Document Database Service

Pasos iniciales

 Edición
 01

 Fecha
 2025-01-23





HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2025. Todos los derechos reservados.

Quedan terminantemente prohibidas la reproducción y la divulgación del presente documento en todo o en parte, de cualquier forma y por cualquier medio, sin la autorización previa de Huawei Technologies Co., Ltd. otorgada por escrito.

Marcas y permisos

HUAWEI y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd. Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

Las funciones, los productos y los servicios adquiridos están estipulados en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, las funciones y los servicios descritos en el presente documento no se encuentren dentro del alcance de compra o de uso. A menos que el contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en este documento constituye garantía alguna, ni expresa ni implícita.

La información contenida en este documento se encuentra sujeta a cambios sin previo aviso. En la preparación de este documento se realizaron todos los esfuerzos para garantizar la precisión de sus contenidos. Sin embargo, ninguna declaración, información ni recomendación contenida en el presente constituye garantía alguna, ni expresa ni implícita.

Índice

1 Descripción	1
2 Tareas iniciales con clústeres	
2.1 Compra de una instancia de clúster	
2.1.1 Config rápido	3
2.1.2 Config personalizado	9
2.2 Conexión a una instancia de clúster	
2.2.1 Métodos de conexión	21
2.2.2 (Recomendado) Conexión a instancias de clúster mediante DAS	
2.2.2.1 Descripción	
2.2.2.2 Conexión a una instancia de clúster mediante DAS	
2.2.3 Conexión a una instancia de clúster a través de una red privada	
2.2.3.1 Configuración de reglas de grupo de seguridad	
2.2.3.2 Conexión a una instancia de clúster mediante Mongo Shell (red privada)	
2.2.4 Conexión a una instancia de clúster a través de una red pública	
2.2.4.1 Vinculación y desvinculación de una EIP	
2.2.4.2 Configuración de un grupo de seguridad	40
2.2.4.3 Conexión a una instancia de clúster mediante Mongo Shell (Red pública)	
2.2.4.4 Conexión a una instancia de clúster mediante Robo 3T	
2.2.5 Conexión a una instancia de clúster mediante código de programa	
2.2.5.1 Java	
2.2.5.2 Python	61
3 Tareas iniciales con conjunto de réplicas	62
3.1 Compra de una instancia de conjunto de réplicas	
3.1.1 Config rápido	
3.1.2 Config personalizado	67
3.2 Conexión a una instancia de conjunto de réplicas	
3.2.1 Métodos de conexión	79
3.2.2 (Recomendado) Conexión a instancias de conjunto de réplicas mediante DAS	
3.2.2.1 Descripción	
3.2.2.2 Conexión a una instancia de conjunto de réplicas mediante DAS	
3.2.3 Conexión a una instancia de conjunto de réplicas a través de una red privada	
3.2.3.1 Configuración de reglas de grupo de seguridad	

3.2.3.2 Conexión a una instancia de conjunto de réplicas mediante Mongo Shell (red privada)	
3.2.3.3 Conexión a réplicas de lectura mediante Mongo Shell.	
3.2.4 Conexión a una instancia de conjunto de réplicas a través de una red pública	
3.2.4.1 Vinculación y desvinculación de una EIP	101
3.2.4.2 Configuración de reglas de grupo de seguridad	
3.2.4.3 Conexión a una instancia de conjunto de réplicas mediante Mongo Shell (Red pública)	
3.2.4.4 Conexión a una instancia de conjunto de réplicas mediante Robo 3T	
3.2.5 Conexión a una instancia de conjunto de réplicas mediante código de programa	
3.2.5.1 Java	
3.2.5.2 Python	
4 Tareas iniciales con nodos únicos	1 2 6
4.1 Compra de una instancia de nodo único	
4.1.1 Quick Config	126
4.1.2 Custom Config	131
4.2 Conexión a una instancia de nodo único	141
4.2.1 Métodos de conexión	141
4.2.2 (Recomendado) Conexión a una instancia de nodo único mediante DAS	142
4.2.2.1 Descripción	
4.2.2.2 Conexión a una instancia de nodo único mediante DAS	142
4.2.3 Conexión a una instancia de nodo único a través de una red privada	
4.2.3.1 Configuración de un grupo de seguridad	143
4.2.3.2 Conexión a una instancia de nodo único mediante Mongo Shell (red privada)	147
4.2.4 Conexión a una instancia de nodo único a través de una red pública	151
4.2.4.1 Vinculación y desvinculación de una EIP	151
4.2.4.2 Configuración de un grupo de seguridad	154
4.2.4.3 Conexión a una instancia de nodo único mediante Mongo Shell (red pública)	156
4.2.4.4 Conexión a una instancia de nodo único mediante Robo 3T	161
4.2.5 Conexión a una instancia de nodo único mediante código de programa	
4.2.5.1 Java	
4.2.5.2 Python	171
5 Iniciar y cerrar sesión en la consola DDS	
6 Ejemplo: Comprar y conectarse a una instancia DDS	
6.1 Conexión a una instancia de base de datos mediante Mongo Shell	
6.2 Conexión a una instancia DDS a través de una EIP	191
A Historial de cambios	209

1 Descripción

Puede crear instancias y conectarse a ellas en la consola de gestión.

Proceso

Para crear y usar una instancia, debe realizar las operaciones descritas en el siguiente diagrama de flujo.





Procedim iento	Descripción	Referencia
Creación de una instancia	Puede personalizar los recursos informáticos y el almacenamiento disponibles para su instancia.	 Compra de una instancia de clúster Compra de una instancia de conjunto de réplicas
Vinculació n de una EIP	(Opcional) Cuando se conecta a una instancia desde Internet, debe configurar una EIP.	Vinculación y desvinculación de una EIP
Configurac ión de reglas de grupo de seguridad	 (Opcional) Agregue los dispositivos que acceden a la instancia al grupo de seguridad asociado a la instancia para que pueda acceder a la instancia desde los dispositivos. Si accede a la instancia desde un ECS que se encuentra en una seguridad diferente de la instancia a través de una red privada, debe configurar la regla de grupo de seguridad. Si se conecta a una instancia a través de una red pública, debe configurar las reglas de grupo de seguridad. 	 Configuración de reglas de grupo de seguridad (red privada) Configuración de reglas de grupo de seguridad (red pública)
Conexión a una instancia	Puede conectarse a instancias a través de DAS, una red privada, una red pública o código de programa.	 Conexión a una instancia de clúster Conexión a una instancia de conjunto de réplicas Conexión a una instancia de nodo único

Tabla 1-1 Proceso de operación

2 Tareas iniciales con clústeres

2.1 Compra de una instancia de clúster

2.1.1 Config rápido

En esta sección se describe cómo comprar rápidamente una instancia de clúster en la consola de gestión. DDS le ayuda a configurar y crear rápidamente un clúster en varios minutos.

Precauciones

Cada cuenta puede crear hasta 10 instancias de clúster.

Prerrequisitos

- Ha registrado un ID de Huawei y ha habilitado servicios de Huawei Cloud.
- El saldo de su cuenta es mayor o igual a \$0 USD.
- Para mostrar si el disco está cifrado en la lista de instancias de base de datos, envíe un ticket de servicio. En la esquina superior derecha de la consola de gestión, elija Service Tickets > Create Service Ticket.

Procedimiento

- Paso 1 Vaya a la página de Quick Config.
- Paso 2 En la página mostrada, seleccione un modo de facturación y configure la información sobre su instancia de base de datos. A continuación, haga clic en Next.

8	5
Billing Mode	Yearly/Monthly Pay-per-use
Region	li Anna III II 🕢
	Regions are geographic areas isolated from each other. For low network latency and quick resource access, select the nearest region.
Project	
AZ	az1 az2 az3 az1,az2,az3
	Deploy your DB instance in a single AZ or three AZs for high availability.
DB Instance Type 🕜	Cluster Repice set Clusters offer more redust performance than repica sets and more flexible scaling options. The high-availability and flexible scaling they provide make them an excellent choice for large enterprises. Clusters of community edition you can still create: 9. Increase Quota
Compatible MongoDB Version	4.4 4.2 4.0 3.4 View Version Details
Specifications	General-purpose Enhanced II
Recommended Specifications	mongos
	Node
	Class 2 vCPUs 8GB Ultra-high I/O 4 vCPUs 16GB Ultra-high I/O 2 vCPUs 8 GB v Ultra-high I/
	Maximum Connections:2,000 Maximum Connections:4,000 Maximum Connections:2,000
	Nodes - 2 + The quantity ranges from 2 to 16.
	Currently selected dds.mongodb.c6.Jarge.4.mongos 2 vCPUs 8GB
	shard
	Nota
	4 vCPUs 160B Ultra-high I/O 2 vCPUs 8 GB ▼ Ultra-high I/ Class
	1003B 200 GB Maximum Connaction: 2 000
	Nodes - 2 + The quantity ranges from 2 to 16.
	Currently selected dds.mongodb.c6.xlarge.4.shard 4 vCPUs 16GB
	aanfig
	comg
	Node Storage 2 vCPUs 4 GB 200B Class Space
	Currently selected dds.mongodb.c6.large.2.config 2 vCPUs 4 GB

Figura 2-1 Configuraciones básicas

Tabla 2-1 Configuraciones básicas

Parámetro	Descripción
Billing Mode	Seleccione un modo de facturación: Yearly/Monthly o Pay-per-use.
	• Para instancias anuales/mensuales
	 Especifique Required Duration y el sistema deduce las tarifas incurridas de su cuenta en función del precio del servicio.
	 Si no espera seguir usando la instancia mucho después de que caduque, puede cambiar el modo de facturación de anual/ mensual a pago por uso. Para más detalles, consulte Cambiar el modo de facturación de anual/mensual a de pago por uso.
	NOTA Las instancias facturadas anualmente/mensualmente no se pueden eliminar. Solo pueden darse de baja de. Para obtener más información, consulte Anulación de la suscripción a una instancia anual/mensual.
	• Para instancias de pago por uso
	 Se le factura el uso basado en el tiempo que el servicio está en uso.
	 Si espera usar el servicio ampliamente durante un largo período de tiempo, puede cambiar su modo de facturación de pago por uso a anual/mensual para reducir los costos. Para más detalles, consulte Cambio del modo de facturación de pago por uso a anual/mensual.

Parámetro	Descripción
Region	La región donde se encuentra el recurso. NOTA Las instancias desplegadas en diferentes regiones no pueden comunicarse entre sí a través de una red privada y no se puede cambiar la región de una instancia una vez que se ha comprado. Tenga cuidado al seleccionar una región.
Project	El proyecto corresponde a la región actual y se puede cambiar.
AZ	Una AZ es una parte de una región con su propia fuente de alimentación y red independiente. Las zonas de disponibilidad están físicamente aisladas pero pueden comunicarse a través de conexiones de red internas.
	Las instancias se pueden desplegar en una única zona de disponibilidad o en tres zonas de disponibilidad.
	NOTA El despliegue de 3-AZ no está disponible en todas las regiones. Si la opción de 3- AZ no se muestra en la página para comprar una instancia, pruebe con una región diferente.
	• Si su servicio requiere baja latencia de red entre instancias, despliega los componentes de la instancia en la misma zona de disponibilidad. Si selecciona una única zona de disponibilidad para desplegar la instancia, se utiliza de forma predeterminada el despliegue antiafinidad. Con un despliegue antiafinidad, sus nodos primarios, secundarios y ocultos se despliegan en diferentes máquinas físicas para una alta disponibilidad.
	• Si desea desplegar una instancia en las zonas de disponibilidad para la recuperación ante desastres, seleccione tres zonas de disponibilidad. En este modo de despliegue, los nodos de mongos, shard y config se distribuyen uniformemente en las tres zonas de disponibilidad.
DB Instance	Seleccione Cluster.
Туре	Una instancia de clúster incluye tres tipos de nodos: mongos, shard y config. Cada shard y config es un conjunto de réplicas de tres nodos para garantizar una alta disponibilidad.
Compatible MongoDB Version	 4.4 4.2 4.0 3.4

Parámetro	Descripción
СРU Туре	DDS admite arquitecturas de CPU x86 y Kunpeng. NOTA Este parámetro solo está disponible para MongoDB 4.0 y 3.4. El valor predeterminado es Kunpeng .
	 x86 Las CPU x86 utilizan el conjunto de instrucciones CISC (Complex Instruction Set Computing). Cada instrucción se puede usar para ejecutar operaciones de hardware de bajo nivel. Las instrucciones CISC varían en longitud, y tienden a ser complicadas y lentas en comparación con la computación de conjunto reducido de instrucciones (RISC).
	• Kunpeng La arquitectura de CPU Kunpeng utiliza RISC. El conjunto de instrucciones RISC es más pequeño y más rápido que CISC, gracias a la arquitectura simplificada. Las CPU de Kunpeng también ofrecen un mejor equilibrio entre potencia y rendimiento que x86.
	Las CPU de Kunpeng ofrecen una opción de alta densidad y bajo consumo que es más rentable para cargas de trabajo pesadas.
Specifications	Con una arquitectura x86, tiene las siguientes opciones:
	• Uso general (s6): Las instancias S6 son adecuadas para aplicaciones que requieren un rendimiento moderado en general, pero ocasionales ráfagas de alto rendimiento, como servidores web de carga ligera, entornos de pruebas y R&D empresariales y bases de datos de bajo y mediano rendimiento.
	 Mejorado II (c6): Las instancias C6 tienen múltiples tecnologías optimizadas para proporcionar un rendimiento informático potente y estable. Las NIC inteligentes de alta velocidad de 25 GE se utilizan para proporcionar un ancho de banda y un rendimiento ultra altos, lo que las convierte en una excelente opción para escenarios de carga pesada. Es adecuado para sitios web, aplicaciones web, bases de datos generales y servidores de caché que tienen requisitos de rendimiento más altos para recursos informáticos y de red; y aplicaciones empresariales de carga media y pesada.
	Para obtener más información sobre las especificaciones de instancia admitidas, consulte Especificaciones de instancia de clúster .
mongos Node Class	Para obtener más información sobre la CPU y la memoria de mongos, consulte Especificaciones de instancias de clúster . Puede cambiar la clase de una instancia después de crearla. Para obtener más información, consulte Cambio de la clase de instancia .
mongos Nodes	El valor varía de 2 a 32. Si es necesario, puede agregar nodos a una instancia después de crearla. Para obtener más información, consulte Adición de nodos de instancia de clúster .

