update_SDBN.cfg` y pulse Entrar para modificar el archivo de configuración de adición de Nodo de datos en un editor de texto.
5. Cree secciones `[nodeN]` numeradas consecutivamente para que coincidan con el número de nuevos Nodo de datos que desea agregar al Almacén de datos. Por ejemplo, si ya tiene 3 Nodos de datos implementados en su red y desea agregar 6 Nodos de datos, su archivo contendrá lo siguiente:

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

```
[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. Comenzando con la sección `[node1]`, introduzca las direcciones IP públicas y privadas en cada nuevo Nodo de datos. Tenga en cuenta lo siguiente:
    - Este script agrega Nodos de datos al Almacén de datos en el orden en que aparecen en la lista, numerando consecutivamente después de que el Nodo de datos cuyo número sea más alto ya forme parte del Almacén de datos. Si ha implementado sus Nodos de datos en diferentes racks, alterne la asignación de nodos entre los racks para maximizar la redundancia de datos.
    - Las direcciones IP privadas no deben ser enrutables, en una LAN o VLAN privada. Debe asignar direcciones IP en el bloque CIDR `169.254.42.0/24`.
    - No superponga las direcciones IP entre Nodo de datos.
    - No agregue su Nodo de datos de repuesto aquí, aunque lo haya implementado en su entorno sin configurarlo. Solo agregue los Nodos de datos que desee que formen parte del Almacén de datos.
7. En la sección `[common]`, actualice `subnet` para que coincida con sus direcciones IP públicas.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

8. En la sección `[common]`, actualice el valor de `firstNode` para que sea uno mayor que el número de los Nodo de datos que ya forman parte de la implementación de Almacén de datos.
9. Pulse Esc, introduzca `:wq` y pulse Entrar para guardar los cambios y salir del editor de texto.
10. Desde la línea de comandos, tiene las siguientes opciones:

    Introduzca `python update_SDBN.py -i update_SDBN.cfg` y pulse Entrar para ejecutar el script de python de adición de Nodos de datos. Este script utiliza el archivo de configuración `update_SDBN.cfg` para agregar los nuevos Nodo de datos en Almacén de datos en el orden especificado. Tenga en cuenta que **no** se agregan a la base de datos en este caso.

    Introduzca `python update_SDBN.py -i update_SDBN.cfg -d` y pulse Entrar para ejecutar el script de python de adición de Nodos de datos. Este script utiliza el archivo de configuración `update_SDBN.cfg` para agregar los nuevos Nodos de datos en Almacén de datos en el orden especificado y también agrega los Nodos de datos como parte de la base de datos.

    Cuando finalice el script, revise los mensajes de estado de la CLI para asegurarse de que el script se ha realizado correctamente.
11. Introduzca `cd /opt/vertica/config` para cambiar los directorios.
12. Introduzca `vi apikeys.dat` para abrir el archivo de claves API en un editor de texto.
13. Pulse Esc y, a continuación, introduzca `q!` y pulse Entrar para salir del editor de texto sin guardar los cambios.
14. Anote la dirección IP de este nodo de datos. Utilice esta dirección IP en **Mantenimiento del almacén de datos** para configurar la VMC en su SMC.

Si no agrega los nuevos Nodos de datos a la base de datos con el script `update_SDBN.py`, puede agregar los Nodos de datos manualmente. Inicie sesión en un Nodo de datos en su Almacén de datos y agregue los Nodos de datos al Almacén de datos.

Agregar nuevos Nodo de datos al Almacén de datos:

Antes de comenzar

- Inicie sesión en un Nodo de datos como `root`.

Procedimiento

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

1. Introduzca `su - dbadmin` y pulse Entrar para ejecutar los siguientes comandos como usuario `dbadmin`.
2. Copie el siguiente comando y péguelo en un editor de texto sin formato:

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

3. Sustituya `[dbadmin-password]` por la contraseña `dbadmin`.
4. Sustituya `[data-node-eth0-addresses]` por una lista separada por comas de las nuevas direcciones IP enrutables Nodo de datos `eth0`.
5. Copie el comando actualizado, péguelo en el símbolo del sistema y pulse Entrar para agregar los nuevos Nodos de datos a la base de datos.

Después de agregar los Nodos de datos a la base de datos, vuelva a equilibrar los datos en los Nodo de datos para crear un almacenamiento de datos equilibrado en cada Nodo de datos.

Volver a equilibrar los datos en el Almacén de datos:

Antes de comenzar

- Inicie sesión en un Nodo de datos como `root`.

Procedimiento

1. Introduzca `su - dbadmin` y pulse Entrar para ejecutar los siguientes comandos como usuario `dbadmin`.
2. Copie el siguiente comando y péguelo en un editor de texto sin formato:

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

3. Sustituya `[dbadmin-password]` por la contraseña `dbadmin`.
4. Copie el comando actualizado, péguelo en el símbolo del sistema y pulse Entrar para iniciar el reequilibrio de datos. Tenga en cuenta que puede tardar un tiempo, dependiendo de varios factores, incluido el número de proyecciones, la cantidad de datos y otros factores.
5. Después de que se complete el reequilibrio, actualice la configuración del conjunto de recursos. Desde vsql, emita el `conjunto de recursos alternos REFRESH MAXCONCURRENCY 2 PLANNEDCONCURRENCY 2 MEMORYSIZE '40%' MAXMEMORYSIZE '0%;`

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Eliminar un Nodo de datos del Almacén de datos

> Póngase en contacto con los servicios profesionales de Cisco para obtener ayuda con la planificación e implementación de estas tareas.

Si desea eliminar un Nodo de datos del Almacén de datos, tenga en cuenta lo siguiente:

- El Almacén de datos debe estar en ejecución.
- Ejecute primero una copia de seguridad. Consulte **Crear una copia de seguridad del Almacén de datos** para obtener más información.
- Debe tener al menos 3 nodos en el Almacén de datos debido a la configuración de tolerancia a errores. Si quiere reemplazar un nodo, consulte **Sustituir un Nodo de datos por un Nodo de datos de repuesto con una dirección IP diferente** para obtener más información.

Eliminar un nodo del Almacén de datos:

Antes de comenzar

- Inicie sesión en la consola de administración de Vertica como `dbadmin`.

Procedimiento

1. Seleccione **Administrar**. Aparece la página Administrar.
2. Seleccione el nodo que desea eliminar y haga clic en **Eliminar nodo**.

Sustituir un Nodo de datos por un Nodo de datos de repuesto con una dirección IP diferente

> Póngase en contacto con los servicios profesionales de Cisco para obtener ayuda con la planificación e implementación de estas tareas.

Preparar el Almacén de datos para sustituir un Nodo de datos con errores

- Haga una copia de seguridad del Almacén de datos. Consulte **Crear una copia de seguridad del Almacén de datos** para obtener más información.
- Agregue el Nodo de datos de repuesto al Almacén de datos. Consulte **Agregar Nodos de datos al Almacén de datos:** para obtener más información.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Reemplazar el Nodo de datos

Si Vertica aún se está ejecutando en el Nodo de datos que desea reemplazar, detenga Vertica. A continuación, sustituya el Nodo de datos anterior por el Nodo de datos nuevo y distribuya la configuración necesaria al nuevo nodo de datos. Elimine el Nodo de datos anterior y reinicie el Nodo de datos nuevo.

Detener Vertica en un Nodo de datos

Si el Nodo de datos que desea eliminar sigue ejecutando Vertica, detenga Vertica en dicho Nodo de datos. Si dicho Nodo de datos está inactivo o no ejecuta Vertica, vaya al siguiente paso.

Antes de comenzar

- Inicie sesión en la consola de un Nodo de datos como `root`.

Procedimiento

1. Introduzca `su - dbadmin` y pulse Entrar para ejecutar los siguientes comandos como usuario `dbadmin`.
2. Copie el siguiente comando y péguelo en un editor de texto sin formato:

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

3. Sustituya `[node-ip-addresses]` por una lista separada por comas de las direcciones IP enrutables Nodo de datos `eth0` que desea eliminar del Almacén de datos.
4. Copie el comando actualizado, péguelo en el símbolo del sistema y pulse Entrar para detener Vertica en dicho Nodo de datos.

Reemplazar un Nodo de datos

Antes de comenzar

- Inicie sesión en la consola de un Nodo de datos como `root`.

Procedimiento

1. Introduzca `su - dbadmin` y pulse Entrar para ejecutar los siguientes comandos como usuario `dbadmin`.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

2. Copie el siguiente comando y péguelo en un editor de texto sin formato:

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

3. Sustituya `[old-data-nodo-hostname]` con el nombre de host de Nodo de datos que desea eliminar de Almacén de datos.
4. Sustituya `[new-data-nodo-hostname]` por el nombre de host de Nodo de datos que desee agregar como sustitución del Almacén de datos.
5. Copie el comando actualizado, péguelo en el símbolo del sistema y pulse Entrar para sustituir el Nodo de datos anterior por el Nodo de datos nuevo.
6. Copie `/opt/vertica/bin/admintools -t distribute_config_files`, péguelo en el símbolo del sistema y pulse Entrar para distribuir los archivos de configuración al nuevo Nodo de datos.
7. Copie el siguiente comando y péguelo en un editor de texto sin formato:

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

8. Sustituya `[old-data-nodo-hostname]` por el nombre de host de Nodo de datos que desea eliminar del Almacén de datos.
9. Copie el comando actualizado, péguelo en el símbolo del sistema y pulse Entrar para eliminar el Nodo de datos anterior del Almacén de datos.
10. Copie el siguiente comando y péguelo en un editor de texto sin formato:

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

11. Sustituya `[new-data-nodo-hostname]` por el nombre de host de Nodo de datos que desee agregar como sustitución del Almacén de datos.
12. Copie el comando actualizado, péguelo en el símbolo del sistema y pulse Entrar para reiniciar el Nodo de datos nuevo.

Copiar información de confianza de Almacén de datos en una SMC de conmutación por error

Si implementa una SMC de conmutación por error en su entorno y la administra su SMC principal, cuando ejecuta el script `setup-sw-datastore-secure-connectivity`, cierta información de confianza, incluidas las contraseñas `dbadmin` y `readonlyuser` y los certificados de identidad para las comunicaciones seguras con los Nodo de datos, no se copian en la SMC de conmutación por error. Antes de poder

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

ascender la SMC de conmutación por error a SMC principal en una implementación de Almacén de datos, debe copiar los archivos de su SMC principal a la SMC de conmutación por error. Si no copia esta información de confianza, su SMC no se puede conectar al Almacén de datos.

Además, si ya ha ascendido su SMC de conmutación por error a SMC principal, degradado su SMC principal a SMC de conmutación por error y desea agregar nuevos appliances a su implementación de Stealthwatch, debe copiar la información de confianza en la nueva SMC de conmutación por error antes de ejecutar `setup-sw-datastore-secure-connectivity`. Si no copia esta información de confianza, el script puede fallar.

Copiar la información de confianza entre SMC:

Antes de comenzar

- Identifique las direcciones IP y las credenciales raíz de la SMC principal y la SMC de conmutación por error.
- Si su SMC de conmutación por error se ha ascendido recientemente a SMC principal, inicie sesión en la consola de dicha SMC como `root`.

Procedimiento

1. Copie el siguiente comando y péguelo en un editor de texto sin formato:

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

2. Sustituya `[demo-smc-ip-address]` por la dirección IP de su SMC recientemente degradada (SMC de conmutación por error actual).