Parámetro	Descripción
shard Node Class	Para obtener más información acerca de la CPU y la memoria del disco, consulte Especificaciones de instancias de clúster . El nodo de shard almacena datos de usuario pero no se puede acceder directamente. Puede cambiar la clase de una instancia después de crearla. Para obtener más información, consulte Cambio de la clase de instancia .
shard Storage Space	El valor oscila entre 10 GB y 2000 GB y debe ser un múltiplo de 10. Puede ampliar verticalmente una instancia después de crearla. Para obtener más información, consulte Ampliación vertical de una instancia de clúster . NOTA
	 Si el espacio de almacenamiento adquirido supera los 600 GB y el espacio de almacenamiento restante es de 18 GB, la instancia se convierte en sólo lectura.
	• Si el espacio de almacenamiento que compró es inferior a 600 GB y el uso de espacio de almacenamiento alcanza el 97%, la instancia se convierte en sólo lectura.
	En estos casos, elimine recursos innecesarios o amplíe la capacidad.
shard Nodes	El valor varía de 2 a 32. Si es necesario, puede agregar nodos a una instancia después de crearla. Para obtener más información, consulte Adición de nodos de instancia de clúster .
config Node Class	Para obtener más información sobre la CPU y la memoria del nodo de configuración, consulte Especificaciones de instancias de clúster . Puede cambiar la clase de una instancia después de crearla. Para obtener más información, consulte Cambio de la clase de instancia .
config Storage Space	De acuerdo con las funciones y los requisitos mínimos del nodo de configuración, el espacio de almacenamiento del nodo de configuración se establece en 20 GB de forma predeterminada. No se puede ampliar el almacenamiento del nodo después de crearlo.

Figura 2-2 Red, duración requerida y cantidad

Network						
VPC	default_vpc •	С	default_subnet(192.168.0.0/24) *	С	Sys-default(b6f16cee-e859-47e2-a418 •	С
	After the DDS instance is created, the VPC ca	nnot be	e changed.			
	Available private IP addresses in the subnet: 227					
	In a security group, rules that authorize connection	ons to D	08 instances apply to all DB instances associated w	ith the s	ecurity group.	
Enterprise Project Enterprise Project	-Select-	Ŧ	C View Project Management ③			
Some settings are configured by defai	ult during purchase, but can still be modified after	the inst	tance is created. If you do not see a setting listed f	or your i	instance, click Custom Config	
✓ Default configuration items						

Parámetro	Descripción
VPC	La VPC donde se encuentran instancias de base de datos. Una VPC aísla las redes para diferentes servicios. Le permite gestionar y configurar fácilmente redes privadas y cambiar las configuraciones de red. Necesita crear o seleccionar la VPC requerida. Para obtener más información, consulte Creación de una VPC en la <i>Guía de usuario de Virtual Private</i> <i>Cloud</i> . Para obtener más información acerca de las restricciones en el uso de VPC, consulte Métodos de conexión .
	Si no hay VPC disponibles, DDS crea una para usted de manera predeterminada.
	NOTA Una vez creada la instancia de DDS, la VPC no podrá modificarse.
Enterprise Project	Solo los usuarios de empresa pueden utilizar esta función. Para utilizar esta función, póngase en contacto con el servicio de atención al cliente.
	Un proyecto empresarial es un modo de gestión de recursos en la nube, en el que los recursos y los miembros en la nube se gestionan de forma centralizada por proyecto.
	Seleccione un proyecto de empresa en la lista desplegable. El proyecto predeterminado es default . Para obtener más información acerca de los proyectos de empresa, consulte Gestión de proyecto en <i>Guía de usuario de Enterprise Management</i> .
	Para personalizar un proyecto de empresa, haga clic en Enterprise en la esquina superior derecha de la consola. Se muestra la página Enterprise Management . Para obtener más información, consulte Creación de un proyecto empresarial en la <i>Guía de usuario de Enterprise Management</i> .

Tabla 2-2 Ajustes de red

Tabla 2-3 Período de uso y cantidad

Parámetro	Descripción
Required Duration	La duración de su suscripción si selecciona Yearly/Monthly . La duración de las suscripciones varía de un mes a tres años.
Auto-renew	 De forma predeterminada, esta opción no está seleccionada. Si selecciona esta opción, el ciclo de renovación automática viene determinado por la duración de la suscripción.
Quantity	La cantidad de compra depende de la cuota de instancia del clúster. Si su cuota actual no le permite comprar el número requerido de instancias, puede solicitar una cuota aumentada. Las instancias anuales/ mensuales que se compraron en lotes tienen las mismas especificaciones, excepto el nombre y el ID de la instancia.

Paso 3 En la página mostrada, confirme los detalles de la instancia.

• Para instancias anuales/mensuales

- Si necesita modificar las especificaciones, haga clic en Previous para volver a la página anterior.
- Si no necesita modificar las especificaciones, lea y acepte el contrato de servicio y haga clic en **Pay Now** para ir a la página de pago y completar el pago.
- Para instancias de pago por uso
 - Si necesita modificar las especificaciones, haga clic en Previous para volver a la página anterior.
 - Si no necesita modificar las especificaciones, lea y acepte el contrato de servicio y haga clic en Submit para comenzar a crear la instancia.
- **Paso 4** Haga clic en **Back to Instance List**. Después de crear una instancia DDS, puede ver y gestionarla en la página **Instances**.
 - Cuando se crea una instancia, el estado que se muestra en la columna **Status** es **Creating**. Este proceso dura unos 15 minutos. Una vez completada la creación, el estado cambia a **Available**.
 - DDS habilita la política de copia de respaldo automatizada de forma predeterminada. Después de crear una instancia, puede modificar o deshabilitar la política de copia de respaldo automatizada. Una copia de respaldo completa automatizada se activa inmediatamente después de la creación de una instancia.

----Fin

2.1.2 Config personalizado

En esta sección se describe cómo comprar una instancia de clúster en modo personalizado en la consola de gestión. Puede personalizar los recursos informáticos y el espacio de almacenamiento de una instancia de clúster en función de sus requisitos de servicio. Además, puede configurar ajustes avanzados, como el registro de consultas lentas y la copia de respaldo automatizada.

Precauciones

Cada cuenta puede crear hasta 10 instancias de clúster.

Prerrequisitos

- Ha registrado un ID de Huawei y ha habilitado servicios de Huawei Cloud.
- El saldo de su cuenta es mayor o igual a \$0 USD.
- Para mostrar si el disco está cifrado en la lista de instancias de base de datos, envíe un ticket de servicio. En la esquina superior derecha de la consola de gestión, elija Service Tickets > Create Service Ticket.

Procedimiento

- Paso 1 Vaya a la página Custom Config.
- Paso 2 En la página mostrada, seleccione un modo de facturación y configure la información sobre su instancia de base de datos. A continuación, haga clic en Next.

Basic Information		
Billing Mode	Yearly/Monthly Pay-per-use	
Region	The share of the second se	
	Regions are geographic areas isolated from each other. For low network latency and quick resource access, select the nearest region.	
Project	- 1 Calc	
AZ	az1 az2 az3 az1,az2,az3	
	Deploy your DB instance in a single AZ or three AZs for high availability.	
DB Instance Name	dds-c5d2	
DB Instance Type	Cluster Replica set	
	Clusters offer more robust performance than replica sets and more flexible scaling options. The high-availability and flexible scaling they provide mak Clusters of community edition you can still create: 9. Increase Quota	them an excellent choice for large enterprises.
Compatible MongoDB Version	4.4 4.2 4.0 3.4 View Version Details	
Storage Type	Ultra-hich UO	
Storage Engine	KODSUB	
Specifications	General-purpose Enhanced II	
inongos		
Node Class	VCPU Memory	Maximum Connections
		4 000
		16.000
		10,000
		16,000
		16.000
	OF VETUS (20 UB Currently selected, dds monordh c6 larne 4 monors (2 vCPI)s (8 GB	16,000
	annen) eanenen annouellenenen lei runellen fellenen och ellenen	
Nodes	- 2 + The quantity ranges from 2 to 16.	
Parameter Template	Default-DDS-4.2-Mongos C View Parameter Template	
Parameter Template	Default-DDS-4.2-Mongos • C Vew Parameter Template	
Parameter Template	Default-005-4.2-Monops C Verve Parameter Template	
Parameter Template shard Node Class	VCPU Memory VCPU Memory	Maximum Connections
Parameter lemplate	VCPU Memory VCPU S GB VCPU S GB	Maximum Connections
Parameter Template shard Node Class	C Vere Parameter Template vCPU Memory 2 vCPU 5 08 2 vCPU 16 08 2 vCPU 16 08	Maximum Connections 2.000 2.000
Parameter Template	C Vew Parameter Template vCPU Memory 2 vCPU 5 GB 2 vCPU 15 GB 4 vCPU 15 GB 4 vCPU 12 GB	Maximum Connections 2.000 2.000 4.000
Parameter Template	VCPU Memory © Verw Parameter Template vCPU Memory 2 vCPU 8 GB 2 vCPU 18 GB 4 vCPU 18 GB 4 vCPU 12 GB 4 vCPU 12 GB	Maximum Connections 2,000 2,000 4,000 4,000 10,000
Parameter Template	VCPU Memory © Verw Parameter Template vCPU Memory 2 vCPus 8 GB 2 vCPus 18 GB 2 vCPUs 18 GB 4 vCPUs 12 GB 4 vCPUs 12 GB 9 vCPUs 20 B 9 vCPUs 20 B 9 vCPUs 20 B	Maximum Connections 2,000 4,000 4,000 16,000 16,000
Parameter Template	vCPU Memory © Vew Parameter Template vCPU Memory 2 vCPUa 8 GB 2 vCPUa 16 GB 2 vCPUa 16 GB 4 vCPUa 15 GB 4 vCPUa 22 GB 3 vCPUa 20 GB 5 vCPUa 24 GB 5 vCPUa 24 GB 4 vCPUa 24 GB 5 vCPUa 24 GB 5 vCPUa 24 GB	Maximum Connections 2.000 2.000 4.000 4.000 10.000 10.000
Parameter Template	vCPU Memory © Vew Parameter Template vCPU Memory 2 vCPUs 8 GB 2 vCPUs 8 GB 2 vCPUs 16 GB 4 vCPUs 15 GB 4 vCPUs 12 GB 4 vCPUs 22 GB 5 vCPUs 24 GB 5 vCPUs 24 GB 5 vCPUs 24 GB 5 vCPUs 24 GB 5 vCPUs 24 GB 5 vCPUs 24 GB 5 vCPUs 24 GB 5 vCPUs 24 GB	Maximum Connections 2.000 2.000 4.000 4.000 1.0,000 1.0,000
Parameter Template	VCPU Memory Image: C Very Parameter Template VCPU Memory 2 vCPu 8 GB 2 vCPu 16 GB 2 vCPu 16 GB 4 vCPu 18 GB 4 vCPu 12 GB 5 vCPU 22 GB 5 vCPU 24 GB 6 vCPU 12 GB 16 vCPU 12 GB 6 vCPU 12 GB 16 vCPU 14 GB 7 vCPU 14 GB 16 vCPU 14 GB 9 vCPU 14 GB 16 vCPU 14 GB 9 vCPU 14 GB 16 vCPU 14 GB	Maximum Connections 2.000 2.000 4.000 10.000 10.000 10.000
Parameter Template shard Node Class Storage Space	vCPU Memory Image: Constraints Image: Constraints VCPU Memory Image: Constraints Image: Constraints	Maximum Connections 2.000 2.000 4.000 4.000 16.000 16.000 10.000 10.000
Parameter Template	vCPU Memory • C Vew Parameter Template • 2 vCPU 8 GB 2 vCPU 16 GB -	Maximum Connections 2.000 2.000 4.000 4.000 10.000 10.000
Parameter Template	vCPU Memory • C Vew Parameter Template • VCPU Memory • 2 vCPu 8 GB • • 2 vCPu 8 GB • • • • 4 vCPu 16 GB • • • • 4 vCPu 16 GB • • • • 4 vCPu 12 GB • • • • 4 vCPu 12 GB • • • • 5 vCPUs 24 GB • • • • 5 vCPUs 24 GB • • • • 5 vCPUs 24 GB • • • • • 16 vCPUs 54 GB • • • • • 16 vCPUs 54 GB • • • • • 16 vCPUs 52 GB • • • • • • 17 vCPUs 54 GB • • • • • • • 17 vCPUs 50 T50 150 T50 175 200 • • • • • • • • • • •	Maximum Connections 2.000
Parameter Template	vCPU Memory • C Vew Parameter Tangate • VCPU Memory • 2 vCPu 8 GB • • 2 vCPu 8 GB • • • • 4 vCPu 16 GB • • • • 4 vCPu 16 GB • • • • 4 vCPu 12 GB • • • • 4 vCPu 12 GB • • • • 4 vCPu 12 GB • • • • 5 vCPu 14 GB • • • • 16 vCPu 14 GB • • • • • 16 vCPu 14 GB • • • • • 16 vCPu 14 GB • • • • • 16 vCPu 14 GB • • • • • • 16 vCPu 14 GB • • • • • • • 16 vCPu 12 vCPu 12 vCPu 10 00 120 150 175 2000 •	Maximum Connections 2.000
Parameter Template	vCPU Memory 2 vCPUs 8 GB 2 vCPUs 16 GB 4 vCPUs 15 GB 4 vCPUs 12 GB 8 vCPUs 22 GB 8 vCPUs 22 GB 8 vCPUs 24 GB 16 vCPUs 44 GB Currently solected 17 20 750 <	Maximum Connections 2.000
Parameter Template	vCPU Memory © 2 vCPUs 8 GB 2 vCPUs 8 GB 2 vCPUs 18 GB 4 vCPUs 18 GB 4 vCPUs 12 GB 8 vCPUs 22 GB 8 vCPUs 22 GB 9 vCPUs 44 GB 16 vCPUs 64 GB Currently selected 17 25 500 750 1000 1250 1500 1750 2000 To ensure that the CB instance can still be used if the storage space is about to be used up, the database is set to read-only, and data cannot be not stored to be used only. Table stored to be used only.	Maximum Connections 2.000
Parameter Template Shard Node Class Storage Space Nodes Parameter Template config	vCPU Memory • C Vew Parameter Tangata • C Vew Parameter Tangata vCPU Memory • C Vew Parameter Tangata	Maximum Connections 2.000
Parameter Template Shorage Space Nodes Parameter Template Config Node Class	vCPU Memory • C Vew Parameter Tangate vCPU Memory • 2 vCPu 8 08 • 2 vCPu 16 08 • • • 4 vCPu 16 08 • • • • 4 vCPu 16 08 • • • 4 vCPu 12 08 • • • 8 vCPu 12 08 • • • 8 vCPu 14 08 • • • 16 vCPu 16 05 • • • • 16 vCPu 17 00 120 150 150 • • 2 • The quantify ranges tom 2 to 16. • • C Vew Parameter Tangitate	Maximum Connections 2.000
Parameter Template Storage Space Nodes Parameter Template Config Node Class	Verwel Parameter Template VCPU Memory • 2 v.CPUs 8 G8 2 v.CPUs 18 G8 4 v.CPUs 18 G8 4 v.CPUs 18 G8 4 v.CPUs 18 G8 4 v.CPUs 12 G8 8 v.CPUs 14 G8 16 v.CPUs 64 G8 Currently selected dis mongooth c6 large 4 shard 2 v.CPUs 8 G8 16 v.CPUs 64 G8 Currently selected dis mongooth c6 large 5 to 10 to 125 10 2 2 3 50 75 100 125 150 175 2000 To ensure that the G8 instance can still be used if the storage space is about to be used up, the database is set to read only, and data cannot be mongooth c6.Larges to 12 to 16. 10 2 + 1 The quantity ranges from 2 to 16. 10 2 + 1 The quantity ranges from 2 to 18. 10 2 + 1 The quantity ranges from 2 to 18. 10 2 + 1 The quantity ranges from 2 to 18. 10 2 + 1 The quantity ranges from 2 to 18. 10 2 + 1 The quantity ranges from 2 to 18. 10 2 + 1 The quantity ranges from 2 to 18. 10 2 - 1 10 C 10 2 - 1 10 C 10 2 - 1 10 C	Maximum Connections 2.000
Parameter Template Shorage Space Nodes Parameter Template Config Node Class Storage Space	C Very Farameter Template vCPU Memory • • C </th <th>Maximum Connections 2.000 </th>	Maximum Connections 2.000
Parameter Template Shorage Space Nodes Parameter Template Config Node Class Storage Space Parameter Template Parameter Template Config Node Class Storage Space Parameter Template	Verw Parameter Template vCPU Memory • 2 vCPUs 8 08 2 vCPUs 18 08 4 vCPUs 18 08 4 vCPUs 12 08 8 vCPUs 14 08 C Verw Parameter Template	Maximum Connections 2.000
Parameter Template Shorage Space Nodes Parameter Template Config Node Class Storage Space Node Class Storage Space Parameter Template Disk Execusion	Understand C Vew Parameter Template vCPU Memory • C Vew Parameter Template • 2 vCPUs 8 08 • • • 2 vCPUs 18 08 • • • 4 vCPUs 18 08 • • • 4 vCPUs 12 08 • • • 8 vCPUs 12 08 • • • 8 vCPUs 14 08 • • Durrently selected dts mongoth c5 large 4 shard 2 vCPUs 8 08 • • • 15 vCPUs 64 08 • • • • 250 500 750 100 1250 150 1200 • 0 1250 150 150 2000 • • • • • • • 1 100 120 150 150 2000 • <t< td=""><td>Maximum Connections 2.000 </td></t<>	Maximum Connections 2.000