3. Copie el comando actualizado, péguelo en el símbolo del sistema y pulse Entrar para copiar la información de confianza de Almacén de datos de la SMC recientemente degradada (SMC de conmutación por error actual) a su SMC recién ascendida (SMC principal actual). Introduzca su contraseña `root` para la SMC recientemente degradada (SMC de conmutación por error actual) cuando se le solicite.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Resolución de problemas de implementación del almacén de datos

Resolución de problemas de implementación de hardware

Si tiene problemas con la implementación o la configuración de SMC o los recopiladores de flujo, consulte la Guía de instalación de hardware Stealthwatch x210 y la Guía de configuración del sistema Stealthwatch para obtener más información.

Resolución de problemas del script "setup-sw-datastore-secure-connectivity"

Si ha subido de nivel a un SMC de conmutación por error a SMC principal, consulte Copiar información de confianza del almacén de datos en un SMC de conmutación por error para obtener información sobre cómo copiar Almacén de datos información de confianza a su SMC recién promocionado (principal actual).

El script `setup-sw-datastore-secure-connectivity` del Almacén de datos de conexión segura registra los mensajes en los archivos de registro en `/lancope/var/logs/containers/setup-sw-datastore-secure-connectivity.log`. Puede consultarlos para obtener información adicional.

Mensajes de error generales de setup-sw-datastore-secure-connectivity

La siguiente tabla enumera los mensajes de error que pueden mostrarse si el script `setup-sw-datastore-secure-connectivity` encuentra un error y las posibles soluciones al problema.

Mensaje de error	Descripción	Posibles soluciones
Error al autorizar el inicio de sesión remoto para `[ip-address]`	El script `setup-sw-datastore-secure-connectivity` no pudo iniciar sesión	• Compruebe que ha proporcionado la contraseña raíz correcta para el acceso. • Compruebe que el appliance se esté ejecutando actualmente. • Compruebe que la conexión entre el

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

	de forma remota en un appliance para proporcionar información clave.	script y el appliance esté activa actualmente.
Error al generar par de claves.	El script `setup-sw-datastore-secure-connectivity` encontró un error al generar las claves asociadas con los certificados de identidad utilizados para las conexiones seguras del Almacén de datos.	• Póngase en contacto con el soporte de Cisco para obtener más información.
No se pudo autenticar con autoridad de token.	El script `setup-sw-datastore-secure-connectivity` no pudo establecer correctamente una conexión con la	• Póngase en contacto con el soporte de Cisco para obtener más información.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

	administración central.	
Error al obtener inventario de SMC.	El script `setup-sw-datastore-secure-connectivity` no pudo recuperar correctamente la información de la administración central.	• Revise `/lancope/var/logs/container/svc-central-management.log` para probar y determinar si hay un problema con la administración central. • Póngase en contacto con el soporte de Cisco para obtener más información.
No se han encontrado clientes de la base de datos.	El SMC y los recopiladores de flujo no se configuraron correctamente para su uso con Almacén de datos.	• Inicie sesión en la CLI del appliance, ejecute la configuración del sistema y active el uso con Almacén de datos.
La contraseña no está disponible. Es posible que desee eliminar /lancope/var/etc/keystore /store y volver a ejecutar setup-sw-datastore-secure-connectivity.	El script `setup-sw-datastore-secure-connectivity` ha detectado un problema al guardar o distribuir las contraseñas de `dbadmin` y de	• Elimine el contenido de `/lancope/var/etc/keystore /store` y, a continuación, vuelva a ejecutar el script `setup-sw-datastore-secure-conectivity`.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

	`readonlyuser`.	
Registre los nodos de datos con la administración central antes de intentar configurar la conexión segura.	Sus Nodos de datos no están gestionados por la administración central.	• Administre sus Nodos de datos con la administración central.
El inventario de SMC está vacío. Agregue un appliance a la administración central.	La administración central no está gestionando Nodo de datos ni recopiladores de flujo.	• Gestione sus recopiladores de flujo y Nodo de datos con la administración central.
sw-datastore-dbadmin-password o sw-datastore-readonlyuser-password no están presentes en la entrada	La contraseña de `dbadmin` o la contraseña de `readonlyuser` no se definieron.	• En el script, ejecute **1. Distribuya de nuevo la contraseña de SW DataStore a los appliances**, si aún no ha iniciado Almacén de datos, y defina una contraseña de `dbadmin` y una contraseña de `readonlyuser`. • Si ha iniciado Almacén de datos, en el script, ejecute **3. Actualice la contraseña del SW DataStore en los appliances** para actualizar la contraseña de `dbadmin` y de `readonlyuser`.
Las contraseñas de SW Datastore ya se han iniciado en `[ip-`	El Almacén de datos ya	• En el script, ejecute **3. Actualice la contraseña del SW DataStore en los appliances** para actualizar la

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

address].	está iniciado; no puede utilizar **1. Distribuya la contraseña de SW DataStore a los appliances** de `setup-sw-datastore-secure-connectivity` para cambiar las contraseñas de `dbadmin` o de `readonlyuser`.	contraseña de `dbadmin` y de `readonlyuser`.
Las contraseñas de SW Datastore no se almacenan debido a: valor vacío	La contraseña de `dbadmin` o la contraseña de `readonlyuser` no se definieron.	• En el script, ejecute **1. Distribuya de nuevo la contraseña de SW DataStore a los appliances**, si aún no ha iniciado Almacén de datos, y defina una contraseña de `dbadmin` y una contraseña de `readonlyuser`. • Si ha inicializado Almacén de datos, en el script, ejecute **3. Actualice la contraseña del SW DataStore en los appliances** para actualizar la contraseña de `dbadmin` y de `readonlyuser`.
No hay nodos de datos gestionados actualmente.	Sus Nodos	• Administre sus Nodos de datos con la administra-ción central.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

	de datos no están gestionados por la administra-ción central.	
No hay SMC/FC administrados actualmente.	La administración central no gestiona sus recopiladores de flujo (ni ningún SMC de conmutación por error).	• Administre sus recopiladores de flujo (y SMC de conmutación por error) con la administración central.
Código de error desconocido: `[error-code]` en `[ip-address]`	El script encontró un error al intentar distribuir las contraseñas de `dbadmin` y de `readonlyuser`.	• Póngase en contacto con el soporte de Cisco para obtener más información.

Resolución de problemas del script install_SDBN_initial.py

El script de inicialización `install_SDBN_initial.py` Almacén de datos registra los mensajes en los archivos de registro en `/lancope/var/database/logs/db_initial_install_[datestamp].log`. Puede consultarlos para obtener información adicional.

Requisitos previos que no se cumplen por completo durante la configuración local (SO) de verify-[data-node-ip-address].xml

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Al iniciar Almacén de datos en la Configuración e iniciación del almacén de datos ejecutando el script de python `install_SDBN_initial.py`, puede tener en cuenta que los `requisitos previos de las salidas de la consola no se cumplen completamente durante la configuración local (SO) de verify-[data-node-ip-address].xml`, seguidos por una serie de mensajes de registro. Estos mensajes de registro se anticipan y no indican un fallo al iniciar Almacén de datos. No es necesario que realice ninguna acción con ninguno de estos mensajes de registro.

La siguiente tabla describe cada mensaje.

Nivel de registro y código de error	**Descripción**	**Explicación**
`ERROR (s0180)`	`Tamaño de intercambio insuficiente. Necesita 2,00 GB, tiene 1,50 GB`	El espacio asignado para la partición de intercambio no cumple las recomendaciones. **No** modifique la asignación de espacio de intercambio. Cisco ha configurado su Almacén de datos con la asignación de espacio de intercambio correcta.
`ERROR (s0311)`	`la cuenta raíz no se encuentra en /etc/sudoers`	El instalador no ha encontrado la cuenta raíz en la lista de permisos de superusuario `/etc/sudoers` y recomienda que actualice Vertica para resolver el problema. **No** actualice Vertica. Esta configuración es intencional por motivos de seguridad.
`HINT (S0040)`	`No se pudieron encontrar las siguientes herramientas que normalmente proporciona el paquete pstack o gstack: pstack/gstack`	El instalador no puede encontrar los paquetes `pstack` o `gstack` para registrar los seguimientos de pila. Estos no son necesarios para su Almacén de datos.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

CONSEJO (S0041)	No se pudieron encontrar las siguientes herramientas que normalmente proporciona el paquete mcelog: mcelog	El instalador no puede encontrar el paquete `mcelog` para registrar comprobaciones de máquinas. Esto no es necesario para su Almacén de datos.
CONSEJO (S0305)	TZ no está definido para dbadmin. Considere actualizar .profile or .bashrc	El instalador no ha encontrado una variable de entorno `TZ` para la cuenta de usuario dbadmin, utilizada para zonas horarias. Esto no es necesario para su Almacén de datos, ya que configura los servidores NTP para la implementación de Stealthwatch.
ADVERTENCIA (N0010)	Linux iptables (firewall) tiene algunas reglas no triviales en las tablas: filtro	Las `iptables` de Nodo de datos contienen reglas preexistentes. El sistema registra una advertencia si `iptables` contiene reglas, pero no comprueba si hay colisiones con los puertos de comunicación necesarios. Esto es previsible y no debería causar problemas con la implementación del nodo de datos.

El parámetro de configuración SSLCA no está establecido; no se solicitarán ni verificarán los certificados de cliente

Al iniciar Almacén de datos en la Configuración y el inicio del almacén de datos ejecutando el script de python `install_SDBN_initial.py`, puede observar que la consola devuelve `Habilitar SSL/TLS para conexiones remotas`, seguidas de `INFO 6403: el parámetro de configuración SSLCA no está establecido; Los certificados de cliente no se solicitarán ni verificarán` una vez para cada Nodo de datos que esté iniciando. Este mensaje de registro es previsible y no indica un error al establecer conexiones seguras con Almacén de datos. No es necesario que realice ninguna acción con ninguno de estos mensajes

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

de registro.

El Almacén de datos se configura en el modo de servidor TLS, que requiere que cuando los appliances establezcan una conexión segura con el Almacén de datos, también verifiquen el certificado del servidor de la base de datos. Compare esto con la configuración de modo mutuo de TLS, que requiere que cuando los appliances establezcan una conexión segura con Almacén de datos, los appliances comprueben el certificado del servidor de la base de datos y la base de datos verifique los certificados de cliente de los appliances. El modo mutuo de TLS requiere la configuración del parámetro `SSLCA` con el archivo `root.crt` que contiene la autoridad de certificación (CA) o la cadena de confianza de CA que se utiliza para firmar los certificados de cliente. Debido a que el modo mutuo no está habilitado, `SSLCA` no está configurado y Almacén de datos no verifica los certificados de cliente al establecer una conexión segura. Sin embargo, la conexión entre los appliances y Almacén de datos en el modo de servidor TLS sigue siendo una conexión segura a través de TLS.

Mensajes de error generales de install_SDBN_initial.py

La siguiente tabla enumera los mensajes de error que pueden mostrarse si el script `install_SDBN_initial.py` detecta un error y las posibles soluciones al problema.