Figura 2-3 Configuraciones básicas

Parámetro	Descripción
Billing Mode	Seleccione un modo de facturación: Yearly/Monthly o Pay-per-use.
	Para instancias anuales/mensuales
	 Especifique Required Duration y el sistema deduce las tarifas incurridas de su cuenta en función del precio del servicio.
	 Si no espera seguir usando la instancia mucho después de que caduque, puede cambiar el modo de facturación de anual/ mensual a pago por uso. Para más detalles, consulte Cambio del modo de facturación de anual/mensual a pago por uso
	NOTA Las instancias facturadas anualmente/mensualmente no se pueden eliminar. Solo pueden darse de baja de. Para obtener más información, consulte Anulación de la suscripción a una instancia anual/mensual.
	 Para instancias de pago por uso
	 Se le factura el uso basado en el tiempo que el servicio está en uso.
	 Si espera usar el servicio ampliamente durante un largo período de tiempo, puede cambiar su modo de facturación de pago por uso a anual/mensual para reducir los costos. Para más detalles, consulte Cambio del modo de facturación de pago por uso a anual/mensual.
Region	La región donde se encuentra el recurso.
	NOTA Las instancias desplegadas en diferentes regiones no pueden comunicarse entre sí a través de una red privada y no se puede cambiar la región de una instancia una vez que se ha comprado. Tenga cuidado al seleccionar una región.
Project	El proyecto corresponde a la región actual y se puede cambiar.

Tabla 2-4 Configuracio	ones básicas
------------------------	--------------

Parámetro	Descripción
AZ	Una AZ es una parte de una región con su propia fuente de alimentación y red independiente. Las zonas de disponibilidad están físicamente aisladas pero pueden comunicarse a través de conexiones de red internas.
	Las instancias se pueden desplegar en una única zona de disponibilidad o en tres zonas de disponibilidad.
	• Si su servicio requiere baja latencia de red entre instancias, despliega los componentes de la instancia en la misma zona de disponibilidad. Si selecciona una única zona de disponibilidad para desplegar la instancia, se utiliza de forma predeterminada el despliegue antiafinidad. Con un despliegue antiafinidad, sus nodos primarios, secundarios y ocultos se despliegan en diferentes máquinas físicas para una alta disponibilidad.
	 Si desea desplegar una instancia en las zonas de disponibilidad para la recuperación ante desastres, seleccione tres zonas de disponibilidad. En este modo de despliegue, los nodos de mongos, shard y config se distribuyen uniformemente en las tres zonas de disponibilidad.
	NOTA El despliegue de 3-AZ no está disponible en todas las regiones. Si la opción de 3- AZ no se muestra en la página para comprar una instancia, pruebe con una región diferente.
DB Instance Name	• El nombre de instancia que especifique después de la compra. El nombre de instancia debe contener entre 4 y 64 caracteres y debe comenzar con una letra. Es sensible a mayúsculas y minúsculas y puede contener letras, dígitos, guiones (-) y guiones bajos (_). No puede contener otros caracteres especiales.
	• El nombre de instancia puede ser el mismo que un nombre de instancia existente.
	 Si compra un lote de instancias a la vez, se agregará un sufijo numérico de 4 dígitos a los nombres de las instancias, comenzando por -0001. Si más adelante realiza otra compra por lotes, los nombres de las nuevas instancias se numerarán primero utilizando los sufijos que falten en la secuencia de sus instancias existentes y, a continuación, continuando desde donde lo dejó su última compra por lotes. Por ejemplo, un lote de 3 instancias obtiene los sufijos -0001, -0002 y -0003. Si eliminó instancia 0002 y luego compró 3 instancias más, las nuevas instancias obtendrían los sufijos -0002, -0004 y -0005.
	 Después de crear la instancia de base de datos, puede cambiar su nombre. Para obtener más información, consulte Cambio del nombre de una instancia.
DB Instance	Seleccione Cluster.
турс	Una instancia de clúster incluye tres tipos de nodos: mongos, shard y config. Cada shard y config es un conjunto de réplicas de tres nodos para garantizar una alta disponibilidad.

Parámetro	Descripción
Compatible MongoDB Version	 4.4 4.2 4.0 3.4
CPU Type	 DDS admite arquitecturas de CPU x86 y Kunpeng. NOTA Este parámetro solo está disponible para MongoDB 4.0 y 3.4. El valor predeterminado es Kunpeng. x86 Las CPU x86 utilizan el conjunto de instrucciones de complejas de computación con Conjunto de Instrucciones Complejas (CISC). Cada instrucción se puede usar para ejecutar operaciones de hardware de bajo nivel. Las instrucciones CISC varían en longitud, y tienden a ser complicadas y lentas en comparación con la computación de conjunto reducido de instrucciones (RISC). Kunpeng La arquitectura de CPU Kunpeng utiliza RISC. El conjunto de instrucciones RISC es más pequeño y más rápido que CISC, gracias a la arquitectura simplificada. Las CPU de Kunpeng también ofrecen un mejor equilibrio entre potencia y rendimiento que x86. Las CPU de Kunpeng ofrecen una opción de alta densidad y bajo consumo que es más rentable para cargas de trabajo pesadas
Storage Type	Si no utiliza DeC, el tipo de almacenamiento es Cloud SSD de forma predeterminada. Para los usuarios de DeC, los tipos de almacenamiento admitidos
	 dependen del tipo de recurso seleccionado. Si selecciona EVS para Resource Type, Storage Type se establece en Cloud SSD. Si selecciona DSS para Resource Type, Storage Type se puede establecer en Common I/O, High I/O o Cloud SSD.
Storage Engine	 WiredTiger WiredTiger es el motor de almacenamiento predeterminado de DDS 3.4 y 4.0. WiredTiger ofrece diferentes mecanismos de control de simultaneidad y compresión de granularidad para la gestión de datos. Puede proporcionar el mejor rendimiento y eficiencia de almacenamiento para diferentes tipos de aplicaciones. RocksDB RocksDB es el motor de almacenamiento predeterminado de DDS 4.2 y 4.4. RocksDB admite búsqueda de puntos eficiente, escaneo de rango y escritura de alta velocidad. RocksDB se puede utilizar como el motor de almacenamiento de datos subyacente de MongoDB y es adecuado para escenarios con un gran número de operaciones de escritura.

Parámetro	Descripción
Specifications	Con una arquitectura x86, tiene las siguientes opciones:
	• Uso general (s6): Las instancias S6 son adecuadas para aplicaciones que requieren un rendimiento moderado en general, pero ocasionales ráfagas de alto rendimiento, como servidores web de carga ligera, entornos de pruebas y R&D empresariales y bases de datos de bajo y mediano rendimiento.
	 Mejorado II (c6): Las instancias C6 tienen múltiples tecnologías optimizadas para proporcionar un rendimiento informático potente y estable. Las NIC inteligentes de alta velocidad de 25 GE se utilizan para proporcionar un ancho de banda y un rendimiento ultra altos, lo que las convierte en una excelente opción para escenarios de carga pesada. Es adecuado para sitios web, aplicaciones web, bases de datos generales y servidores de caché que tienen requisitos de rendimiento más altos para recursos informáticos y de red; y aplicaciones empresariales de carga media y pesada.
	Para obtener más información sobre las especificaciones de instancia admitidas, consulte Especificaciones de instancia de clúster.
mongos Node Class	Para obtener más información sobre la CPU y la memoria de mongos, consulte Especificaciones de instancias de clúster . Puede cambiar la clase de una instancia después de crearla. Para obtener más información, consulte Cambio de la clase de instancia .
mongos Nodes	El valor varía de 2 a 32. Si es necesario, puede agregar nodos a una instancia después de crearla. Para obtener más información, consulte Adición de nodos de instancia de clúster .
mongos Parameter Template	Los parámetros que se aplican a los nodos mongos. Después de crear una instancia, puede cambiar la plantilla de parámetros de un nodo para obtener el mejor rendimiento.
	Para obtener más información, consulte Edición de una plantilla de parámetro .
shard Node Class	Para obtener más información acerca de la CPU y la memoria del disco, consulte Especificaciones de instancias de clúster . El nodo de shard almacena datos de usuario pero no se puede acceder directamente. Puede cambiar la clase de una instancia después de crearla. Para obtener más información, consulte Cambio de la clase de instancia .
shard Storage Space	El valor oscila entre 10 GB y 2000 GB y debe ser un múltiplo de 10. Puede ampliar verticalmente una instancia después de crearla. Para obtener más información, consulte Ampliación vertical de una instancia de clúster .
	NOTA
	• Si el espacio de almacenamiento adquirido supera los 600 GB y el espacio de almacenamiento restante es de 18 GB, la instancia se convierte en sólo lectura.
	• Si el espacio de almacenamiento que compró es inferior a 600 GB y el uso de espacio de almacenamiento alcanza el 97%, la instancia se convierte en sólo lectura.
	En estos casos, elimine recursos innecesarios o amplíe la capacidad.