Mensaje de error	Descripción	Posibles soluciones
No se encontró el archivo de configuración o no hay secciones válidas	El script `install_SDBN_initial.py` no puede localizar el archivo de configuración `install_SDBN.cfg` o los datos del archivo de configuración no tienen el formato esperado.	• Asegúrese de que tiene una copia de `install_SDBN_example.cfg` guardada en `/lancope/database/install_SDBN.cfg` en esta Nodo de datos. • Asegúrese de que el formato de `install_SDBN.cfg` coincide con el formato de `install_SDBN_example.cfg`, de que asigna un nombre a cada sección de nodo en el `nodo#` de formato, de que ha definido una dirección IP pública y privada para cada sección de configuración de Nodo de datos y de que tiene una subred definida en la sección común.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

No se pudo encontrar el archivo jar esperado para recuperar las contraseñas de usuario de base de datos, compruebe que está ejecutando una imagen que contiene este soporte	El script `install_SDBN_initial.py` no puede encontrar el archivo `sw-datastore-admin.jar` que contiene las contraseñas de `dbadmin` y `readonlyuser`.	• Asegúrese de que su appliance sea de la versión 7.3+. • Ejecute el script `setup-sw-datastore-secure-connectivity` en `/lancope/admin/cds` y seleccione la opción **1. Distribuya la contraseña de SW DataStore a los appliances** para distribuir las contraseñas de dbadmin y de solo usuario. Después de completar esto, si aún no lo ha hecho, ejecute también la opción 2. **Distribuya certificados para una conexión de base de datos segura**. • Póngase en contacto con el servicio de atención al cliente de Cisco si el error persiste.
cada nodo debe tener una entrada de dirección pública y privada	El archivo de configuración `install_SDBN.cfg` tiene una o más entradas de nodo que no tienen definidas una dirección IP pública y privada.	• Asegúrese de haber definido una dirección IP pública y privada para cada sección de configuración de Nodo de datos en `/lancope/database/install_SDBN.cfg`.
El archivo de almacenamiento secreto no existe O la contraseña no existe en el archivo. Inicie sesión en SMC y ejecute el script adecuado para establecer y	El script `install_SDBN_initial.py` ha detectado un problema al intentar recuperar las contraseñas de `dbadmin` y de	• Desde la CLI de SMC, ejecute el script `setup-sw-datastore-secure-connectivity` en `/lancope/admin/cds` y seleccione la opción **1. Distribuya la contraseña de SW DataStore a los appliances** para distribuir las contraseñas de dbadmin y de solo usuario. Después

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

distribuir las contraseñas de la base de datos.	`readonlyuser`.	de completar esto, si aún no lo ha hecho, ejecute también la opción 2. **Distribuya certificados para una conexión de base de datos segura**.
No se pudieron recuperar las contraseñas de la base de datos	El script `install_SDBN_initial.py` ha detectado un problema al intentar recuperar las contraseñas de `dbadmin` y de `readonlyuser`.	• Desde la CLI de SMC, ejecute el script `setup-sw-datastore-secure-connectivity` en `/lancope/admin/cds` y seleccione la opción **1. Distribuya la contraseña de SW DataStore a los appliances** para distribuir las contraseñas de dbadmin y de solo usuario. Después de completar esto, si aún no lo ha hecho, ejecute también la opción 2. **Distribuya certificados para una conexión de base de datos segura**.
Excepción de I/O al intentar leer el archivo	El script `install_SDBN_initial.py` ha detectado un problema al intentar recuperar las contraseñas de `dbadmin` y de `readonlyuser`.	• Póngase en contacto con el soporte de Cisco y proporcione el mensaje de error.
Una de las dos contraseñas no existe en el archivo. Inicie sesión en SMC y ejecute el script adecuado para establecer y distribuir las contraseñas de la	El script `install_SDBN_initial.py` ha detectado un problema al intentar recuperar las contraseñas de `dbadmin` y de	• Desde la CLI de SMC, ejecute el script `setup-sw-datastore-secure-connectivity` en `/lancope/admin/cds` y seleccione la opción **1. Distribuya la contraseña de SW DataStore a los appliances** para distribuir las contraseñas de dbadmin y de solo usuario. Después de completar esto, si aún no lo ha

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

base de datos.	`readonlyuser`.	hecho, ejecute también la opción 2. **Distribuya certificados para una conexión de base de datos segura**.
Se debe especificar la privateAddrs	El archivo de configuración `install_SDBN.cfg` tiene una o más entradas de nodo que no tiene una dirección IP privada definida.	• Asegúrese de haber definido una dirección IP privada para cada sección de configuración de Nodo de datos en `/lancope/database/install_SDBN.cfg`. Tenga en cuenta que Nodo de datos utiliza esta dirección IP no enrutable en `eth2` para comunicarse con otros Nodo de datos como parte de Almacén de datos.
publicAddrs debe especificarse	El archivo de configuración `install_SDBN.cfg` tiene una o más entradas de nodo que no tienen una dirección IP pública definida.	• Asegúrese de haber definido una dirección IP pública para cada sección de configuración de Nodo de datos en `/lancope/database/install_SDBN.cfg`. Tenga en cuenta que Nodo de datos utiliza esta dirección IP enrutable en `eth0` para comunicarse con otros appliances de Stealthwatch como parte de la implementación de su Stealthwatch.
publicSubnet debe especificarse	El archivo de configuración `install_SDBN.cfg` tiene una o más entradas de nodo que no tienen una subred definida.	• Asegúrese de que tiene una subred definida en la sección de configuración común en `/lancope/database/install_SDBN.cfg`. Tenga en cuenta que este subconjunto está asociado con las direcciones IP enrutables que se utilizan en `eth0` Nodos de datos para comunicarse con otros appliances de Stealthwatch como parte de la implementación de su Stealthwatch.
Excepción inesperada al leer	El script	• Ejecute el script `setup-sw-`

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

los secretos	`install_SDBN_initial.py` ha detectado un problema al intentar recuperar las contraseñas de `dbadmin` y de `readonlyuser`.	`datastore-secure-connectivity` en `/lancope/admin/cds` y seleccione la opción **1. Distribuya la contraseña de SW DataStore a los appliances** para distribuir las contraseñas de dbadmin y de solo usuario. Después de completar esto, si aún no lo ha hecho, ejecute también la opción 2. **Distribuya certificados para una conexión de base de datos segura**. • Póngase en contacto con el servicio de atención al cliente de Cisco si el error persiste.
Valor de retorno inesperado	El script `install_SDBN_initial.py` recibió un valor y se detuvo porque no pudo continuar.	• Póngase en contacto con el soporte de Cisco y proporcione el mensaje de error.

Actualice las contraseñas de Almacén de datos dbadmin y de readonlyuser después de la inicialización:

Si ya ha inicializado Almacén de datos, tal y como se describe en Inicialización y configuración del almacén de datos, y desea cambiar las contraseñas de `dbadmin` y `readonlyuser`, ejecute el script `setup-sw-datastore-secure-connectivity` de bash de conectividad segura. Después de proporcionar la contraseña de `dbadmin` actual, puede asignar nuevas contraseñas para `dbadmin` y `readonlyuser`. El script distribuye las credenciales actualizadas a sus appliances a través de SSH y actualiza las credenciales de la cuenta de usuario de `dbadmin` y `readonlyuser`.

Si ha perdido la contraseña de `dbadmin`, póngase en contacto con el servicio de asistencia de Cisco para obtener ayuda para recuperarla.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Cada contraseña debe cumplir los siguientes requisitos:

- al menos 1 número
- al menos 1 minúscula
- al menos 1 mayúscula
- al menos 1 carácter especial de la siguiente lista: `<>.,?/'"|:;`~!@#$%^&*()-_+={}[]`
- al menos 8 caracteres, no hay longitud máxima
- solo caracteres codificacos en ASCII

Tenga en cuenta que utiliza esta opción si ya ha inicializado Almacén de datos, Si está realizando una implementación y una configuración inicial de Almacén de datos, consulte Distribuir contraseñas del almacén de datos a los recopiladores de flujos, nodos de datos y SMC, para asignar contraseñas para `dbadmin` y `readonlyuser` y configurar valores de conexión seguros con la base de datos de Almacén de datos.

Si realizó una copia de seguridad de la base de datos de Almacén de datos y luego cambió la contraseña de `dbadmin`, actualice el archivo de contraseña de copia de seguridad de `pw.ini` con la nueva contraseña de `dbadmin`. Consulte Creación de una copia de seguridad del almacén de datos para obtener más información.

Antes de comenzar

- Compile una lista de contraseñas raíz para su SMC, Nodos de datos, colectores de flujos y SMC secundarios si implementó alguno.
- Active el acceso SSH y el acceso raíz SSH en su SMC, Nodos de datos y los recopiladores de flujo.

  > ⚠ Cuando SSH está habilitado, aumenta el riesgo de compromiso del sistema. Es importante habilitar SSH solo cuando lo necesite. Cuando haya terminado de usar SSH, deshabilítelo.

- Inicie sesión en su CLI de SMC como usuario raíz.

Procedimiento

1. Desde la línea de comandos, introduzca `cd/lancope/admin/cds` y pulse Intro para cambiar los directorios.
2. Introduzca `./setup-sw-datastore-secure-connectivity` y pulse Intro para ejecutar el script de bash de conectividad segura de Almacén de datos.
3. En el menú principal del script, seleccione **3. Actualice la contraseña de SW**

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

DataStore en los appliances.

4. Introduzca la contraseña actual de **dbadmin** y seleccione **Aceptar**.
5. En la línea de comandos, cuando se le pida la contraseña raíz de cada appliance, introduzca la contraseña y pulse Intro.

   > Ya que introduce varias contraseñas, asegúrese de que introduce la contraseña adecuada para ese appliance.

   Después de que introduzca las contraseñas raíz de todos los appliances, el script le pide las contraseñas de `dbadmin` y `readonlyuser`.
6. Introduzca la nueva contraseña de **dbadmin**.
7. Introduzca la misma contraseña de `dbadmin` en el campo de **dbadmin (confirmación)**.
8. Introduzca la contraseña de **readonlyuser**.
9. Introduzca la misma contraseña de `readonlyuser` en el campo de **readonlyuser (confirmación)**.

   > No introduzca la misma contraseña para `dbadmin` y `readonlyuser`. Asignar la misma contraseña hace que el script falle y no asigne contraseñas a ninguna cuenta de usuario.
10. Seleccione **Aceptar**.

    El script distribuye estas contraseñas de forma segura a sus appliances. Cuando finaliza, muestra una lista de los appliances actualizados.
11. Seleccione **Aceptar** para volver al menú principal del script.

Siguientes pasos

- Inicie sesión en VMC como `dbadmin`. Se le solicitará que actualice su contraseña.

  > Si no actualiza la contraseña para que coincida con la nueva contraseña de `dbadmin`, VMC no envía notificaciones de alerta de estado ni supervisa adecuadamente su Almacén de datos.

Resolución de problemas del script update_SDBN.py

El script `update_SDBN_initial.py` agrega Nodo de datos mensajes de registros en los archivos de registro de `/lancope/var/database/logs/db_update_[datestamp].log`. Puede consultarlos para obtener información adicional.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Mensajes de error generales de update_SDBN_initial.py

La siguiente tabla enumera los mensajes de error que pueden mostrarse si el script `update_SDBN_initial.py` detecta un error y las posibles soluciones al problema.

Mensaje de error	Descripción	Posibles soluciones
No se encontró el archivo de configuración o no hay secciones válidas	El script `update_SDBN.py` no puede localizar el archivo de configuración `update_SDBN.cfg` o los datos del archivo de configuración no tienen el formato esperado.	• Asegúrese de que tiene una copia de `update_SDBN.cfg` guardada en `/lancope/database/update_SDBN.cfg` en este Nodo de datos. • Asegúrese de que el formato de `update_SDBN.cfg` coincide con el formato de `update_SDBN_example.cfg`, de que asigna un nombre a cada sección de nodo en el `nodo#` de formato, de que ha definido una dirección IP pública y privada para cada sección de configuración de Nodo de datos, de que tiene una subred definida en la sección común y de que definió el primer nodo como uno más que el número total de nodos que ya hay en su Almacén de datos.
cada nodo debe tener una entrada de dirección pública y privada	El archivo de configuración `update_SDBN.cfg` tiene una o más entradas de nodo que no tienen definidas una dirección IP pública y privada.	• Asegúrese de haber definido una dirección IP pública y privada para cada sección de configuración de Nodo de datos en `/lancope/database/update_SDBN.cfg`.
No se pudo recuperar la	El script `update_`	• Asegúrese de que su appliance sea de la versión 7.3+.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

contraseña de dbadmin de la base de datos	`SDBN.py` no puede encontrar la contraseña de `dbadmin`.	• Ejecute el script `setup-sw-datastore-secure-connectivity` en `/lancope/admin/cds` y seleccione la opción **3. Actualice la contraseña de SW DataStore en los appliances** para establecer las contraseñas de `dbadmin` y `readonlyuser`. • Póngase en contacto con el servicio de atención al cliente de Cisco si el error persiste.
firstNode debe especificarse	El archivo de configuración `update_SDBN.cfg` no tiene un valor `firstNode` definido.	• Asegúrese de haber definido un valor firstNode en la sección de configuración común en `/lancope/database/update_SDBN.cfg`.
Se debe especificar la privateAddrs	El archivo de configuración `update_SDBN.cfg` tiene una o más entradas de nodo que no tienen una dirección IP privada definida.	• Asegúrese de haber definido una dirección IP privada para cada sección de configuración de Nodo de datos en `/lancope/database/update_SDBN.cfg`. Tenga en cuenta que Nodo de datos utiliza esta dirección IP no enrutable en `eth2` para comunicarse con otros Nodo de datos como parte de la base de datos de Almacén de datos.
publicAddrs debe especificarse	El archivo de configuración `update_SDBN.cfg` tiene una o más entradas de nodo que no tiene una dirección IP pública definida.	• Asegúrese de haber definido una dirección IP pública para cada sección de configuración de Nodo de datos en `/lancope/database/update_SDBN.cfg`. Tenga en cuenta que Nodo de datos utiliza esta dirección IP enrutable en `eth0` para comunicarse con otros appliances de Stealthwatch como parte de la implementación de su Stealthwatch.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

publicSubnet debe especificarse	El archivo de configuración `update_SDBN.cfg` tiene una o más entradas de nodo que no tienen una subred definida.	• Asegúrese de que tiene una subred definida en la sección de configuración común en `/lancope/database/update_SDBN.cfg`. Tenga en cuenta que este subconjunto está asociado con las direcciones IP enrutables que se utilizan en `eth0` Nodos de datos para comunicarse con otros appliances de Stealthwatch como parte de la implementación de su Stealthwatch.

Resolución de problemas de la consola de administración de Vertica

Si su instancia de VMC no se actualiza automáticamente en su navegador web, es posible que tenga que actualizarla manualmente para ver los cambios en su Almacén de datos o cambios de configuración.

Almacén de datos Resolución de problemas

Tenga en cuenta que Almacén de datos reserva hasta el 40 % del espacio de almacenamiento disponible para mantener el Almacén de datos. Como mínimo, el 60 % del espacio total está disponible para el almacenamiento de flujo.

Vertica Analytics Platform no se reinicia automáticamente después de que un nodo de datos pierda energía y se reinicie

Si Nodo de datos pierde la alimentación inesperadamente y reinicia el appliance, la instancia de Vertica Analytics Platform (Vertica) que Nodo de datos no se puede reiniciar automáticamente, debido a posibles datos dañados. Si aún hay suficientes Nodo de datos en ejecución para permitir que Almacén de datos se siga ejecutando, Almacén de datos continúa ingiriendo datos desde los recopiladores de flujo. Sin embargo, debe reiniciar Nodo de datos lo antes posible para que pueda volver a unirse a Almacén de datos, recuperar los datos perdidos de Nodo de datos adyacentes y ponerse al día con el resto de Nodo de datos.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

En esta situación, inicie sesión en Nodo de datos y fuerce un reinicio manual de Vertica, que elimina los datos dañados y permite que Vertica se reinicie correctamente.

Además, es posible que tenga que actualizar la política de restauración de energía antes de que Nodo de datos se reinicie. Si la política de restauración de energía está establecida en Apagar, debe reiniciar manualmente Nodo de datos después de una pérdida de energía. Consulte la Guía de configuración de la GUI del UCS Serie C para obtener más información sobre la configuración de la política de restauración de energía en CIMC.

Antes de comenzar

- Inicie sesión en CLI de Nodo de datos como raíz.

Procedimiento

1. Copie el siguiente comando y péguelo en un editor de texto:

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

2. Sustituya *[node_name]* por el nombre de su Nodo de datos (por ejemplo, `nodo0001`).
3. Copie el comando actualizado y péguelo en la CLI y, a continuación, presione Intro para revisar las entradas más recientes en el archivo de error `ErrorReport.txt`. Si el mensaje de error detecta posibles problemas de consistencia o corrupción de datos, continúe con el siguiente paso para forzar el reinicio de Vertica.
4. Copie el siguiente comando y péguelo en un editor de texto:

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

5. Sustituya *[data-node-ip-address]* con su dirección IP de Nodo de datos afectada.
6. Sustituya *[dbadmin-password]* con su contraseña Almacén de datos `dbadmin`.
7. Copie el comando actualizado y péguelo en la CLI y, a continuación, presione Intro para forzar el reinicio de Vertica en sus Nodo de datos afectados. Vertica elimina todos los datos dañados y los recupera de los Nodo de datos adyacentes.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

8. Si el sistema le avisa con `¿Desea seguir esperando? (sí/no) [sí]`, introduzca `sí` y pulse Intro para seguir esperando.

   Debido a que Vertica restaura la información del Nodo de datos afectado de los Nodo de datos adyacentes, si estos Nodo de datos ingieren una gran cantidad de tráfico mientras el Nodo de datos afectado está inactivo, el Nodo de datos afectado puede tardar un tiempo en recuperarse.

Siguientes pasos

- Revise las recomendaciones de Cisco para el suministro de energía a su Nodo de datos en Requisitos y consideraciones sobre la implementación del almacén de datos.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Apéndice A. Preparación para la instalación

Advertencias de instalación

Lea el documento Información de seguridad normativa y de cumplimiento antes de instalar los Stealthwatch Almacén de datos appliances.

Tome nota de las siguientes advertencias:

Declaración 1071: Definición de advertencia

INSTRUCCIONES DE SEGURIDAD IMPORTANTES

⚠ Este símbolo de advertencia significa peligro. Se encuentra en una situación que podría causar lesiones corporales. Antes de manipular cualquier equipo, debe ser consciente de los peligros que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. Utilice el número de advertencia que aparece al final de cada una para localizar su traducción en las advertencias de seguridad que acompañan a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Declaración 1005: Interruptor de circuito

⚠ Este producto utiliza el sistema de protección contra cortocircuitos (sobretensión) instalado en el edificio. Asegúrese de que el dispositivo de protección no sea superior a: EU: 250 V, 16 A (EE. UU.: 120, 15 A)

Declaración 1004: Instrucciones de instalación

⚠ Lea las instrucciones de instalación antes de usar, instalar o conectar el sistema al suministro eléctrico.

Declaración 12: Advertencia de desconexión de la fuente de alimentación

⚠ Antes de trabajar en un chasis o cerca de fuentes de alimentación, desconecte el cable de alimentación de las unidades de CA; desconecte la alimentación de las unidades de CC en el interruptor de circuitos.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Declaración 43: Advertencia de eliminación de joyería

Antes de comenzar a trabajar con el equipo conectado a las líneas de alimentación, quítese las joyas (incluidos anillos, collares y relojes). Los objetos metálicos se calientan cuando están conectados a una fuente de alimentación y a tierra, y pueden provocar quemaduras graves o que el objeto metálico se suelde a los terminales.

Declaración 94: Advertencia de correa de muñeca

Durante este procedimiento, utilice correas de muñecas para evitar daños por descarga electrostática en la tarjeta. No toque directamente la placa base con la mano o cualquier herramienta metálica o podría electrocutarse.

Declaración 1045: Protección contra cortocircuitos

Este producto necesita protección contra cortocircuitos (sobretensión) que se suministra como parte de la instalación del edificio. Instale solo conforme a las normativas de cableado locales y nacionales.

Declaración 1021: Circuito SELV

Para evitar descargas eléctricas, no conecte circuitos de seguridad de muy baja tensión (SELV) a circuitos de la red de telecomunicaciones (TNV). Los puertos LAN contienen circuitos SELV, mientras que los puertos WAN tienen circuitos TNV. Algunos puertos, tanto LAN como WAN, utilizan conectores RJ-45. Tenga cuidado al conectar los cables.

Declaración 1024: Conductor de conexión a tierra

Este equipo debe estar conectado a tierra. No desactive nunca el conductor de puesta a tierra ni utilice el equipo sin un conductor de puesta a tierra correctamente instalado. Póngase en contacto con la autoridad de inspección eléctrica pertinente o con un electricista si no está seguro de contar con una conexión a tierra apropiada.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Declaración 1040: Desechar el producto

Al desechar este producto, deben tenerse en cuenta todas las leyes y normativas nacionales.

Declaración 1074: Cumplimiento con los códigos eléctricos locales y nacionales

La instalación del equipo debe cumplir con los códigos eléctricos locales y nacionales.

Declaración 19: Advertencia de alimentación de red de telecomunicaciones

El dispositivo ha sido diseñado para trabajar con sistemas de alimentación de red de telecomunicaciones.

Instrucciones de instalación

Tome nota de las siguientes advertencias:

Declaración 1047: Prevención de sobrecalentamiento

Para evitar que el sistema se sobrecaliente, no lo utilice en una zona que supere la temperatura ambiente máxima recomendada de: 5 a 35 °C (41 a 95 °F)

Declaración 1019: Dispositivo de desconexión principal

La combinación de la caja de enchufe debe estar siempre accesible porque sirve como dispositivo de desconexión principal.

Declaración 1005: Interruptor de circuito

Este producto utiliza el sistema de protección contra cortocircuitos (sobretensión) instalado en el edificio. Asegúrese de que el dispositivo de protección no sea superior a: EU: 250 V, 16 A (EE.UU.: 120, 15 A)

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Declaración 1074: Cumplimiento con los códigos eléctricos locales y nacionales

La instalación del equipo debe cumplir con los códigos eléctricos locales y nacionales.

Declaración 371: Cable de alimentación y adaptador de corriente alterna

Utilice los cables de conexión / cables de alimentación / baterías / adaptadores de corriente alterna proporcionados o designados cuando instale el producto. Usar cualquier otro cable o adaptador podría provocar un error o un incendio. La ley de seguridad de aparatos y materiales eléctricos prohíbe el uso de cables con la certificación UL (aquellos que lleven las marcas “UL” o “CSA” en el cable), que no estén sujetos a dicha ley y por la cual debe figurar “PSE” en el cable, en ningún dispositivo eléctrico que no sean los productos designados por CISCO.

Declaración 1073: No hay piezas de mantenimiento para el usuario

No hay piezas de mantenimiento para el usuario en el interior. No abrir.

Cuando instale un chasis, utilice las siguientes directrices:

- Asegúrese de que hay un espacio adecuado alrededor del chasis para permitir el mantenimiento y un flujo de aire adecuado. El flujo de aire en el chasis va desde la parte frontal a la trasera.