Parámetro	Descripción	
shard Nodes	El valor varía de 2 a 32. Si es necesario, puede agregar nodos a una instancia después de crearla. Para obtener más información, consulte Adición de nodos de instancia de clúster .	
shard Parameter Template	Los parámetros que se aplican a los nodos de shard. Después de crear una instancia, puede cambiar la plantilla de parámetros de un nodo para obtener el mejor rendimiento.	
	Para obtener más información, consulte Edición de una plantilla de parámetro.	
config Node Class	Para obtener más información sobre la CPU y la memoria del nodo de configuración, consulte Especificaciones de instancias de clúster . Puede cambiar la clase de una instancia después de crearla. Para obtener más información, consulte Cambio de la clase de instancia .	
config Storage Space	De acuerdo con las funciones y los requisitos mínimos del nodo de configuración, el espacio de almacenamiento del nodo de configuración se establece en 20 GB de forma predeterminada. No se puede ampliar el almacenamiento del nodo después de crearlo.	
config Parameter Template	Los parámetros que se aplican a los nodos config. Después de crear una instancia, puede cambiar la plantilla de parámetros de un nodo para obtener el mejor rendimiento.	
	Para obtener más información, consulte Edición de una plantilla de parámetro.	
Disk Encryption	• Disabled: Desactivar la encriptación.	
	 Enabled: Habilitar la encriptación. Esta característica mejora la seguridad de los datos, pero afecta ligeramente el rendimiento de lectura/escritura. Key Name: Seleccione o cree una clave privada, que es la clave del tenant. 	
	NOTA	
	 Después de crear una instancia, el estado de encriptación del disco y la clave no se pueden cambiar. La encriptación de disco no cifrará los datos de copia de respaldo almacenados en OBS. Para habilitar la encriptación de datos de copia de respaldo, póngase en contacto con el servicio de atención al cliente. 	
	 Para comprobar si el disco está cifrado, puede ver Disk Encrypted en la lista de instancias de base de datos. 	
	 Si la encriptación de disco o la encriptación de datos de copia de respaldo están habilitados, mantenga la clave correctamente. Una vez que la clave está deshabilitada, eliminada o congelada, la base de datos no estará disponible y los datos no se restaurarán. Si la encriptación de disco está habilitado pero la encriptación de datos de copia de respaldo no está habilitado, puede restaurar datos a una nueva instancia desde copias de respaldo. 	
	Si tanto la encriptación de disco como la encriptación de datos de copia de respaldo están habilitados, los datos no se pueden restaurar.	
	 Para obtener más información sobre cómo crear una clave, consulte "Creación de un CMK" en Guía de usuario de Data Encryption Workshop. 	

Figura 2-4 Configuración del administrador



Tabla 2-5 Configuración del administrador

Parámetro	Descripción
Password	• Configure Introduzca y confirme la nueva contraseña de administrador. Después de crear una instancia, puede conectarse a la instancia mediante la contraseña.
	 Skip Para iniciar sesión, tendrá que restablecer la contraseña más adelante en la página Basic Information. Si necesita conectarse a una instancia después de crearla, busque la instancia y elija More > Reset Password en la columna Operation para establecer primero una contraseña para la instancia.
Administrator	La cuenta predeterminada es rwuser .
Administrator Password	Establezca una contraseña para el administrador. La contraseña debe tener entre 8 y 32 caracteres y contener letras mayúsculas, minúsculas, dígitos y al menos uno de los siguientes characters: ~!@#%^*=+?()\$ Mantenga esta contraseña segura. Si se pierde, el sistema no puede recuperarlo para usted.
Confirm Password	Ingrese la contraseña de administrador de nuevo.

Figura 2-5 Red y	duración requerida
------------------	--------------------

Network		
VPC	default_vpc 🔹	C View VPC
	After the DDS instance is created, the VPC ca	not be changed.
Subnet	default_subnet(192.168.0.0/24) •	C View Subnet
	Available private IP addresses in the subnet: 227	
Security Group	Sys-default(b6f16cee-e859-47e2-a418 •	C View Security Group
	In a security group, rules that authorize connection	ns to DB instances apply to all DB instances associated with the security group.
SSL	View Details	
	▲ To encrypt transmission, enable SSL.	
Database Port	Default port: 8635	
Enterprise Project		
Enterprise Project	Select	C View Project Management (2)

Tabla 2-6 Ajustes de red

Parámetro	Descripción
VPC	La VPC donde se encuentran instancias de base de datos. Una VPC aísla las redes para diferentes servicios. Le permite gestionar y configurar fácilmente redes privadas y cambiar las configuraciones de red. Deberá crear o seleccionar la VPC requerida. Para obtener más información sobre cómo crear una VPC, consulte "Creación de una VPC" en la <i>Guía del usuario de Virtual Private Cloud</i> . Para obtener más información sobre las restricciones en el uso de VPC, consulte Métodos de conexión. Si no hay VPC disponibles, DDS crea una para usted de manera predeterminada.
	Una vez creada la instancia de DDS, la VPC no podrá modificarse.
Subnet	Una subred proporciona recursos de red dedicados que están lógicamente aislados de otras redes por razones de seguridad.
	Una vez creada la instancia, puede cambiar la dirección IP privada asignada por la subred. Para obtener más información, consulte Cambio de una dirección IP privada .
	NOTA Se admiten las subredes IPv4 e IPv6.

Parámetro	Descripción
Security Group	 Un grupo de seguridad controla el acceso entre DDS y otros servicios. Si no hay grupos de seguridad disponibles, DDS crea una para usted de manera predeterminada. NOTA Asegúrese de que haya una regla de grupo de seguridad configurada que permita a los clientes acceder a las instancias. Por ejemplo, seleccione una regla TCP entrante con el puerto predeterminado 8635 e introduzca una dirección IP de subred o seleccione un grupo de seguridad al que pertenece la instancia.
SSL	Secure Sockets Layer (SSL) encripta las conexiones entre clientes y servidores, evitando que los datos sean manipulados o robados durante la transmisión. Puede habilitar SSL para mejorar la seguridad de los datos. Después de crear una instancia, puede conectarse a ella mediante SSL.
Database Port	 El puerto DDS predeterminado es 8635, pero este puerto se puede modificar si es necesario. Si cambia el puerto, agregue una regla de grupo de seguridad correspondiente para permitir el acceso a la instancia. NOTA El puerto de la base de datos es el puerto del nodo mongos. El puerto predeterminado es 8635. Para cambiar el puerto, consulte Cambio de un puerto de base de datos. El puerto del nodo de shard es 8637, y el puerto del nodo de config es 8636, que no se puede cambiar. Para obtener más información sobre cómo conectarse a los nodos de disco y configuración, consulte Habilitación de direcciones IP de nodos de shard y config.
Enterprise Project	Solo los usuarios de empresa pueden utilizar esta función. Para utilizar esta función, póngase en contacto con el servicio de atención al cliente. Un proyecto empresarial es un modo de gestión de recursos en la nube, en el que los recursos y los miembros en la nube se gestionan de forma centralizada por proyecto. Seleccione un proyecto de empresa en la lista desplegable. El proyecto predeterminado es default . Para obtener más información acerca del proyecto de empresa, consulte <i>Guía del usuario de Enterprise</i> <i>Management</i> .

Figura 2-6 Configuración avanzada

Advanced Settings	
Automated Backup	0
Retention Period	- 7 + Enter an Integer from 1 to 732.
Time Window	00:00 - 01:00 • GMT+08:00
Maintenance Window	Skip Configure ⑦
Tags	It is recommended that you use TMS's predefined tag function to add the same tags to different cloud resources. C View predefined tags
	Tag key Tag value
	You can add 20 more tags.

Parámetro	Descripción
Automated Backup	DDS habilita una política de copia de respaldo automatizada de forma predeterminada, pero puede deshabilitarla después de crear una instancia. Una copia de respaldo completa automatizada se activa inmediatamente después de la creación de una instancia. Para obtener más información, consulte Configuración de una copia de respaldo automatizada .
Retention Period (days)	Retention Period se refiere al número de días que se conservan los datos. Puede aumentar el período de retención para mejorar la fiabilidad de los datos. El período de retención de copias de respaldo es de 1 a 732 días.
Time Window	Un período de una hora la copia de respaldo se programará dentro de las 24 horas, como 01:00-02:00. El tiempo de copia de respaldo está en formato UTC.

Tabla 2-7 Configuración avanzada

Parámetro	Descripción		
Tags	(Opcional) Puede agregar etiquetas a instancias DDS para que pueda buscar y filtrar rápidamente instancias especificadas por etiqueta. Cada instancia de DDS puede tener hasta 20 etiquetas.		
	 Crear una etiqueta. Puede crear etiquetas en la consola DDS y configurar key y value de la etiqueta. 		
	Key: Este parámetro es obligatorio.		
	 Cada clave de etiqueta debe ser única para cada instancia. 		
	– Una clave de etiqueta consta de hasta 36 caracteres.		
	 La clave debe consistir únicamente en dígitos, letras, guiones bajos (_), y guiones (-). 		
	Valor: Este parámetro es opcional.		
	 El valor consta de hasta 43 caracteres. 		
	 El valor debe consistir únicamente en dígitos, letras, guiones bajos (_), puntos y guiones (-). 		
	 Agregar una etiqueta predefinida. Las etiquetas predefinidas se pueden utilizar para identificar múltiples recursos en la nube. 		
	Para etiquetar un recurso en la nube, puede seleccionar una etiqueta predefinida creada en la lista desplegable, sin introducir una clave y un valor para la etiqueta.		
	Por ejemplo, si se ha creado una etiqueta predefinida, su clave es Usage y valor es Project1. Cuando configura la clave y el valor de un recurso en la nube, la etiqueta predefinida creada se mostrará en la página.		
	Después de crear una instancia, puede hacer clic en el nombre de la instancia para ver sus etiquetas. En la página Tags , también puede modificar o eliminar las etiquetas . Además, puede buscar y filtrar rápidamente instancias especificadas por etiqueta .		
	Puede agregar una etiqueta a una instancia después de crearla. Para obtener más información, consulte Adición de una etiqueta.		

Si tiene alguna pregunta sobre el precio, haga clic en Price Details.

NOTA

El rendimiento de la instancia depende de las especificaciones que seleccione durante la creación. Los elementos de configuración de hardware que se pueden seleccionar incluyen la clase de nodo y el espacio de almacenamiento.

Paso 3 En la página mostrada, confirme los detalles de la instancia.

- Para instancias anuales/mensuales
 - Si necesita modificar las especificaciones, haga clic en Previous para volver a la página anterior.

- Si no necesita modificar las especificaciones, lea y acepte el contrato de servicio y haga clic en **Pay Now** para ir a la página de pago y completar el pago.
- Para instancias de pago por uso
 - Si necesita modificar las especificaciones, haga clic en Previous para volver a la página anterior.
 - Si no necesita modificar las especificaciones, lea y acepte el contrato de servicio y haga clic en Submit para comenzar a crear la instancia.
- **Paso 4** Haga clic en **Back to Instance List**. Después de crear una instancia DDS, puede ver y gestionarla en la página **Instances**.
 - Cuando se crea una instancia, el estado que se muestra en la columna **Status** es **Creating**. Este proceso dura unos 15 minutos. Una vez completada la creación, el estado cambia a **Available**.
 - Las instancias anuales/mensuales que se compraron en lotes tienen las mismas especificaciones, excepto el nombre y el ID de la instancia.

----Fin

2.2 Conexión a una instancia de clúster

2.2.1 Métodos de conexión

Puede acceder a DDS a través de redes privadas o públicas.

Método	Direcció n IP	Escenario	Descripción
DAS	No requerido	DAS proporciona una GUI y le permite realizar operaciones visualizadas en la consola. La ejecución SQL, la gestión avanzada de bases de datos y la operación inteligente están disponibles para hacer que la gestión de bases de datos sea simple, segura e inteligente. De forma predeterminada, el permiso para conectarse a DAS está habilitado.	 Fácil de usar, seguro, avanzado e inteligente Recomendada

Tabla	2-8	Métodos	de	conexión
1.0010		111010400	au	contention

Método	Direcció n IP	Escenario	Descripción
Red privada	Dirección IP privada	DDS proporciona una dirección IP privada de forma predeterminada. Si sus aplicaciones se ejecutan en un ECS en la misma región y VPC que su instancia DDS, se recomienda utilizar una dirección IP privada para conectar el ECS a sus instancias DDS.	 Rendimiento seguro y excelente Para una transmisión más rápida y una seguridad mejorada, se recomienda migrar sus aplicaciones a un ECS que esté en la misma subred que su instancia de DDS y utilizar una dirección IP privada para acceder a la instancia.
Red pública	EIP	 Si las aplicaciones se ejecutan en un ECS que se encuentra en una región diferente de la donde se encuentra la instancia DDS, utilice una EIP para conectar el ECS a las instancias DDS. Si utiliza un dispositivo de terceros o su dispositivo local para conectarse a una instancia DDS, puede utilizar una EIP para conectarse a la instancia de base de datos. 	• Bajo nivel de seguridad

2.2.2 (Recomendado) Conexión a instancias de clúster mediante DAS

2.2.2.1 Descripción

DAS proporciona una GUI y le permite realizar operaciones visualizadas en la consola. La ejecución SQL, la gestión avanzada de bases de datos y la operación inteligente están disponibles para hacer que la gestión de bases de datos sea simple, segura e inteligente. Se recomienda utilizar DAS para conectarse a instancias.

En esta sección se describe cómo comprar una instancia de clúster en la consola de gestión y cómo conectarse a la instancia de clúster a través de DAS.

Proceso

Para comprar y conectarse a una instancia de clúster, realice los siguientes pasos:

- 1. Comprar una instancia de clúster.
- 2. Conectarse a la instancia del clúster a través de DAS.