  Para asegurar el flujo de aire adecuado es necesario asegurar su chasis con un kit de raíles. La colocación física de las unidades una encima de otra o el apilamiento sin el uso de los kit de raíles bloquea las ranuras de ventilación encima del chasis, lo que podría dar como resultado sobrecalentamiento, velocidades del ventilador más altas y un mayor consumo energético. Le recomendamos que monte su chasis en los kit de raíles cuando los instale en el rack, ya que estos raíles ofrecen el espaciado mínimo necesario entre los chasis. No se necesita un espaciado adicional entre el chasis cuando los monte utilizando kit de raíles.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

- Asegúrese de que el aire acondicionado puede mantener el chasis a una temperatura de 5 a 35 °C (41 a 95 °F).
- Asegúrese de que el armario o rack cumple con los requisitos del rack.
- Asegúrese de que la alimentación del sitio cumple con los requisitos de alimentación que aparecen en la hoja de especificaciones para su appliance. Si está disponible, puede utilizar un UPS para protegerse frente a fallos de alimentación.

> Evite las UPS que utilizan la tecnología ferrorresonante. Este tipo de UPS pueden volverse inestables con estos sistemas, que pueden tener importantes fluctuaciones de toma de corriente de patrones de trafico de datos fluctuantes.

Recomendaciones de seguridad

La siguiente información le ayuda a garantizar su seguridad y a proteger el chasis. Puede que esta información no sea aplicable a todas las situaciones potencialmente peligrosas de su entorno de trabajo, así que esté atento y siga siempre un buen criterio.

Tenga en cuenta estas directrices de seguridad:

- Mantenga el área limpia y sin polvo antes, durante y después de la instalación.
- Mantenga las herramientas fuera de las zonas de paso donde usted u otras personas podrían tropezarse.
- No lleve ropa holgada ni joyas como pendientes, pulseras o cadenas que puedan engancharse en el chasis.
- Utilice gafas de seguridad si trabaja en cualquier condición que pueda ser peligrosa para sus ojos.
- No realice ninguna acción que pueda resultar potencialmente peligrosa para las personas o que haga que el equipo no sea seguro.
- Nunca intente levantar un objeto demasiado pesado para una sola persona.

Mantener la seguridad con electricidad

> Antes de trabajar en un chasis, asegúrese de que el cable de alimentación está desconectado.

Siga estas directrices cuando trabaje con equipo eléctrico:

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

- No trabaje solo si hay condiciones potencialmente peligrosas en su espacio de trabajo.
- Nunca dé por hecho que la alimentación está desconectada, compruébelo siempre.
- Busque cuidadosamente posibles riesgos en su zona de trabajo como suelos húmedos, cables de alimentación de prolongación sin conexión a tierra, cables de alimentación desgastados y la falta de conexiones a tierra de seguridad.
- Si se produce un accidente eléctrico:
    - Tenga precaución, no se perjudique a usted mismo.
    - Desconecte la alimentación del sistema.
    - Si es posible, envíe a otra persona para conseguir asistencia médica. Si no, evalúe el estado de la víctima y, a continuación, pida ayuda.
    - Determine si el accidentado necesita respiración boca a boca o masaje cardíaco y, a continuación, realice la acción apropiada.
- Utilice el chasis según las especificaciones eléctricas y las instrucciones de uso del producto.

Evite daños por ESD

La ESD se produce cuando se manejan de manera incorrecta los componentes electrónicos y puede dañar el equipo y afectar al circuito eléctrico, lo que puede dar lugar a un fallo intermitente o completo de su equipo.

Siga siempre los procedimientos de prevención de ESD cuando retire y sustituya componentes. Asegúrese de que el chasis esté eléctricamente conectado a tierra. Utilice una correa para la muñeca antiestática y asegúrese de que está en contacto con su piel. Conecte la pinza de toma a tierra a una zona sin pintura del marco del chasis para conectar a tierra de forma segura los voltajes de ESD. Para protegerse de manera adecuada frente a daños y descargas causadas por ESD, tanto la correa para la muñeca como el cable deben funcionar correctamente. Si no hay una correa de muñeca disponible, establezca una conexión a tierra usted mismo tocando una parte metálica del chasis.

Por su seguridad, compruebe periódicamente el valor de resistencia de la correa antiestática, que debe estar entre 1 y 10 megaohmios.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Entorno del sitio

Para evitar fallos en el equipo y reducir la posibilidad de que se apague por el entorno, planifique el diseño del sitio y la ubicación del equipo con cuidado. Si su equipo actual se apaga o experimenta tasas de error inusualmente altas, estas consideraciones pueden ayudarle a aislar la causa de los fallos y evitar futuros problemas.

Consideraciones de la fuente de alimentación

Al instalar el chasis, tenga en cuenta lo siguiente:

- Compruebe la alimentación en el sitio antes de instalar el chasis para garantizar que no tenga picos ni ruido. Instale un acondicionador de potencia si es necesario para asegurarse de utilizar niveles de tensión y potencia adecuados en la tensión de entrada del appliance.
- Instale una conexión a tierra adecuada para el sitio para evitar daños por rayos y subidas de potencia.
- El chasis no cuenta con un rango de funcionamiento seleccionable por el usuario. Consulte la etiqueta del chasis para conocer los requisitos de potencia de entrada correctos del appliance.
- Hay disponibles varios tipos de cables de alimentación de entrada de CA para el appliance, asegúrese de utilizar el adecuado para su sitio.
- Si utiliza fuentes de alimentación redundantes (1+1) dobles, le recomendamos que use circuitos eléctricos independientes para cada fuente de alimentación.
- Instale una fuente de alimentación continua para su sitio si es posible.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Consideraciones sobre la configuración en rack

Tenga en cuenta lo siguiente durante la planificación de la configuración en rack:

- Si monta un chasis en un rack abierto, asegúrese de que el marco del rack no bloquee los puertos de entrada o salida.
- Asegúrese de que los racks encerrados dispongan de una ventilación adecuada. Asegúrese de que el rack no se congestione excesivamente, puesto que cada chasis genera calor. Un rack encerrado debe tener laterales de ventilación y un ventilador que proporcione aire de refrigeración.
- En un rack encerrado con un ventilador de ventilación en la parte superior, el calor generado por el equipo que está cerca de la parte inferior del rack puede dirigirse hacia arriba y por los puertos de entrada del equipo de encima en el rack. Asegúrese de que se proporcione una ventilación adecuada al equipo de la parte inferior del rack.
- Los deflectores pueden ayudar a aislar el aire de salida del aire de entrada, lo cual también ayuda a guiar el aire de refrigeración en su paso por el chasis. La mejor ubicación de los deflectores depende de los patrones del flujo de aire en el rack. Pruebe diferentes disposiciones para colocar los deflectores de forma eficaz.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Apéndice B. Instalación del hardware de Stealthwatch

Este apartado abarca la instalación de sus appliances en su entorno. Incluye:

- **Montaje de su appliance**
- **Conectar su appliance a la red**
- **Conectarse a su appliance**
- **Configurar los ajustes de red mediante la Configuración de primera vez**

Montaje de su appliance

Puede montar appliances de Stealthwatch directamente en un rack o armario estándar de 19", cualquier otro armario adecuado o en una superficie plana. Al montar un appliance en un rack o en un armario, siga las instrucciones que se incluyen en los kits de montaje en raíles. Al determinar dónde colocar un appliance, asegúrese de que la separación en los paneles frontales y traseros es la siguiente:

- Los indicadores del panel frontal se pueden leer con facilidad
- El acceso a los puertos en el panel trasero es suficiente para conectar el cableado sin restricciones
- La entrada de alimentación del panel trasero está al alcance de una fuente de alimentación de CA acondicionada.
- El flujo de aire en torno al appliance y a través de los orificios de ventilación no se encuentra obstaculizado.

Hardware incluido en el appliance

El siguiente hardware se incluye en appliances de Stealthwatch:

- Cable de alimentación de CA
- Llaves de acceso (para la placa frontal)
- Kit de raíles para el montaje en rack o agarraderas de montaje para appliances más pequeños
- Un cable SFP de 10 GB para el recopilador de flujo 5210

Hardware adicional necesario

Debe proporcionar el siguiente hardware adicional necesario:

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

- Tornillo de montaje para un rack estándar de 19"
- Fuente de alimentación ininterrumpida (UPS) para cada appliance que instale
- Para configurar de forma local (opcional), utilice uno de los siguientes métodos:
  - Un ordenador portátil con un cable de vídeo y un cable USB (para el teclado)
  - Un monitor de vídeo con un cable de vídeo y un teclado con un cable USB

Conectar su appliance a la red

Utilice el mismo procedimiento para conectar cada appliance a la red. La única diferencia para la conexión es el tipo de appliance que tiene.

> ⚠ No actualice la BIOS del appliance, ya que puede provocar problemas con la funcionalidad del appliance.

Para obtener información detallada sobre las especificaciones de cada appliance, consulte las hojas de especificaciones de Stealthwatch.

> ℹ Todo el hardware de Cisco x2xx utiliza la misma plataforma de UCS, UCSC-C220-M5SX, excepto en el caso del recopilador de flujo de 5120 DB, que utiliza UCSC-C240-M5SX. Las variaciones en los appliances se encuentran en las tarjetas NIC, el procesador, la memoria, el almacenamiento y RAID.

> ℹ El recopilador de flujo 5210 consta de dos servidores conectados (motor y base de datos) para que funcionen como un solo appliance. Por este motivo, la instalación cambia ligeramente respecto a otros appliances. En primer lugar, conéctelos directamente mediante un cable cruzado de 10 G SFP+ de conexión directa. A continuación, conéctese a la red.

Para conectar su appliance a su red:

1. Conecte un cable de Ethernet al puerto de gestión, en la parte trasera del appliance.
2. Conecte al menos un puerto de supervisión para el sensor de flujo y los UDP Director.

   Para la HA de UDP Director, conecte los dos UDP Director mediante cables cruzados. Conecte el puerto eth2 de un UDP Director al puerto eth2 del segundo UDP Director. De manera similar, conecte el puerto de eth3 de cada UDP Director con un segundo cable cruzado. Puede ser el cable de fibra o de cobre.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Asegúrese de tener en cuenta la etiqueta de Ethernet (eth2, eth3, etc.) para cada puerto. Estas etiquetas corresponden a las interfaces de red (eth2, eth3, etc.) que se muestran y se pueden configurar en la página de inicio de la interfaz de administración del appliance.

3. Conecte el otro extremo de los cables Ethernet a su switch de red.
4. Conecte los cables de alimentación a la fuente de alimentación. Algunos appliances tienen dos conexiones de alimentación: fuente de alimentación 1 y fuente de alimentación 2.

Conectarse a su appliance

Esta sección describe cómo conectarse a su appliance para cambiar las contraseñas predeterminadas del usuario.

Puede conectarse al appliance en uno de estos dos modos:

- con un teclado y un monitor
- con un ordenador portátil (y un emulador del terminal)

El SSH está desactivado para los nuevos appliances. Debe iniciar sesión en la interfaz web de administración del appliance para activarlo.

Conexión con un teclado y un monitor

Para configurar la dirección IP de forma local, siga estos pasos:

1. Conecte el cable de alimentación al appliance.
2. Pulse el botón de alimentación para encender el appliance. Espere a que haya terminado de arrancar por completo. No interrumpa el proceso de arranque.

> Puede que tenga que quitar el panel frontal para que llegue la alimentación.
>
> Los ventiladores de la fuente de alimentación se conectan en algunos modelos cuando el sistema no está encendido. Compruebe que el LED en el panel frontal está encendido.