2.2.2.2 Conexión a una instancia de clúster mediante DAS

Data Admin Service (DAS) le permite gestionar instancias de bases de datos en una consola basada en web, simplificando la gestión de bases de datos y mejorando la eficiencia del trabajo. Puede conectar y gestionar instancias a través de DAS. De forma predeterminada, tiene el permiso necesario para el inicio de sesión remoto. Se recomienda utilizar el servicio DAS para conectarse a instancias de base de datos. DAS es seguro y conveniente.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic 🔍 en la esquina superior izquierda y seleccione una región y un proyecto.

Si desea recursos informáticos y de red dedicados a su uso exclusivo, **habilite un DeC** y **solicite recursos de DCC**. Después de habilitar un DeC, puede seleccionar la región y el proyecto de DeC.

- **Paso 3** Haga clic = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.
- Paso 4 En la página Instances, busque la instancia de base de datos de destino y haga clic en Log In en la columna Operation.

También puede hacer clic en la instancia de destino en la página **Instances**. En la página **Basic Information** mostrada, haga clic en **Log In** en la esquina superior derecha de la página.

- Paso 5 En el cuadro de diálogo Instance Login, introduzca la información correcta y haga clic en Log In para acceder a la base de datos y gestionarla.
- **Paso 6** Una vez que el inicio de sesión se haya realizado correctamente, puede realizar operaciones como crear una base de datos, gestionar cuentas y bases de datos.

Para obtener más información, consulte Gestión de datos.

----Fin

2.2.3 Conexión a una instancia de clúster a través de una red privada

2.2.3.1 Configuración de reglas de grupo de seguridad

Un grupo de seguridad es una colección de reglas de control de acceso para ECS e instancias de DDS que tienen los mismos requisitos de protección de seguridad y son de confianza mutua en una VPC.

Para garantizar la seguridad y confiabilidad de la base de datos, debe configurar reglas de grupo de seguridad para permitir que las direcciones IP y los puertos específicos accedan a instancias de DDS.

Puede conectarse a una instancia mediante la configuración de las reglas de grupo de seguridad de las dos maneras siguientes:

• Si el ECS y la instancia están en el mismo grupo de seguridad, pueden comunicarse entre sí de forma predeterminada. No es necesario configurar ninguna regla de grupo de seguridad. Vaya a Conexión a una instancia de clúster mediante Mongo Shell (red privada).

Figura 2-7 Mismo grupo de seguridad



• Si el ECS y la instancia están en diferentes grupos de seguridad, debe configurar las reglas de grupo de seguridad para ellos, por separado.





- Instancia: configura una inbound rule para el grupo de seguridad asociado a la instancia.
- ECS: La regla de grupo de seguridad predeterminada permite todos los paquetes de datos salientes. En este caso, no es necesario configurar una regla de grupo de seguridad para el ECS. Si no se permite que todo el tráfico llegue a la instancia, configure una regla de **outbound** para el ECS.

Esta sección describe cómo configurar una regla de inbound para una instancia.

Precauciones

- De forma predeterminada, una cuenta puede crear hasta 500 reglas de grupo de seguridad.
- Demasiadas reglas de grupo de seguridad aumentarán la latencia del primer paquete, por lo que se recomienda un máximo de 50 reglas para cada grupo de seguridad.
- Una instancia DDS solo puede asociarse a un grupo de seguridad.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

- Paso 2 Haga clic en 💿 en la esquina superior izquierda, y seleccione una región y un proyecto.
- **Paso 3** Haga clic en = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia. Se muestra la página Basic Information.
- **Paso 5** En el área **Network Information** de la página **Basic Information**, haga clic en el grupo de seguridad.

Figura 2-9 Grupo de seguridad

Network Information			
VPC	dds-st-test-vpc	Subnet	dds-st-test-subnet-2 (1)
Security Group	Sys-default 🖉	Database Port	8635 🖉

También puede elegir **Connections** en el panel de navegación de la izquierda. En la pestaña **Private Connection**, en el área **Security Group**, haga clic en el nombre del grupo de seguridad.

Figura 2-10 Grupo de seguridad

Security Group				
Security Group	Sys-default 🖉			
Add Rule	Delete			С
Inbound Rules(1)	Outbound Rules	(1)		
Protocol & Port (?)		Source (?)	Description	
All		Sys-default		

- Paso 6 En la página Security Group, busque el grupo de seguridad de destino y haga clic en Manage Rule en la columna Operation.
- Paso 7 En la pestaña Inbound Rules, haga clic en Add Rule. Aparece el cuadro de diálogo Add Inbound Rule.
- Paso 8 Agregue una regla de grupo de seguridad como se le solicite.

Figura 2-11 Agregar regla de entrada

Add Inbound Rule Learn more about security group configuration.				
inbound rules allow incoming traffic to	instances associated with the	security group.		
Security Group Sys-default You can import multiple rules in a batch.				
Protocol & Port ?	Туре	Source ⑦	Description	Operation
TCP Example: 22 or 22-30	IPv4 v	IP address ▼ 0.0.0.0/0		Operation 🗸
	\oplus Ad	dd Rule		
		OK Cancel		

Tabla 2-9 Configuración de reglas entrantes

Parámetro	Descripción	Ejemplo
Priority	Prioridad de regla de grupo de seguridad. El valor de prioridad varía de 1 a 100. La prioridad predeterminada es 1 y tiene la prioridad más alta. La regla de grupo de seguridad con un valor menor tiene mayor prioridad.	1
Action	Las acciones de la regla del grupo de seguridad. Una regla con una acción de denegación invalida a otra con una acción de permiso si las dos reglas tienen la misma prioridad.	Allow
Protocol & Port	El protocolo de red requerido para el acceso. Opciones disponibles: TCP, UDP, ICMP, o GRE	ТСР
	Puerto: el puerto en el que desea permitir el acceso a DDS. El puerto predeterminado es 8635. El puerto oscila entre 2100 y 9500 o puede ser 27017, 27018, o 27019.	8635
Туре	Tipo de dirección IP. Solo IPv4 y IPv6 son compatibles.	IPv4

Parámetro	Descripción	Ejemplo
Source	Especifica la dirección IP, el grupo de seguridad y el grupo de direcciones IP compatibles, que permiten el acceso desde direcciones IP o instancias de otro grupo de seguridad. Ejemplo:	0.0.0/0
	• Dirección IP única: 192.168.10.10/32	
	 Segmento de dirección IP: 192.168.1.0/24 	
	• Todas las direcciones IP: 0.0.0.0/0	
	• Grupo de seguridad: sg-abc	
	• Grupo de direcciones IP: ipGroup-test	
	Si introduce un grupo de seguridad, todos los ECS asociados al grupo de seguridad cumplen con la regla creada.	
	Para obtener más información acerca de los grupos de direcciones IP, consulte Grupo de direcciones IP .	
Description	(Opcional) Proporciona información adicional acerca de la regla del grupo de seguridad. Este parámetro es opcional.	-
	La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	

Paso 9 Haga clic en OK.

----Fin

2.2.3.2 Conexión a una instancia de clúster mediante Mongo Shell (red privada)

Mongo shell es el cliente por defecto para el servidor de base de datos MongoDB. Puede utilizar Mongo Shell para conectarse a instancias de base de datos y consultar, actualizar y gestionar datos en bases de datos. Para usar Mongo Shell, descargue e instale primero el cliente MongoDB y, a continuación, use el shell Mongo para conectarse a la instancia de base de datos.

De forma predeterminada, una instancia DDS proporciona una dirección IP privada. Si sus aplicaciones se despliegan en un ECS y están en la misma región y VPC que las instancias DDS, puede conectarse a las instancias DDS mediante una dirección IP privada para lograr una velocidad de transmisión rápida y una alta seguridad.

En esta sección se describe cómo utilizar Mongo Shell para conectarse a una instancia de clúster a través de una red privada.

Puede conectarse a una instancia mediante una conexión SSL o una conexión sin cifrar. La conexión SSL es encriptada y más segura. Para mejorar la seguridad de la transmisión de datos, conéctese a instancias mediante SSL.

Prerrequisitos

- 1. Para obtener más información acerca de cómo crear e iniciar sesión en un ECS, consulte Comprar un ECS e iniciar sesión en un ECS.
- 2. Instale el cliente MongoDB en el ECS. Para garantizar la autenticación correcta, instale el cliente MongoDB de la misma versión que la instancia de destino.

Para obtener más información sobre cómo instalar un cliente MongoDB, consulte ¿Cómo puedo instalar un cliente MongoDB?

3. El ECS puede comunicarse con la instancia DDS. Para obtener más información, véase **Configuración de reglas de grupo de seguridad**.

Conexión de SSL

AVISO

Si se conecta a una instancia a través de la conexión SSL, habilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo habilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

- Paso 1 Inicie sesión en la consola de gestión.
- Paso 2 Haga clic en 🔍 en la esquina superior izquierda, y seleccione una región y un proyecto.
- Paso 3 Haga clic en = en la esquina superior izquierda de la página y elija Databases > Document Database Service.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia.
- Paso 5 En el panel de navegación de la izquierda, elija Connections.
- Paso 6 En el área Basic Information, haga clic en 📥 junto al campo SSL.
- Paso 7 Cargue el certificado raíz al ECS para conectarse a la instancia.

A continuación se describe cómo cargar el certificado en un ECS de Linux y Windows:

- En Linux, ejecute el siguiente comando:
 - scp

<IDENTITY_FILE><REMOTE_USER>@<REMOTE_ADDRESS>:<REMOTE_DIR>

🛄 NOTA

- IDENTITY_FILE es el directorio donde reside el certificado raíz. El permiso de acceso al archivo es 600.
- **REMOTE_USER** es el usuario del sistema operativo de ECS.
- **REMOTE_ADDRESS** es la dirección de ECS.
- **REMOTE_DIR** es el directorio del ECS al que se carga el certificado raíz.
- En Windows, cargue el certificado raíz mediante una herramienta de conexión remota.
- Paso 8 Conéctese a la instancia en el directorio donde se encuentra el cliente MongoDB.

Método 1: Uso de la dirección de conexión HA privada (recomendado)

DDS proporciona una dirección de conexión HA privada que consiste en direcciones IP y puertos de todos los nodos mongos en una instancia de clúster. Puede utilizar esta dirección para conectarse a la instancia de clúster para mejorar la disponibilidad de la instancia de clúster.

Ejemplo de comando:

```
./mongo <Private HA connection address> --ssl --sslCAFile <FILE_PATH> --
sslAllowInvalidHostnames
```

Descripción de parámetros:

• Private HA Connection Address: En la página Instances, haga clic en el nombre de la instancia. Se muestra la página Basic Information. Elija Connections. Haga clic en la pestaña Private Connection y obtenga la dirección de conexión de la instancia actual en el campo Private HA Connection Address.

Figura 2-12 Obtención de la dirección de conexión HA privada

Private Connection	Public Connection			
Basic Information				
Database Port	8635 🖉	VPC	dds-st-test-vpc	
SSL	T T	Subnet	dds-st-test-subnet-2 ()	
Auto-switch Private IP Address				
Address				
Cross-CIDR Access	Disabled Enable			
Private HA Connection	Private HA Connection Address mongodb://rwuser: <password>@ //test?authSource=admin&replicaSet=replica 🗗 Learn more</password>			

El formato de la dirección de conexión HA privada es el siguiente. El nombre de usuario de la base de datos **rwuser** y la base de datos de autenticación **admin** no se pueden cambiar.

mongodb://**rwuser:**<*password*>@192.168.xx.xx:8635,192.168.xx.xx:8635/**test? authSource=admin**

Preste atención a los siguientes parámetros en la dirección HA privada:

Tabla	2-10	Informac	ión de	parámetros
-------	------	----------	--------	------------

Parámetro	Descripción		
rwuser	Nombre de usuario de la base de datos		
<password></password>	Contraseña para el nombre de usuario de la base de datos. Reemplácelo con la contraseña real.		
	Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.		
	Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25*** %21%24.		

Parámetro	Descripción
192.168.xx.xx:8635,192.1 68.xx.xx:8635	Dirección IP y puerto del nodo mongos de la instancia de clúster que se va a conectar
test	El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.
authSource=admin	La base de datos de autenticación del usuario rwuser debe ser admin . authSource=admin está fijo en el comando.

- FILE_PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: Para asegurarse de que la comunicación interna del clúster no ocupe recursos como la dirección IP del usuario y el ancho de banda, el certificado del clúster se genera mediante la dirección IP de gestión interna. -sslAllowInvalidHostnames es necesario para la conexión SSL a través de una red privada.

Ejemplo de comandos:

./mongo mongodb://rwuser:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/test? authSource=admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames

Método 2: Uso de la dirección de conexión HA privada (base de datos y cuenta definidas por el usuario)

Ejemplo de comando:

```
./mongo <Private HA connection address> --ssl --sslCAFile <FILE_PATH> --
sslAllowInvalidHostnames
```

Descripción de parámetros:

 Private HA Connection Address: En la página Instances, haga clic en el nombre de la instancia. Se muestra la página Basic Information. Elija Connections. Haga clic en la pestaña Private Connection y obtenga la dirección de conexión de la instancia actual en el campo Private HA Connection Address.

Figura 2-13 Obtención de la dirección de conexión HA privada

vrivate Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	Ū ₹	Subnet	dds-st-test-subnet-2 ()
Auto-switch Private IP Address			
Address			
Cross-CIDR Access	Disabled Enable		
Private HA Connection	n Address mongodb://rwuser: <password>@*</password>		/test?authSource=admin&replicaSet=replica 🗇 Learn more

El formato de la dirección de conexión HA privada obtenida es el siguiente:

mongodb://**rwuser:**<*password*>@192.168.xx.xx:8635,192.168.xx.xx:8635/**test? authSource=admin**

La siguiente tabla muestra los parámetros requeridos en la dirección de HA privada.