>
> Asegúrese de conectar el appliance a una fuente de alimentación ininterrumpida (UPS). La fuente de alimentación precisa alimentación o de lo contrario el sistema mostrará un error.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

3. Conecte el teclado:
   - Si dispone de un teclado estándar, conéctelo al conector estándar de teclado.
   - Si dispone de un teclado USB, conéctelo a un conector USB.
4. Conecte el cable de vídeo al conector de vídeo. Aparecerá la indicación de inicio de sesión.
5. Continúe con la sección **Configurar los ajustes de red mediante la Configuración de primera vez**.

Conexión con un ordenador portátil

También puede conectarse al appliance con un ordenador portátil que tenga un emulador del terminal.

Para conectarse a un appliance con un ordenador portátil:

1. Conecte su ordenador portátil al appliance utilizando uno de los siguientes métodos:
   - Conecte un cable RS232 del conector de puertos en serie (DB8) en su ordenador portátil al puerto de consola en el appliance.
   - Conecte un cable cruzado del puerto Ethernet en su ordenador portátil al puerto de gestión en el appliance.
2. Conecte el cable de alimentación al appliance.
3. Pulse el botón de alimentación para encender el appliance. Espere a que haya terminado de arrancar por completo. No interrumpa el proceso de arranque.

   > Puede que tenga que quitar el panel frontal para que llegue la alimentación.
   >
   > Los ventiladores de la fuente de alimentación se conectan en algunos modelos cuando el sistema no está encendido. Compruebe que el LED en el panel frontal está encendido. Asegúrese de conectar el appliance a una fuente de alimentación ininterrumpida (UPS). La fuente de alimentación precisa alimentación o de lo contrario el sistema mostrará un error.

4. En el ordenador portátil, establezca una conexión con el appliance.

   Puede utilizar cualquier emulador del terminal para comunicarse con el appliance.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

5. Aplique los siguientes ajustes:

   - BPS: 115200
   - Bits de datos: 8
   - Bit de parada: 1
   - Paridad: ninguna
   - Control de flujo: ninguno

   Se muestran la pantalla y la indicación de inicio de sesión.

6. Continúe con la siguiente sección, **Configurar los ajustes de red mediante la Configuración de primera vez**.

Configurar los ajustes de red mediante la Configuración de primera vez

Después de conectarse al dispositivo, utilice Configuración de primera vez para configurar los ajustes de red, incluidas las direcciones IP. Tenga en cuenta lo siguiente:

- Si implementa SMC 2210 o Recopilador de flujo 4210 con un Almacén de datos, además de configurar las direcciones IP, también puede configurar SMC o Recopilador de flujo para Almacén de datos su uso y el tipo de puerto físico que utiliza para el puerto de administración `eth0`.

  > ⚠ Después de elegir configurar SMC o Recopilador de flujo para usarlo con un Almacén de datos, no puede actualizar la configuración del appliance para cambiar esto. Debe seleccionar el dispositivo con RFD si selecciona una opción incorrecta. Active esta opción solo si tiene previsto implementar un Almacén de datos en la red.

- Si su appliance es un Nodo de datos, puede configurar el tipo de puerto físico que utiliza para el puerto de administración `eth0` y la dirección IP e información relacionada para el canal del puerto `eth2` o `eth2`/`eth3` para las comunicaciones Nodo de datos.

Consulte la Guía de instalación y configuración de hardware del clúster del almacén de datos para obtener más información sobre la instalación de SMC 2210, FC 4210 y los appliances Nodo de datos.

Después de que haya configurado las direcciones IP, cambie las contraseñas del usuario.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

> La primera vez que introduzca la Configuración del sistema, se iniciará el asistente de primera configuración y le guiará a través de la configuración inicial del appliance. Si sale de la configuración de primera vez antes de completar el asistente, la próxima vez que entre en la configuración del sistema, el asistente de configuración de primera vez se iniciará de nuevo.

En función de cuál sea su appliance, vaya a la siguiente sección:

- **Almacén de datos Appliances compatibles (SMC 2210, FC 4210)**
- **Configuración general de appliances de Stealthwatch**
- **Nodo de datos Configuración**

Configuración general de appliances de Stealthwatch

Para todos los appliances, excepto para Nodo de datos, SMC 2210 y FC 4210, el asistente de primera configuración muestra la siguiente configuración:

- Configure la dirección IP del appliance y la información de administración

Configure la dirección IP del appliance y la información de administración:

Puede configurar la dirección IP de administración de eth0 de su dispositivo y la información relacionada en Configuración de primera vez. Para la mayoría de los dispositivos, esta es la primera configuración en Configuración de primera vez.

Antes de comenzar

- Si está configurando un Nodo de datos, vaya a Configuración de nodo de datos.
- Si está configurando una SMC o un recopilador de flujo compatible con Almacén de datos, vaya a Appliances compatibles con el almacén de datos (SMC 2210, FC 4210).
- Si está configurando cualquier otro appliance Stealthwatch, comience con el paso 1.

Procedimiento

1. Inicie sesión en el programa de configuración del sistema:
    - Si está configurando un appliance compatible con Nodo de datos o Almacén de datos, escriba `root` y, a continuación, pulse **Entrar**. Si está configurando

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

cualquier otro appliance, escriba `sysadmin` y, a continuación, pulse **Entrar**.

> Se necesitan permisos de `root` para configurar correctamente la compatibilidad de Almacén de datos y Almacén de datos.

- Cuando aparezca la indicación de la contraseña, escriba **lan1cope** y, a continuación, pulse **Intro**.
- En la siguiente indicación escriba **SystemConfig** y, a continuación, pulse **Intro**.

2. Si es la primera vez que introduce la configuración del sistema en este dispositivo, se iniciará la configuración de primera vez.

   Se abrirá el menú de configuración de sistema. Seleccione **Management** (Gestión) y, a continuación, pulse **Intro**.
3. Introduzca una **dirección IP** para este appliance.
4. Introduzca una **Netmask** para la red.
5. Introduzca una dirección de **gateway** para la dirección IP de este appliance.
6. Introduzca una dirección de **difusión** para el appliance.
7. Introduzca un **nombre de host** para su appliance.
8. Introduzca un **dominio** para su dispositivo.
9. Seleccione **Seleccionar** y, a continuación, **Sí** para confirmar sus entradas.

   Esta es la última opción de configuración en Configuración de primera vez. El appliance se reinicia e implementa los cambios. Una vez que se complete, se abre la página de inicio de sesión.

Siguientes pasos

- Cambiar las contraseñas del usuario. Consulte **Cambio de la contraseña del usuario del administrador de sistemas** para obtener más información.

Almacén de datos Appliances compatibles (SMC 2210, FC 4210)

Para SMC 2210 y FC 4210, la configuración de primera vez muestra la siguiente configuración:

1. Configure el puerto físico de administración de eth0
2. Configure la dirección IP del appliance y la información de administración
3. Configurar la compatibilidad del almacén de datos

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Configure el puerto físico de administración de eth0

Si configura una SMC o un recopilador de flujo que sea compatible con Almacén de datos e implementa un Almacén de datos, puede configurar `eth0` como puerto SFP+ DAC, en lugar del puerto de cobre BASE-T predeterminado. Para estos appliances, esta es la primera configuración en Configuración de primera vez.

Antes de comenzar

- Si está configurando un Nodo de datos, SMC o Flow Collector compatible con Almacén de datos, consulte la hoja de especificaciones de Stealthwatch de su appliance para obtener información sobre los puertos SFP + y BASE-T compatibles.
- Si está configurando un Nodo de datos, vaya a Configuración de nodo de datos.
- Si está configurando cualquier otro appliance Stealthwatch además de appliances compatibles con Almacén de datos, consulte Configuración general de appliances de Stealthwatch.

Procedimiento

1. Inicie sesión en el programa de configuración del sistema:
   - Escriba **root**y, a continuación, pulse **Intro**.

     > Se necesitan permisos de `root` para configurar correctamente la compatibilidad de Almacén de datos.

   - Cuando aparezca la indicación de la contraseña, escriba **lan1cope** y, a continuación, pulse **Intro**.
   - En la siguiente indicación escriba **SystemConfig** y, a continuación, pulse **Intro**.
2. Si es la primera vez que introduce la configuración del sistema en este dispositivo, se iniciará la configuración de primera vez y se mostrará la configuración del pedido de puertos. Vaya al paso 5.

   Se abrirá el menú de configuración de sistema. Seleccione **Management** (Gestión) y, a continuación, pulse **Intro**.
3. En el menú System Configuration (Configuración del sistema), seleccione **Network** y, a continuación, pulse **Intro**.
4. Seleccione **Orden de los puertos** y pulse Intro.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

5. Tiene las siguientes opciones:
    - Seleccione **LOM** para configurar su appliance para utilizar un puerto de cobre BASE-T para eth0.
    - Seleccione **SFP +** para configurar su appliance para que utilice un puerto de fibra SFP + para eth0.
6. Seleccione **Aceptar** para confirmar su selección.

Siguientes pasos

- Configure la dirección IP y la información de gestión del puerto de administración eth0. Consulte el siguiente procedimiento.

Configure la dirección IP del appliance y la información de administración:

Puede configurar la dirección IP de administración de eth0 de su dispositivo y la información relacionada en Configuración de primera vez. Para appliances compatibles con Almacén de datos, esta configuración se produce después de configurar el puerto físico de administración eth0.

Antes de comenzar

- Si está configurando una SMC o un recopilador de flujo compatible con Almacén de datos, después de configurar el orden de los puertos, el asistente de primera configuración muestra la configuración de gestión de `eth0`. Vaya al paso 3.

Procedimiento

1. Inicie sesión en el programa de configuración del sistema:
    - Si está configurando un appliance compatible con Almacén de datos, escriba `root` y, a continuación, pulse **Entrar**.

      > Se necesitan permisos de `root` para configurar correctamente la compatibilidad de Almacén de datos y Almacén de datos.

    - Cuando aparezca la indicación de la contraseña, escriba **lan1cope** y, a continuación, pulse **Intro**.
    - En la siguiente indicación escriba **SystemConfig** y, a continuación, pulse **Intro**.
2. Si es la primera vez que introduce la configuración del sistema en este dispositivo,

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

se iniciará la configuración de primera vez.

Se abrirá el menú de configuración de sistema. Seleccione **Management** (Gestión) y, a continuación, pulse **Intro**.

3. Introduzca una **dirección IP** para este appliance.
4. Introduzca una **Netmask** para la red.
5. Introduzca una dirección de **gateway** para la dirección IP de este appliance.
6. Introduzca una dirección de **difusión** para el appliance.
7. Introduzca un **nombre de host** para su appliance.
8. Introduzca un **dominio** para su dispositivo.
9. Seleccione **Seleccionar** y, a continuación, **Sí** para confirmar sus entradas.

Siguientes pasos

- Configure el appliance para su uso sin un Almacén de datos. Consulte el siguiente procedimiento para obtener más información.

Configurar el uso del almacén de datos

Configure su SMC 2210 o FC 4210 para que funcione con un Almacén de datos. Sus Recopilador de flujo se conectarán al Almacén de datos y su SMC consultará el Almacén de datos.

> ⚠ Después de elegir configurar SMC o Recopilador de flujo para usarlo con un Almacén de datos, no puede actualizar la configuración del appliance para cambiar esto. Debe seleccionar el dispositivo con RFD si selecciona una opción incorrecta. Active esta opción **solo si** tiene previsto implementar un Almacén de datos en la red.