Parámetro	Descripción		
rwuser	Nombre de usuario de base de datos. El valor predeterminado es rwuser . Puede cambiar el valor por el nombre de usuario en función de sus requisitos de servicio.		
<password></password>	Contraseña para el nombre de usuario de la base de datos. Reemplácelo con la contraseña real.		
	Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.		
	Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25*** %21%24 .		
192.168.xx.xx:8635,192.1 68.xx.xx:8635	Dirección IP y puerto del nodo mongos de la instancia de clúster que se va a conectar		
test	El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.		
authSource=admin	La base de datos de autenticación de usuario rwuser es admin .		
	NOTA Si utiliza una base de datos definida por el usuario para la autenticación, cambie la base de datos de autenticación en la dirección de conexión HA por el nombre de la base de datos definida por el usuario. Además, reemplace rwuser con el nombre de usuario creado en la base de datos definida por el usuario.		

Tabla 2-11 Inform	ación de	parámetros
-------------------	----------	------------

- FILE_PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: Para asegurarse de que la comunicación interna del clúster no ocupe recursos como la dirección IP del usuario y el ancho de banda, el certificado del clúster se genera mediante la dirección IP de gestión interna. -sslAllowInvalidHostnames es necesario para la conexión SSL a través de una red privada.

Por ejemplo, si crea una base de datos definida por el usuario **Database** y un usuario **test1** en la base de datos, el comando de conexión es el siguiente:

./mongo mongodb://test1:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/Database? authSource=Database --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames

Método 3: Usar una dirección IP privada

Ejemplo de comando:

```
./mongo --host <DB_HOST> --port <DB_PORT> -u <DB_USER> -p --
authenticationDatabase admin --ssl --sslCAFile <FILE_PATH> --
sslAllowInvalidHostnames
```

Descripción de parámetros:

• **DB_HOST** es la dirección IP del nodo mongos de la instancia de clúster que se va a conectar.

Haga clic en el nombre de la instancia. En la página **Basic Information**, elija **Connections** > **Private Connection**, obtenga la dirección IP privada del nodo mongos en la pestaña **mongos** en el área **Node Information**.

Figura 2-14 Obtención de la dirección IP privada

rivate Connection	Public Conn	nection			
Basic Information					
Database Port	8635 🖉			VPC	dds-st-test-vpc
SSL				Subnet	dds-st-test-subnet-2 ()
Address					
Private HA Connection A	Address mor	ngodb://rwuser:< <mark>password</mark> :	>@	t	est?authSource=admin 🗗 Learn more
Node Information	config	The parameters in ora	nge are variables and ne	ed to be modified b	ased on service requirements. For details, click Learn more.
Name/ID A2	z	Private IP Address	Private Domain Name	EIP	Operation
dds-c582_xwx az	2	192.	b382774b302b46608	Our Contract Output Contrac	Change Private IP Address More 👻
dds-c582_xwx az	2	192.	b7a18e7fdb184f639a	Onbound	Change Private IP Address More 👻

• **DB_PORT** es el puerto de la instancia que se va a conectar. El puerto predeterminado es 8635.

Haga clic en el nombre de la instancia. En la página **Basic Information**, elija **Connections**. En la pestaña **Private Connection**, obtenga la información del puerto de la base de datos en el campo **Database Port** en el área **Basic Information**.

Figura 2-15 Obtención del puerto

Private Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	Ŧ	Subnet	dds-st-test-subnet ()

- **DB_USER** es el usuario de la base de datos. El valor predeterminado es **rwuser**.
- FILE PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: Para asegurarse de que la comunicación interna del clúster no ocupe recursos como la dirección IP del usuario y el ancho de banda, el
certificado del clúster se genera mediante la dirección IP de gestión interna. -sslAllowInvalidHostnames es necesario para la conexión SSL a través de una red privada.

Introduzca la contraseña de la cuenta de la base de datos cuando se le solicite:

Enter password:

Ejemplo de comandos:

./mongo --host 192.168.1.6 --port 8635 -u rwuser -p --authenticationDatabase admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames

Paso 9 Compruebe el resultado de la conexión. Si se muestra la siguiente información, la conexión se realiza correctamente.

----Fin

mongos>

Conexión sin encriptar

AVISO

Si se conecta a una instancia a través de una conexión no cifrada, deshabilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo deshabilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

Paso 1 Conéctese al ECS.

Paso 2 Conéctese a la instancia en el directorio donde se encuentra el cliente MongoDB.

Método 1: Dirección de conexión privada HA (recomendado)

Ejemplo de comando:

./mongo "<Private HA Connection Address>"

Private HA Connection Address: En la página **Instances**, haga clic en el nombre de la instancia. Se muestra la página **Basic Information**. Elija **Connections**. Haga clic en la pestaña **Private Connection** y obtenga la dirección de conexión de la instancia actual en el campo **Private HA Connection Address**.

Figura 2-16 Obtención de la dirección de conexión HA privada

ivate Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	▲	Subnet	dds-st-test-subnet-2 ()
Auto-switch Private IP Address			
Address			
Cross-CIDR Access	Disabled Enable		
Private HA Connection	Address mongodb://rwuser: <password>@'</password>		/test?authSource=admin&replicaSet=replica 🗗 Learn more

El formato de la dirección de conexión HA privada es el siguiente. El nombre de usuario de la base de datos **rwuser** y la base de datos de autenticación **admin** no se pueden cambiar.

mongodb://rwuser:<*password*>@192.168.xx.xx:8635,192.168.xx.xx:8635/test? authSource=admin

La siguiente tabla muestra los parámetros requeridos en la dirección de HA privada.

Parámetro	Descripción
rwuser	Nombre de usuario de la base de datos
<password></password>	Contraseña para el nombre de usuario de la base de datos. Reemplácelo con la contraseña real.
	Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.
	Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25***%21%24 .
192.168.xx.xx:8635,192.168 .xx.xx:8635	Dirección IP y puerto del nodo mongos de la instancia de clúster que se va a conectar
test	El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.
authSource=admin	La base de datos de autenticación del usuario rwuser debe ser admin . authSource=admin está fijo en el comando.

Tabla 2-12 Información de parámetros

Ejemplo de comandos:

./mongo mongodb://rwuser:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/test? authSource=admin

Método 2: Conexión HA privada (base de datos y cuenta definidas por el usuario)

Ejemplo de comando:

./mongo "<Private HA Connection Address>"

Private HA Connection Address: En la página **Instances**, haga clic en el nombre de la instancia. Se muestra la página **Basic Information**. Elija **Connections**. Haga clic en la pestaña **Private Connection** y obtenga la dirección de conexión de la instancia actual en el campo **Private HA Connection Address**.

Figura 2-17 Obtención de la dirección de conexión HA privada

Private Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	▲	Subnet	dds-st-test-subnet-2 (
Auto-switch Private IP Address			
Address			
Cross-CIDR Access	Disabled Enable		
Private HA Connection	Address mongodb://rwuser: <password>@</password>	/1	test?authSource=admin&replicaSet=replica 🗖 Learn more

El formato de la dirección de conexión HA privada obtenida es el siguiente:

mongodb://**rwuser:**<*password*>@192.168.xx.xx:8635,192.168.xx.xx:8635/**test? authSource=admin**

La siguiente tabla muestra los parámetros requeridos en la dirección de HA privada.

Parámetro	Descripción
rwuser	Nombre de usuario de base de datos. El valor predeterminado es rwuser . Puede cambiar el valor por el nombre de usuario en función de sus requisitos de servicio.
<pre><password></password></pre>	Contraseña para el nombre de usuario de la base de datos. Reemplácelo con la contraseña real.
	Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.
	Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25***%21%24 .
192.168.xx.xx:8635,192.168 .xx.xx:8635	Dirección IP y puerto del nodo mongos de la instancia de clúster que se va a conectar
test	El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.
authSource=admin	La base de datos de autenticación de usuario rwuser es admin .
	NOTA Si utiliza una base de datos definida por el usuario para la autenticación, cambie la base de datos de autenticación en la dirección de conexión HA por el nombre de la base de datos definida por el usuario. Además, reemplace rwuser con el nombre de usuario creado en la base de datos definida por el usuario.

 Tabla 2-13 Información de parámetros

Por ejemplo, si crea una base de datos definida por el usuario **Database** y un usuario **test1** en la base de datos, el comando de conexión es el siguiente:

./mongo mongodb://test1:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/Database? authSource=Database

Método 3: Usar una dirección IP privada

Ejemplo de comando:

./mongo --host <*DB_HOST*> --port <*DB_PORT*> -u <*DB_USER*> -p -authenticationDatabase admin

Descripción de parámetros:

• **DB_HOST** es la dirección IP del nodo mongos de la instancia de clúster que se va a conectar.

Haga clic en el nombre de la instancia. En la página **Basic Information**, elija **Connections** > **Private Connection**, obtenga la dirección IP privada del nodo mongos en la pestaña **mongos** en el área **Node Information**.

Figura 2-18 Obtención de la dirección IP privada

asic Information						
atabase Port	8635 🖉		N N	VPC	dds-st-test-vpc	
SL		Ŧ	2	Subnet	dds-st-test-subnet-2 ()	
ddress						
rivate HA Connection A	Address n	nongodb://rwuser: <passwor< td=""><td>'d>@</td><td></td><td>test?authSource=admin 🗗 Learn more</td><td></td></passwor<>	'd>@		test?authSource=admin 🗗 Learn more	
	P	Note The parameters in c	orange are variables and nee	ed to be modified l	based on service requirements. For details, click Learn i	more.
lode Information	r con	Note The parameters in c	orange are variables and nee	ed to be modified l	based on service requirements. For details, click Learn i	more.
lode Information mongos shard Name/ID A	l cont	tote The parameters in o	Private Domain Name	ed to be modified b	based on service requirements. For details, click Learn i Operation	more.
Node Information mongos shard Name/ID A dds-c582_xwx au	I con z z2	The parameters in c fig Private IP Address 192.	Private Domain Name b382774b302b46608	EIP S Unbound	Dased on service requirements. For details, click Learn of Operation Change Private IP Address More +	more.

• **DB_PORT** es el puerto de la instancia que se va a conectar. El puerto predeterminado es 8635.

Haga clic en el nombre de la instancia. En la página **Basic Information**, elija **Connections**. En la pestaña **Private Connection**, obtenga la información del puerto de la base de datos en el campo **Database Port** en el área **Basic Information**.

Figura 2-19 Obtención del puerto

Private Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	Ŧ	Subnet	dds-st-test-subnet (

• DB_USER es el usuario de la base de datos. El valor predeterminado es rwuser.

Introduzca la contraseña de la base de datos cuando se le solicite: Enter password:

Ejemplo de comandos:

./mongo --host 192.168.1.6 --port 8635 -u rwuser -p --authenticationDatabase admin

Paso 3 Compruebe el resultado de la conexión. Si se muestra la siguiente información, la conexión se realiza correctamente.

----Fin

2.2.4 Conexión a una instancia de clúster a través de una red pública

2.2.4.1 Vinculación y desvinculación de una EIP

Después de crear una instancia de clúster, puede enlazar una EIP a ella para permitir el acceso externo. Si más adelante desea prohibir el acceso externo, también puede desvincular la EIP de la instancia.

Precauciones

- La supresión de una EIP vinculada no significa que la EIP no esté vinculada.
- Antes de acceder a una base de datos, solicite una EIP en la consola de VPC. A continuación, agregue una regla de entrada para permitir las direcciones IP o los intervalos de direcciones IP de los ECS. Para obtener más información, véase Configuración de un grupo de seguridad.
- En la instancia de clúster, solo mongos puede tener una vinculación de EIP. Para cambiar la EIP que se ha enlazado a un nodo, primero debe desvincularlo del nodo.

Vinculación de una EIP

- Paso 1 Inicie sesión en la consola de gestión.
- **Paso 2** Haga clic en 🔍 en la esquina superior izquierda y seleccione una región y un proyecto.
- **Paso 3** Haga clic en = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia del clúster.
- Paso 5 En el panel de navegación de la izquierda, elija Connections. Haga clic en la pestaña Public Connection. En el área Basic Information, localice el nodo mongos y haga clic en Bind EIP en la columna Operation.

Figura 2-20 Vinculación de una EIP

e Connection	Public Con	nection			
asic Information	1				
atabase Port	8635 🖉		s	SL	Ť
ddress					
ublic Network Con	nection Address	Unbound			
Name/ID	AZ	Private IP Address	Private Domain Name	EIP	Operation
dds-c582_xwx	az2	192.168.21.111	b382774b302b46608	Onbound	Change Private IP Address More 🔺
					Change Private Domain Name

Alternativamente, en el área **Node Information** página **Basic Information**, localice el nodo mongos y elija **More** > **Bind EIP** en la columna **Operation**.

Figura 2-21 Vinculación de una EIP



Paso 6 En el cuadro de diálogo que se muestra, se muestran todos las EIP independientes disponibles. Seleccione la EIP requerido y haga clic en OK. Si no se muestran EIPs disponibles, haga clic en View EIP y cree una EIP en la consola de VPC.

Figura 2-22 Selección de una EIP

outbound and int	oound rules in th	e security group.		-
Node Information	Node Name		Status	
		_mongos_node_1	 Available 	
Select EIP				
EIP		Status	Bandwidth	
		⊗ Unbound	5 Mbit/s	
0		⊗ Unbound	5 Mbit/s	
0		S Unbound	88 Mbit/s	

Paso 7 En la columna EIP de la pestaña mongos, puede ver la EIP que estaba enlazado.
Para desvincular una EIP de la instancia, consulte Desvinculación de una EIP.
----Fin

Desvinculación de una EIP

Paso 1 Inicie sesión en la consola de gestión.

- **Paso 2** Haga clic en 🔍 en la esquina superior izquierda y seleccione una región y un proyecto.
- **Paso 3** Haga clic en = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia del clúster.
- Paso 5 En el panel de navegación de la izquierda, elija Connections. Haga clic en la pestaña Public Connection. En el área Basic Information, localice el nodo mongos y haga clic en Unbind EIP en la columna Operation.