> ℹ Debe configurar todos sus SMC y recopiladores de flujo para utilizarlos con un Almacén de datos si implementa un Almacén de datos. No puede configurar algunos de los recopiladores de flujo para conectarse al Almacén de datos y otros para conectarse directamente al SMC.

Antes de comenzar

- Si se encuentra en la configuración de primera vez, la configuración del sistema muestra la configuración del almacén de datos después de que termine de configurar la dirección IP del appliance. Vaya al paso 3.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Procedimiento

1. Menú de configuración de sistema. Seleccione **Advanced** (Avanzada) y, a continuación, pulse **Enter**.
2. Seleccione **Data Store** (Almacén de datos) y, a continuación, pulse Enter.
3. Seleccione **Sí** para configurar su appliance para que sea compatible con un Almacén de datos.

   > ⚠ Después de elegir configurar SMC o Recopilador de flujo para usarlo con un Almacén de datos, no puede actualizar la configuración del appliance para cambiar esto. Debe seleccionar el dispositivo con RFD si selecciona una opción incorrecta. Active esta opción **solo si** tiene previsto implementar un Almacén de datos en la red.

4. Seleccione **Aceptar** para confirmar su selección.

   Esta es la última opción de configuración en Configuración de primera vez. El appliance se reinicia e implementa los cambios. Una vez que se complete, se abre la página de inicio de sesión.

Siguientes pasos

- Cambiar las contraseñas del usuario. Consulte **Cambio de la contraseña del usuario del administrador de sistemas** para obtener más información.

Nodo de datos Configuración

Para Nodo de datos, la Configuración de primera vez muestra la siguiente configuración:

1. Configure el puerto físico de administración de eth0
2. Configure la dirección IP del appliance y la información de administración
3. Configurar eth2 y eth3 para comunicaciones entre Nodo de datos

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Configure el puerto físico de administración de eth0

Si configura un Nodo de datos, puede configurar `eth0` como puerto de cobre BASE-T, en lugar del puerto SFP+ DAC predeterminado. Para estos appliances, esta es la primera configuración en Configuración de primera vez.

Antes de comenzar

- Si está configurando un Nodo de datos, consulte la hoja de especificaciones de Stealthwatch de su appliance para obtener información sobre los puertos SFP+ y BASE-T compatibles.
- Si está configurando una SMC o un recopilador de flujo compatible con Almacén de datos, vaya a Appliances compatibles con el almacén de datos (SMC 2210, FC 4210).
- Si está configurando cualquier otro appliance Stealthwatch además de appliances compatibles con Almacén de datos, consulte Configuración general de appliances de Stealthwatch.

Procedimiento

1. Inicie sesión en el programa de configuración del sistema:
   - Escriba **root**y, a continuación, pulse **Intro**.

     > Se necesitan permisos de `root` para configurar correctamente la compatibilidad de Almacén de datos.

   - Cuando aparezca la indicación de la contraseña, escriba **lan1cope** y, a continuación, pulse **Intro**.
   - En la siguiente indicación escriba **SystemConfig** y, a continuación, pulse **Intro**.
2. Si es la primera vez que introduce la configuración del sistema en este dispositivo, se iniciará la configuración de primera vez y se mostrará la configuración del pedido de puertos. Vaya al paso 5.

   Se abrirá el menú de configuración de sistema. Seleccione **Management** (Gestión) y, a continuación, pulse **Intro**.
3. En el menú System Configuration (Configuración del sistema), seleccione **Network** y, a continuación, pulse **Intro**.
4. Seleccione **Orden de los puertos** y pulse Intro.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

5. Tiene las siguientes opciones:
    - Seleccione **SFP +** para configurar su appliance para que utilice un puerto de fibra SFP + para eth0.
    - Seleccione **LOM** para configurar su appliance para utilizar un puerto de cobre BASE-T para eth0.
6. Seleccione **Aceptar** para confirmar su selección.

Siguientes pasos

- Configure la dirección IP y la información de gestión del puerto de administración eth0. Consulte el siguiente procedimiento.

Configure la dirección IP del appliance y la información de administración:

Puede configurar la dirección IP de administración de eth0 de su dispositivo y la información relacionada en Configuración de primera vez.

Antes de comenzar

- Si está configurando un Nodo de datos, después de configurar el orden de los puertos, el asistente de primera configuración muestra la configuración de gestión de `eth0`. Vaya al paso 3.

Procedimiento

1. Inicie sesión en el programa de configuración del sistema:
    - Si está configurando un Nodo de datos, escriba `root` y, a continuación, pulse **Entrar**.

      > Se necesitan permisos de `root` para configurar correctamente la compatibilidad de Almacén de datos y Almacén de datos.

    - Cuando aparezca la indicación de la contraseña, escriba **lan1cope** y, a continuación, pulse **Intro**.
    - En la siguiente indicación escriba **SystemConfig** y, a continuación, pulse **Intro**.
2. Si es la primera vez que introduce la configuración del sistema en este dispositivo, se iniciará la configuración de primera vez.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Se abrirá el menú de configuración de sistema. Seleccione **Management** (Gestión) y, a continuación, pulse **Intro**.

3. Introduzca una **dirección IP** para este appliance.
4. Introduzca una **Netmask** para la red.
5. Introduzca una dirección de **gateway** para la dirección IP de este appliance.
6. Introduzca una dirección de **difusión** para el appliance.
7. Introduzca un **nombre de host** para su appliance.
8. Introduzca un **dominio** para su dispositivo.
9. Seleccione **Seleccionar** y, a continuación, **Sí** para confirmar sus entradas.

Siguientes pasos

- Configure la información de administración de puertos de comunicación de Nodo de datos. Consulte **Configure eth2 y eth3 para las comunicaciones entre Nodo de datos:**

Configure eth2 y eth3 para las comunicaciones entre Nodo de datos:

Al configurar un appliance Nodo de datos, configure el puerto de comunicaciones entre Nodo de datos con una dirección IP no enrutable. Puede configurar lo siguiente:

- `eth2`
- canal de puerto que contiene `eth2` y `eth3`

> Debe asignar direcciones IP no enrutables desde el bloque CIDR `169.254.42.0/24`.

Antes de comenzar

- Consulte la hoja de especificaciones de Stealthwatch de su appliance para obtener información sobre los puertos SFP+ `eth2` y `eth3`. Tenga en cuenta que `eth2` y `eth3` dependen de cómo configure `eth0`.
- Si se encuentra en la configuración por primera vez, la configuración del sistema muestra la configuración del canal de puerto `eth2` o `eth2/eth3` después de que termine de configurar la información de administración de `eth0` del appliance. Vaya al paso 3.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Procedimiento

1. En el menú System Configuration (Configuración del sistema), seleccione **Network** y, a continuación, pulse **Intro**.
2. Seleccione **Node Communications** (Comunicaciones de nodo) y, a continuación, pulse Enter.
3. Seleccione la configuración del puerto de comunicación entre Nodo de datos. Tiene las siguientes opciones:
   - Seleccione **Sí** para agregar `eth2` y `eth3` como canal de puerto para las comunicaciones entre Nodo de datos.
   - Seleccione **No** para utilizar `eth2` en las comunicaciones entre Nodo de datos.
4. Ingrese una **dirección IP** no enrutable del bloque CIDR `169.254.42.0/24` para el canal de puerto `eth2` o `eth2/eth3`.
5. Introduzca una **Netmask** de `255.255.255.0` para esta dirección IP.
6. Introduzca una dirección de **gateway** para esta dirección IP.
7. Introduzca una dirección de **difusión** para esta dirección IP.
8. Seleccione **Seleccionar** y, a continuación, **Sí** para confirmar sus entradas.

   Esta es la última opción de configuración en Configuración de primera vez. El appliance se reinicia e implementa los cambios. Una vez que se complete, se abre la página de inicio de sesión.

Siguientes pasos

- Cambiar las contraseñas del usuario. Consulte **Cambio de la contraseña del usuario del administrador de sistemas** para obtener más información.

Cambio de la contraseña del usuario del administrador de sistemas

Para garantizar que la red es segura, cambie la contraseña predeterminada del administrador de sistemas para los appliances.

Para cambiar la contraseña del administrador de sistemas:

Antes de comenzar

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

- Inicie sesión en la consola del appliance como **sysadmin**.
- Introduzca la configuración del sistema.

Procedimiento

1. En el menú System Configuration (Configuración del sistema), seleccione **Password** (Contraseña) y pulse **Intro**.

   Si cambia la lista de hosts de confianza de los valores predeterminados, asegúrese de que se incluyen todos los appliances de Stealthwatch de confianza en la lista de hosts de confianza para cada appliance de Stealthwatch en su implementación. De lo contrario, los appliances no podrán comunicarse entre sí.

   Aparecerá una indicación para la contraseña actual bajo el menú.

2. Escriba la contraseña actual y, a continuación, pulse **Intro**.

   Aparecerá la indicación para una contraseña nueva.

3. Escriba la contraseña nueva y, a continuación, pulse **Intro**.

   La contraseña debe tener entre 8 y 30 caracteres alfanuméricos sin espacios. También puede utilizar los siguientes caracteres especiales: `$.~!@#%_=?:,{}()`

4. Escriba la contraseña de nuevo y, a continuación, pulse **Intro**.
5. Cuando se acepte su contraseña, pulse **Intro** de nuevo para volver al menú System Configuration (Configuración del sistema).
6. Continúe con la siguiente sección,**Cambio de la contraseña del usuario raíz**.

Cambio de la contraseña del usuario raíz

Después de cambiar la contraseña de usuario del administrador de sistemas, cambie la contraseña predeterminada del usuario raíz para proteger más la seguridad de su red.

Cambio de la contraseña del usuario de raíz:

Antes de comenzar

- Inicie sesión en la consola del appliance como **sysadmin**.
- Introduzca la configuración del sistema.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Procedimiento

1. Vaya al shell de raíz.
2. En el menú System Configuration (Configuración del sistema), seleccione **Advanced** (Avanzada) y, a continuación, pulse **Intro**. Aparecerá el menú Advanced (Avanzada).
3. Seleccione **RootShell** y, a continuación, pulse **Intro**.

   Aparece una indicación para la contraseña raíz.
4. Escriba la contraseña raíz y, a continuación, pulse **Intro**. Aparece la indicación de shell de raíz.
5. Escriba **SystemConfig** y, a continuación, pulse **Intro**.

   Esto le devuelve al menú System Configuration (Configuración del sistema) para que pueda cambiar la contraseña raíz.
6. Seleccione **Password** (Contraseña) y, a continuación, pulse **Intro**. La indicación de contraseña aparece debajo del menú.
7. Escriba la nueva contraseña raíz y, a continuación, pulse **Intro**. Aparece una segunda indicación.
8. Vuelva a escribir la nueva contraseña raíz y, a continuación, pulse **Intro**.
9. Cuando el cambio de contraseña se realice correctamente, pulse **Intro**. Ha cambiado sus contraseñas raíz y de administrador de sistemas predeterminadas. Esto le devuelve al menú System Configuration Console (Consola de configuración del sistema)
10. Seleccione **Cancel** (Cancelar) y pulse **Intro**. Se cierra la consola de configuración del sistema y aparece la indicación del shell de raíz.
11. Escriba **exit** (salir) y pulse **Intro**. Aparecerá la indicación de inicio de sesión.
12. Pulse **Ctrl + Alt** para salir del entorno de la consola.

Ahora está listo para configurar su appliance. Para configurar su appliance, consulte la **Guía de sistemas y configuración de Stealthwatch** correspondiente a su versión de software. La serie x2xx es compatible con las versiones de software 7.x de Stealthwatch.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Apéndice C. Configuración de los appliances

Cuando inicie sesión en el appliance por primera vez, utilizará la herramienta de configuración del appliance para configurar los ajustes del mismo.