Name/	AZ	Private IP Addre	EIP	Operation
b76d17	azlpo	192.168.106.237		Change Private IP Address Unbind EIP
65fd4c	azlpo	192.168.111.99	Our Contract Out Contract Ou	Change Private IP Address Bind EIP

Figura 2-23 Desvinculación de una EIP

Alternativamente, en el área **Node Information** de la página **Basic Information**, localice el nodo mongos y elija **More** > **Unbind EIP** en la columna **Operation**.

Figura 2-24 Desvinculación de una EIP

Node Information						
mongos shard config						
Add mongos						
Q Select one or more filters from the pop-up lists.	If you enter a keyword wi	hout a filter applied, the system	will search for all names mat	ching this keyword.		
Name/ID	Status	Node Class	AZ	Private IP Address	EIP	Operation
dds-ea44_mongos_node_1 8aa255e236e34eeb8522891ce32cb25eno02	Available	Enhanced II 2 vCPUs	az1	192.168.0.60	159.138.235.185	Change Class Restart More ▲
dds-ea44_mongos_node_2 872f23330ea3429a8fcd7ce609b2e7b3no02	 Available 	Enhanced II 2 vCPUs	az1	192.168.0.128	Unbound	Change Change Private IP Address
						Lipbind EIP

Paso 6 En el cuadro de diálogo que se muestra, haga clic en Yes.

Para enlazar una EIP a la instancia de nuevo, consulte Vinculación de una EIP.

----Fin

2.2.4.2 Configuración de un grupo de seguridad

Un grupo de seguridad es una colección de reglas de control de acceso para ECS e instancias de DDS que tienen los mismos requisitos de protección de seguridad y son de confianza mutua en una VPC.

Para garantizar la seguridad y confiabilidad de la base de datos, debe configurar reglas de grupo de seguridad para permitir que las direcciones IP y los puertos específicos accedan a instancias de DDS.

Para tener acceso a una instancia desde Internet, agregue una regla de entrada para el grupo de seguridad asociado a la instancia.

Precauciones

- De forma predeterminada, una cuenta puede crear hasta 500 reglas de grupo de seguridad.
- Demasiadas reglas de grupo de seguridad aumentarán la latencia del primer paquete, por lo que se recomienda un máximo de 50 reglas para cada grupo de seguridad.
- Una instancia DDS solo puede asociarse a un grupo de seguridad.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

- **Paso 2** Haga clic en 🔍 en la esquina superior izquierda y seleccione una región y un proyecto.
- Paso 3 Haga clic en = en la esquina superior izquierda de la página y elija Databases > Document Database Service.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia. Se muestra la página Basic Information.
- **Paso 5** En el área **Network Information** de la página **Basic Information**, haga clic en el grupo de seguridad.

Figura 2-25 Grupo de seguridad

Network Information			
VPC	dds-st-test-vpc	Subnet	dds-st-test-subnet-2 (1)
Security Group	Sys-default 🖉	Database Port	8635 🖉

También puede elegir **Connections** en el panel de navegación de la izquierda. En la pestaña **Public Connection**, en el área **Security Group**, haga clic en el nombre del grupo de seguridad.

Figura 2-26 Grupo de seguridad

Security Group		
Security Group Sys-default 🖉		
Add Rule Delete		C
Inbound Rules(1) Outbound Rules	(1)	
Protocol & Port ?	Source (?)	Description
All	Sys-default	-

- Paso 6En la página Security Group, busque el grupo de seguridad de destino y haga clic en
Manage Rule en la columna Operation.
- Paso 7 En la pestaña Inbound Rules, haga clic en Add Rule. Aparece el cuadro de diálogo Add Inbound Rule.
- Paso 8 Agregue una regla de grupo de seguridad como se le solicite.

Figura 2-27 Agregar regla de entrada

Add Inbound Rule Learn more about security group configuration.								
1 Inbound rules allow incoming traffic to instances associated with the security group.								
Security Group Sys-default You can import multiple rules in a batcl	h.							
Protocol & Port ⑦	Туре	Source 🕐	Description	Operation				
TCP Example: 22 or 22-30	IPv4 v	IP address 0.0.0.0/0	•	Operation 🗸				
Add Rule								
		OK Cancel						

Tabla 2-14 Configuración de reglas entrantes

Parámetro	Descripción	Valor de ejemplo
Priority	Prioridad de regla de grupo de seguridad. El valor de prioridad varía de 1 a 100. La prioridad predeterminada es 1 y tiene la prioridad más alta. La regla de grupo de seguridad con un valor menor tiene mayor prioridad.	1
Action	Las acciones de la regla del grupo de seguridad. Una regla con una acción de denegación invalida a otra con una acción de permiso si las dos reglas tienen la misma prioridad.	Allow
Protocol & Port	El protocolo de red requerido para el acceso. La opción puede ser All, TCP, UDP, ICMP, o GRE.	ТСР
	Puerto: el puerto en el que desea permitir el acceso a DDS. El puerto predeterminado es 8635. El puerto oscila entre 2100 y 9500 o puede ser 27017, 27018, o 27019.	8635
Туре	Tipo de dirección IP. Solo IPv4 y IPv6 son compatibles.	IPv4

Parámetro	Descripción	Valor de ejemplo
Source	Especifica la dirección IP, el grupo de seguridad y el grupo de direcciones IP compatibles, que permiten el acceso desde direcciones IP o instancias de otro grupo de seguridad. Ejemplo:	0.0.0/0
	• Dirección IP única: 192.168.10.10/32	
	 Segmento de dirección IP: 192.168.1.0/24 	
	• Todas las direcciones IP: 0.0.0/0	
	• Grupo de seguridad: sg-abc	
	• Grupo de direcciones IP: ipGroup-test	
	Si introduce un grupo de seguridad, todos los ECS asociados al grupo de seguridad cumplen con la regla creada.	
	Para obtener más información acerca de los grupos de direcciones IP, consulte Grupo de direcciones IP .	
Description	(Opcional) Proporciona información adicional acerca de la regla del grupo de seguridad. Este parámetro es opcional.	-
	La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	

Paso 9 Haga clic en OK.

----Fin

2.2.4.3 Conexión a una instancia de clúster mediante Mongo Shell (Red pública)

En los siguientes escenarios, puede acceder a una instancia DDS desde Internet vinculando una EIP a la instancia.

Escenario 1: Las aplicaciones se despliegan en un ECS y no están en la misma región que la instancia DDS.



Figura 2-28 Acceso a DDS desde ECS en todas las regiones

Escenario 2: Sus aplicaciones se despliegan en un servidor en la nube proporcionado por otros proveedores.



Figura 2-29 Acceso a DDS desde otros servidores en la nube

En esta sección se describe cómo utilizar Mongo Shell para conectarse a una instancia de clúster a través de una red pública.

Puede conectarse a una instancia mediante una conexión SSL o una conexión sin cifrar. La conexión SSL es encriptada y más segura. Para mejorar la seguridad de la transmisión de datos, conéctese a instancias mediante SSL.

Prerrequisitos

- 1. Para obtener más información acerca de cómo crear e iniciar sesión en un ECS, consulte Comprar un ECS e iniciar sesión en un ECS.
- 2. Vincule una EIP a la instancia del clúster y establezca reglas de grupo de seguridad para garantizar que se pueda acceder a la instancia desde el ECS.
- 3. Instale el cliente MongoDB en el ECS.

Para obtener más información sobre cómo instalar un cliente MongoDB, consulte ¿Cómo puedo instalar un cliente MongoDB?

SSL

AVISO

Si se conecta a una instancia a través de la conexión SSL, habilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo habilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

Paso 1 Inicie sesión en la consola de gestión.

- **Paso 2** Haga clic en 🔍 en la esquina superior izquierda y seleccione una región y un proyecto.
- **Paso 3** Haga clic en = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia.
- Paso 5 En el panel de navegación de la izquierda, elija Connections.
- Paso 6 En el área Basic Information, haga clic en 📥 junto al campo SSL.
- Paso 7 Cargue el certificado root obtenido en Paso 6 al ECS.

A continuación se describe cómo cargar el certificado en un ECS de Linux y Windows:

• En Linux, ejecute el siguiente comando:

scp<IDENTITY_FILE><REMOTE_USER>@<REMOTE_ADDRESS>:<REMOTE_DI
R>

NOTA

- IDENTITY_FILE es el directorio donde reside el certificado raíz. El permiso de acceso al archivo es 600.
- **REMOTE_USER** es el usuario del sistema operativo de ECS.
- **REMOTE_ADDRESS** es la dirección de ECS.
- **REMOTE_DIR** es el directorio del ECS al que se carga el certificado raíz.
- En Windows, cargue el certificado raíz mediante una herramienta de conexión remota.
- Paso 8 Conéctese a la instancia en el directorio donde se encuentra el cliente MongoDB.

Método 1: Uso de una dirección de conexión de red pública

Ejemplo de comando:

./mongo <Public network connection address> --ssl --sslCAFile <FILE_PATH> -sslAllowInvalidHostnames

Descripción de parámetros:

 Public Network Connection Address: En la página Instances, haga clic en la instancia para cambiar a la página Basic Information. En el panel de navegación de la izquierda, elija Connections. En la página mostrada, haga clic en la pestaña Public Connection. En el área Address, obtenga la dirección de conexión de instancia del campo Public Network Connection Address. Figura 2-30 Obtención de la dirección de conexión de red pública

Private Connection	Public Cor	inection	
Basic Information			
Database Port	8635 🖉	SSL	▲
Address			
Public Network Connect	ion Address	mongodb://rwuser: <password>@:</password>	:8635/test?authSource=
		admin 🗇	

El formato de la dirección de conexión pública es el siguiente. El nombre de usuario de la base de datos **rwuser** y la base de datos de autenticación **admin** no se pueden cambiar.

mongodb://**rwuser:**<*password*>@192.168.xx.xx:8635/**test?authSource=admin** Preste atención a los siguientes parámetros en la dirección de conexión pública:

Tabla 2-15 Descripción del parámetro

Parámetro	Descripción
rwuser	Nombre de cuenta, es decir, el nombre de usuario de la base de datos.
<password></password>	Contraseña para la cuenta de la base de datos. Reemplácelo con la contraseña real. Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente. Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25***%21%24.
192.168 <i>.xx.xx</i> :8635	EIP y puerto enlazados al nodo mongos de la instancia del clúster
test	El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.
authSource=admin	La base de datos de autenticación del usuario rwuser debe ser admin . authSource=admin está fijo en el comando.

- FILE_PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: Para asegurarse de que la comunicación interna del clúster no ocupe recursos como la dirección IP del usuario y el ancho de banda, el certificado del clúster se genera mediante la dirección IP de gestión interna. -sslAllowInvalidHostnames es necesario para la conexión SSL a través de una red pública.

Ejemplo de comandos:

./mongo mongodb://rwuser:<password>@192.168.xx.xx:8635/test?authSource=admin -ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames Método 2: Conéctese a una instancia usando una EIP.

Ejemplo de comando:

```
./mongo --host <DB_HOST> --port <DB_PORT> -u <DB_USER> -p --
authenticationDatabase admin --ssl --sslCAFile <FILE_PATH> --
sslAllowInvalidHostnames
```

Descripción de parámetros:

• **DB_HOST** es la EIP enlazada a la instancia que se va a conectar.

Puede hacer clic en el nombre de la instancia para ir a la página **Basic Information**. En el panel de navegación de la izquierda, elija **Connections**. En la pestaña **Public Connection**, obtenga la EIP enlazada al nodo mongos en la columna EIP.

Si hay varios nodos MongoDB, la EIP de cualquier nodo se puede utilizar para conectarse a la instancia.

Figura 2-31 Obtención de una EIP

Basic Information					
Database Port	8635	5 <u>@</u>	:	SSL	● ±
Address					
Public Network Conne	ection Add	ress m	ongodb://rwus	er: <password>@7</password>	3635/test?authSource=
		ad	dmin 🗇		
Name/ID	AZ	Private I	EIP	Operation	
dds-ce25_mong 000e813fb5574c	az4	192.168		Change Private IP Address	Unbind EIP
dds-ce25_mong bad06d1cf2594e	az4	192.168		Change Private IP Address	Bind EIP

• **DB_PORT** es el puerto de la instancia que se va a conectar. El número de puerto predeterminado es 8635.

Puede hacer clic en la instancia para ir a la página **Basic Information**. En el panel de navegación de la izquierda, elija **Connections**. En la página mostrada, haga clic en la pestaña **Public Connection** y obtenga el puerto del campo **Database Port** en el área **Basic Information**.

Figura 2-32 Obtención del puerto

asic Information								
Database Port	863	5 🖉		SSL				
Address								
Public Network Con	nection Add	Iress	mongodb://r	wuser: <password>@</password>	8635/test?authSource=			
			admin 🗇					
Name/ID	AZ	Private I	EIP	Operation				
dds-ce25_mong 000e813fb5574c	az4	192.168		Change Private IP Addr	ress Unbind EIP			
dds-ce25_mong bad06d1cf2594e	az4	192.168		Change Private IP Addr	ress Bind EIP			

- **DB_USER** es el usuario de la base de datos. El valor predeterminado es **rwuser**.
- FILE_PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: Para asegurarse de que la comunicación interna del clúster no ocupe recursos como la dirección IP del usuario y el ancho de banda, el

certificado del clúster se genera mediante la dirección IP de gestión interna. -sslAllowInvalidHostnames es necesario para la conexión SSL a través de una red pública.