Requisitos de la herramienta de configuración del appliance

- Confirme que sus firewalls y ACL (lista de control de acceso) permitirán el acceso.
- Recopile el nombre de host del appliance y las direcciones IP para lo siguiente:
    - appliance
    - máscara de subred
    - Gateways predeterminadas y de difusión
    - Servidores NTP y DNS
    - Dirección IP de SMC para la administración central

Gestionados

Como parte de la herramienta de configuración de appliances, configurará el appliance para que lo administre su consola de administración de Stealthwatch (SMC) principal.

Cuando la consola de administración de Stealthwatch (SMC) administra sus appliances, puede utilizar Administración central para editar las configuraciones de los appliances, actualizar el software, reiniciar, apagar y más.

Conmutación por error de SMC

Si tiene más de una consola de administración de Stealthwatch (SMC), puede configurar un par de conmutación por error de SMC para que una de ellas sirva de consola de respaldo a la otra.

- Utilice la herramienta de configuración de appliances para configurar cada SMC individual.
- Planifique qué SMC será primario y secundario.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

- Después de configurar cada SMC individual, utilizará el almacén de confianza de administración central y el cliente de escritorio de Stealthwatch para configurar la relación de conmutación por error de SMC.

Prácticas recomendadas

Para configurar su sistema correctamente, asegúrese de seguir las instrucciones de esta guía.

Recomendamos lo siguiente:

- **Uno a la vez**: configure un appliance a la vez. Confirme que el appliance esté **activo** antes de comenzar a configurar el siguiente appliance del clúster.
- **Orden:** siga el orden de la configuración.
- **Múltiples administradores centrales:** puede configurar más de un administrador central en el sistema. Sin embargo, cada appliance solo puede ser gestionado por un administrador central/SMC principal.
- **Acceso:** necesita privilegios de administrador para acceder a Administración central.

Orden de configuración

Configure los appliances en el siguiente orden y tenga en cuenta los detalles de cada appliance:

Pedido	Appliance	Detalles
1.	SMC principal	Su SMC principal es su administrador central. Asegúrese de que SMC se muestra como Activo antes de comenzar a configurar el siguiente appliance en el sistema.
2.	Directores UDP (también conocidos como FlowReplicators)	
3.	Nodo de datoss	
4.	Base de datos del recopilador de	Asegúrese de que la base de datos de

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

	flujo Serie 5000	Flow Collector serie 5000 se muestre como activa antes de iniciar la configuración del motor.
5.	Motor del recopilador de flujo Serie 5000	Asegúrese de que la base de datos de Flow Collector serie 5000 se muestre como activa antes de iniciar la configuración del motor.
6.	Todos los demás recopiladores de flujo (NetFlow y sFlow)	
7.	Sensores de flujo	Asegúrese de que su recopilador de flujo se muestre como activo antes de iniciar la configuración del sensor de flujo.
8.	Concentrador de terminal	
9.	SMC secundario (si se utiliza)	Asegúrese de que el SMC principal se muestre como activo antes de iniciar la configuración de SMC secundario. El SMC secundario se selecciona a sí mismo como administrador central. Configure la conmutación por error después de configurar todos los appliances.

Es posible que su sistema no tenga todos los appliances mostrados aquí.

1. Iniciar sesión

Utilice las siguientes instrucciones para configurar cada appliance mediante la herramienta de configuración de appliances.

1. En el campo de dirección de su navegador, escriba **https://** seguido de la dirección IP del appliance.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

- **SMC primario:** configure primero el SMC primario.
- **Activo**: confirme que cada appliance esté activo antes de comenzar a configurar el siguiente appliance del clúster.
- **Orden**: asegúrese de configurar los appliances en orden para que se comuniquen correctamente.

2. Introduzca las siguientes credenciales para iniciar sesión:

   - **Nombre de usuario:** admin
   - **Contraseña:** lan411cope

2. Configurar el appliance

Cuando inicie sesión en el appliance por primera vez, la herramienta de configuración del appliance le guiará en cada paso de la configuración.

1. **Cambiar contraseña predeterminada:** introduzca nuevas contraseñas para admin, root y sysadmin. Haga clic en **Siguiente** para desplazarse hasta cada usuario.

   Utilice los siguientes criterios:

   - **Longitud:** de 8 a 30 caracteres
   - **Cambio:** asegúrese de que la nueva contraseña es diferente de la contraseña predeterminada en al menos 4 caracteres.

Usuario	Contraseña predeterminada
administrador	lan411cope
raíz	lan1cope
sysadmin	lan1cope

Los menús sysadmin y raíz no están disponibles si ya ha cambiado las contraseñas predeterminadas durante la instalación del hardware. Consulte la Guía de instalación de hardware de la serie Stealthwatch x210 para obtener más información.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

2. **Gestión de interfaz de red:** revise la dirección IP y los campos de la interfaz de red. Confirme que la configuración predeterminada es correcta. Haga clic en **Siguiente**.

    - **Cambios:** para cambiar esta información, consulte con su administrador de red y consulte Resolución de problemas.
    - **IPv6 (opcional):** para activar IPv6, haga clic en **IPv6**. Marque la casilla de verificación **Habilitar IPv6** y complete los campos.

3. **Nombre de host y dominios:** introduzca el nombre de host y el nombre de dominio de red. Haga clic en **Siguiente**.

    - **Nombre de host:** se necesita un nombre de host único para cada appliance. Si asigna los mismos nombres de host a sus appliances, no se instalarán correctamente.
    - **Dominio de red:** se necesita un nombre de dominio completo para cada appliance.
    - **Dominio de Stealthwatch (solo SMC):** introduzca un dominio de Stealthwatch para sus appliances Stealthwatch.
    - **Rangos de direcciones IP (solo SMC):** seleccione el rango de direcciones IP para su red de Stealthwatch.

4. **Configuración de DNS**: confirme que el valor predeterminado sea correcto o introduzca la dirección IP del servidor de dominio. Haga clic en **Siguiente**.

    Agregar o eliminar servidores DNS (opcional):

    - **Agregar:** haga clic en el icono +.
    - **Eliminar:** haga clic en la casilla de verificación para seleccionar el servidor DNS. Haga clic en el icono –.

5. **Configuración NTP:** confirme que el valor predeterminado es correcto o haga clic en el icono **Menú** para seleccionar el servidor de protocolo de hora de red (NTP). Haga clic en **Siguiente**.

    - **Varios servidores NTP:** recomendamos configurar varios servidores NTP para garantizar la redundancia y la precisión.
    - **Fuente pública:** pool.ntp.org es una buena fuente pública de NTP.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Agregar o eliminar servidores NTP (opcional):

- **Agregar:** haga clic en el icono +.
- **Eliminar:** haga clic en la casilla de verificación para seleccionar el servidor NTP. Haga clic en el icono –.

6. Si el appliance es un SMC, vaya a **3. Registre la consola de gestión de Stealthwatch.**.

   Si el appliance no es un SMC, vaya a **4. Agregar appliances a la administración central**.

3. Registre la consola de gestión de Stealthwatch.

1. **Revise su configuración**: confirme que la información del appliance sea precisa.
2. Haga clic en **Aplicar** o en **Reiniciar y continuar**.

   Siga las indicaciones en pantalla mientras se reinicia el appliance.

   Espere unos minutos a que la nueva configuración del sistema surta efecto. Puede que tenga que actualizar la página.

3. Consola de gestión de Stealthwatch
4. La herramienta de configuración del appliance se abre de nuevo. Haga clic en **Continuar**.
5. En la pestaña Registrar su appliance, revise la dirección IP y haga clic en **Guardar**.

   - Esto instala la administración central en la consola de administración de Stealthwatch.

   - La dirección IP de SMC se detecta automáticamente y no se puede cambiar.

6. Cuando se complete la configuración del appliance, haga clic en **Ir al panel**.
7. Haga clic en el icono **Configuración global**. Seleccione **Administración central**.
8. Revise el inventario. Confirme que el estado del appliance SMC se muestra como **activo**.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

> ⚠ Asegúrese de que el SMC principal y cada appliance se muestran como activos antes de comenzar a configurar el siguiente appliance del clúster utilizando el orden de configuración y los detalles.

9. Implemente y configure su Almacén de datos. Vuelva a la Descripción general de la implementación del almacén de datos de Stealthwatch para revisar el proceso de implementación.

4. Agregar appliances a la administración central

La herramienta de configuración del appliance continúa guiándolo a través de la configuración del appliance con la administración central. Algunos de los pasos pueden variar según el appliance. Siga las instrucciones que aparecen en pantalla.

1. En la pestaña Administración central, introduzca la dirección IP de su SMC principal.

   Su SMC principal es su administrador central.

2. Haga clic en **Guardar**.
3. Siga las indicaciones en pantalla para confiar en el certificado de identidad del appliance SMC principal. Haga clic en **Sí** para confiar en el certificado y permitir que el appliance se comunique con el SMC.
4. Introduzca las credenciales de inicio de sesión para su SMC principal.
5. Seleccione su dominio de Stealthwatch.

   - **Colectores de flujo:** introduzca el número de puerto de colección de flujo.

     Valor predeterminado de NetFlow: 2055

     Valor predeterminado de sFlow: 6343

   - **Sensores de flujo:** seleccione un colector de flujo.

6. Haga clic en **Ir a Administración central**. Vaya a **5. Confirme el estado del appliance**.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

5. Confirme el estado del appliance

Después de configurar un appliance en la herramienta de configuración de appliances, confirme el estado del appliance en Administración central.

1. La herramienta de configuración del appliance se abre en el inventario de administración central, o puede abrirla de la siguiente manera:

   - Inicie sesión en su consola de gestión de Stealthwatch principal.
   - Haga clic en el icono **Configuración global**.
   - Seleccione **Administración central**.

2. Revise los appliances en el inventario del administrador del appliance.

   - Confirme que el appliance se muestra en el inventario.
   - Confirme que el estado del appliance se muestra como activo.

> ⚠ Asegúrese de que el SMC principal y cada appliance se muestran como activos antes de comenzar a configurar el siguiente appliance del clúster utilizando el orden de configuración y los detalles.

3. Para configurar el siguiente appliance de su sistema, vaya a **1. Iniciar sesión** y complete los procedimientos hasta el **5. Confirme el estado del appliance**.

   Si no tiene otro appliance que configurar, consulte la Guía de configuración del sistema de Stealthwatch para obtener más información sobre cómo completar las configuraciones del appliance. Como alternativa, vuelva a Stealthwatch Descripción general de la implementación del almacén de datos para revisar el proceso de implementación.

© 2021 Cisco Systems, Inc. o sus filiales. Todos los derechos reservados.

Información de copyright

Cisco y el logotipo de Cisco son marcas comerciales o registradas de Cisco y/o sus filiales en Estados Unidos y otros países. Para ver una lista de las marcas comerciales de Cisco, vaya a esta URL: https://www.cisco.com/go/trademarks. Las marcas comerciales de terceros que aquí se mencionan pertenecen a sus respectivos propietarios. El uso de la palabra "partner" no implica la existencia de una asociación entre Cisco y cualquier otra empresa. (1721R)

© 2021 Cisco Systems, Inc. o sus filiales.
Todos los derechos reservados.