Introduzca la contraseña de la cuenta de la base de datos cuando se le solicite:

Enter password:

Ejemplo de comandos:

./mongo --host 192.168.xx.xx --port 8635 -u rwuser -p --authenticationDatabase admin -ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames

Paso 9 Compruebe el resultado de la conexión. Si se muestra la siguiente información, la conexión se realiza correctamente.

----Fin

mongos>

Conexión sin encriptar

AVISO

Si se conecta a una instancia a través de una conexión no cifrada, deshabilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo deshabilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

- Paso 1 Inicie sesión en el ECS.
- Paso 2 Conéctese a la instancia en el directorio donde se encuentra el cliente MongoDB.

Método 1: Uso de una dirección de conexión de red pública

Ejemplo de comando:

./mongo <Public network address>

Public Network Connection Address: Puede hacer clic en el nombre de la instancia para ir a la página **Basic Information**. En el panel de navegación de la izquierda, elija **Connections**. En la página mostrada, haga clic en la pestaña **Public Connection**. En el área **Address**, obtenga la dirección de conexión de instancia del campo **Public Network Connection Address**.

Figura 2-33 Obtención de la dirección de conexión de red pública

Private Connection Public Con	nnection	
Basic Information		
Database Port 8635 🖉	SSL	▲
Address		
Public Network Connection Address	mongodb://rwuser: <password>@;</password>	:8635/test?authSource=
	admin 🗇	

El formato de la dirección de conexión pública es el siguiente. El nombre de usuario de la base de datos **rwuser** y la base de datos de autenticación **admin** no se pueden cambiar.

mongodb://rwuser:password>@192.168.xx.xx:8635/test?authSource=admin

En la siguiente tabla se describen los parámetros necesarios en la dirección de conexión pública.

Parámetro	Descripción
rwuser	Nombre de cuenta, es decir, el nombre de usuario de la base de datos.
<password></password>	Contraseña para la cuenta de la base de datos. Reemplácelo con la contraseña real.
	Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.
	Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25***%21%24 .
192.168 <i>.xx.xx</i> :8635	EIP y puerto enlazados al nodo mongos de la instancia del clúster
test	El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.
authSource=admin	La base de datos de autenticación del usuario rwuser debe ser admin . authSource=admin está fijo en el comando.

Tabla 2-16 Descripción del parámetro

Ejemplo de comandos:

./mongo mongodb://rwuser:<password>@192.168.xx.xx:8635/test?authSource=admin

Método 2: Uso de una EIP

Ejemplo de comando:

./mongo --host <*DB_HOST*> --port <*DB_PORT*> -u <*DB_USER*> -p -authenticationDatabase admin

Descripción de parámetros:

• **DB_HOST** es la EIP enlazada a la instancia que se va a conectar.

Puede hacer clic en el nombre de la instancia para ir a la página **Basic Information**. En el panel de navegación de la izquierda, elija **Connections**. En la pestaña **Public Connection**, obtenga la EIP enlazada al nodo mongos en la columna EIP.

Si hay varios nodos MongoDB, la EIP de cualquier nodo se puede utilizar para conectarse a la instancia.

Figura 2-34 Obtención de una EIP

Basic Information					
Database Port	8635	<u>0</u>	5	SSL	▲
Address					
Public Network Connection Address mongodb://rwuser: <password>@7 3635/test?authSource=</password>					
admi			dmin 🗖		
Name/ID	AZ	Private I	EIP	Operation	
dds-ce25_mong 000e813fb5574c	az4	192.168		Change Private IP Addres	s Unbind EIP
dds-ce25_mong bad06d1cf2594e	az4	192.168		Change Private IP Addres	s Bind EIP

• **DB_PORT** es el puerto de la instancia que se va a conectar. El número de puerto predeterminado es 8635.

Puede hacer clic en la instancia para ir a la página **Basic Information**. En el panel de navegación de la izquierda, elija **Connections**. En la página mostrada, haga clic en la pestaña **Public Connection** y obtenga el puerto del campo **Database Port** en el área **Basic Information**.

Figura 2-35 Obtención del puerto

Basic Information					
Database Port	8635	2		SSL C	
Address					
Public Network Conne	ction Addr	ess n	hongodb://rwus	er: <password>6</password>	8635/test?authSource=
		а	dmin 🗇		
Name/ID	AZ	Private I	EIP	Operation	
dds-ce25_mong 000e813fb5574c	az4	192.168		Change Private IP Address	Unbind EIP
dds-ce25_mong bad06d1cf2594e	az4	192.168		Change Private IP Address	Bind EIP

• **DB_USER** es el usuario de la base de datos. El valor predeterminado es **rwuser**.

Introduzca la contraseña de la cuenta de la base de datos cuando se le solicite:

Enter password:

Ejemplo de comandos:

./mongo --host 192.168.xx.xx --port 8635 -u rwuser -p --authenticationDatabase admin

Paso 3 Compruebe el resultado de la conexión. Si se muestra la siguiente información, la conexión se realiza correctamente.

mongos>

----Fin

2.2.4.4 Conexión a una instancia de clúster mediante Robo 3T

Para conectarse a una instancia desde un dispositivo local, puede usar Robo 3T para acceder a la instancia desde Internet.

Esta sección describe cómo usar Robo 3T para conectarse a una instancia de clúster desde un dispositivo local. En esta sección, se utiliza como ejemplo el sistema operativo Windows utilizado por el cliente.

Robo 3T puede conectarse a una instancia con una conexión no cifrada o una conexión cifrada (SSL). Para mejorar la seguridad de la transmisión de datos, conéctese a instancias mediante SSL.

Diagrama de conexión

Figura 2-36 Diagrama de conexión



Prerrequisitos

- 1. **Vincule una EIP** a la instancia del clúster y **configure las reglas de grupo de seguridad** para garantizar que se pueda acceder a la instancia mediante Robo 3T.
- 2. Instala Robo 3T.

Para obtener más información, consulte Instalación de Robo 3T.

SSL

AVISO

Si se conecta a una instancia a través de la conexión SSL, habilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo habilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

Paso 1 Ejecute el Robo 3T instalado. En el cuadro de diálogo mostrado, haga clic en Create.

🛃 MongoDB	Connections						×
Create, edit,	<u>remove</u> , <u>clone</u> or	reorder connections	via drag'n'	drop.			
Name		Address		Attributes	Auth.	Database / 1	Vser
						📃 C <u>o</u> nnect	Cancel

Figura 2-37 Conexiones

- Paso 2 En el cuadro de diálogo Connection Settings, establezca los parámetros de la nueva conexión.
 - 1. En la pestaña **Connection**, escriba el nombre de la nueva conexión en el cuadro de texto **Name** e introduzca el puerto EIP y la base de datos enlazados a la instancia de base de datos DDS en el cuadro de texto **Name**.

Figura 2-38 Conexión

Connection	Authentication SSH TLS Advanced
уре:	Direct Connection
lame:	test
Address:	: 8635
	Specity host and port of MongoUB server. Host can be eith IPv4, IPv6 or domain name.
	Specity host and port of MongoUB server. Host can be eith IPv4, IPv6 or domain name.
From URI	Specity host and port of MongoUB server. Host can be eith IPv4, IPv6 or domain name.

2. En la pestaña Authentication, establezca Database en admin, User Name en rwuser y Password en la contraseña de administrador establecida durante la creación de la instancia de clúster.

Figura 2-39 Autenticación

📃 Connection Se	ettings	×		
Connection	Authentication SSH TLS Advanced			
🗹 Perform authentication				
Database	admin			
The admin database is unique in MongoDB. Users with				
User Name	rwuser			
Password	<u>کې</u>			
Auth Mechanism	SCRAM-SHA-1			
🗌 Manually specify visible databases				
i <u>T</u> est	Save Cancel			

3. En la pestaña TLS, seleccione Use TLS protocol y seleccione Self-signed Certificate para Authentication Method.

Figura 2-40 SSL

Connection	Settings							×
Connection	Authentica	ation	SSH	TLS	Advance	ed		
🗹 Use TLS p	rotocol							
Authenticati	on Method:	Self-s	signed (Certific	ate			\sim
		In gen unless certif will b valida	eral, a the ne icate i e encry tion of	void us: twork i: s used, pted how server	ing self- s trusted the comm wever the identity	-signed cert d. If self-s unications ere will be /.	ificates igned channel no	
🗌 Vse PEM C	ert./Key:	Enable requir	this o es CA-s	ption to igned ci	o connect lient cer	t to a Mongo tificates/}	DB that ey file.	
Advanced	Options							
<u>i</u> <u>T</u> est					[Save	Canc	el

- 4. Haga clic en Save.
- Paso 3 En la página MongoDB Connections, haga clic en Connect para conectarse a la instancia del clúster.

🛃 MongoDB Connections				×
<u>Create</u> , <u>edit</u> , <u>remove</u> , <u>clone</u> or	reorder connections via drag'n'	drop.		
Name	Address	Attributes	Auth. Database / User	
📃 test	:8635	TLS	🔎 admin / rwuser	
			Connect Canc	el

Figura 2-41 Información de conexión de clúster

Paso 4 Si la instancia del clúster se conecta correctamente, se muestra la página mostrada en Figura 2-42.

Figura 2-42 Clúster conectado correctamente.

🌢 Robo 3T - 1.4	
ile View Options Wind	iow Help
 test (3) System admin 	 ♦ Welcome × ♦ db. getCollection(' system ··· × ♦ db. getCollection(' system ··· × i test = 10.154.221.78:8635 admin
Collections (4)	<pre>db.getCollection('system.roles').find((\$))</pre>
> system.k > system.r	(§) 0.089 sec. Fetched 0 record(s) in 88ms
> system.u > system.v	
 Functions Users 	
> 🗐 local > 🗐 config	



AVISO

Conexión sin encriptar

Si se conecta a una instancia a través de una conexión no cifrada, deshabilite SSL primero. De lo contrario, se notifica un error. Para obtener más información, consulte Habilitar y deshabilitar SSL.

Paso 1 Ejecute el Robo 3T instalado. En el cuadro de diálogo mostrado, haga clic en Create.

🛃 MongoDB Connections					×
Create, edit, remove, clone or :	reorder connections via drag'n'	drop.			
Name	Address	Attributes	Auth.	Database / U	Íser
			1	Connect	Cancel

Figura 2-43 Conexiones

- Paso 2 En el cuadro de diálogo Connection Settings, establezca los parámetros de la nueva conexión.
 - 1. En la pestaña **Connection**, escriba el nombre de la nueva conexión en el cuadro de texto **Name** e introduzca el puerto EIP y la base de datos enlazados a la instancia de base de datos DDS en el cuadro de texto **Name**.

Figura 2-44 Conexión

Connection	Authentication SSH TLS Advanced
уре:	Direct Connection
lame:	test
Address:	: 8635
	Specity host and port of MongoUB server. Host can be eith IPv4, IPv6 or domain name.
	Specity host and port of MongoUB server. Host can be eith IPv4, IPv6 or domain name.
From URI	Specity host and port of MongoUB server. Host can be eith IPv4, IPv6 or domain name.

2. En la pestaña Authentication, establezca Database en admin, User Name en rwuser y Password en la contraseña de administrador establecida durante la creación de la instancia de clúster.

Figura 2-45 Autenticación

📃 Connection Se	ettings	×	
Connection	Authentication SSH TLS Advanced		
Perform authentication			
Database	admin		
	The admin database is unique in MongoDB. Users with		
User Name	rwuser		
Password	<u>۵</u>		
Auth Mechanism	SCRAM-SHA-1 ~		
	ecify visible databases	-	
i <u>I</u> est	Save Cancel		

- 3. Haga clic en Save.
- Paso 3 En la página MongoDB Connections, haga clic en Connect para conectarse a la instancia del clúster.

Figura 2-4	6 Inform	nación de	conexión	de	clúster
------------	----------	-----------	----------	----	---------

🛃 MongoDB Connections				×
Create, edit, remove, clone or	reorder connections via drag'n'	drop.		
Name	Address	Attributes	Auth. Database / User	
📃 test	:8635	TLS	🔎 admin / rwuser	
			📃 C <u>o</u> nnect 🛛 Cancel	

Paso 4 Si la instancia del clúster se conecta correctamente, se muestra la página mostrada en Figura 2-47.



Robo 3T - 1.4				
File View Options Winde	ow Help			
✓ Intest (3) ✓ Integration System ✓ Integration admin	♦ Welcome × ♦ db.getCollection('system… × = test = 10.154.221.78:8635 = admin	<pre> db.getCollection('system.''' x) </pre>		
Collections (4)	db.getCollection('system.roles').find(())			
👻 📙 System	() 0.089 sec.			
> system.k > system.r > system.u > system.v	Fetched 0 record(s) in 08ms			
> <mark>-</mark> Functions > <mark>-</mark> Users > - local				
> 🛢 config				

----Fin

2.2.5 Conexión a una instancia de clúster mediante código de programa

2.2.5.1 Java

Si se está conectando a una instancia mediante Java, un certificado SSL es opcional, pero descargar un certificado SSL y cifrar la conexión mejorará la seguridad de su instancia. SSL está deshabilitado de forma predeterminada para instancias recién creadas, pero puede habilitar SSL haciendo referencia a **Habilitación o deshabilitación de SSL**.

Prerrequisitos

Familiarícese con:

- Conceptos básicos de computadora
- Código Java

Obtención y uso de Java

- Descargue el controlador Jar desde: https://repo1.maven.org/maven2/org/mongodb/ mongo-java-driver/3.0.4/
- Para ver la guía de uso, visite https://mongodb.github.io/mongo-java-driver/4.2/ driver/getting-started/installation/.

Uso de un certificado SSL

NOTA

- Descargue el certificado SSL y verifique el certificado antes de conectarse a las bases de datos.
- En la página Instances, haga clic en el nombre de la instancia de base de datos de destino. En el área

DB Information de la página **Basic Information**, haga clic en de en el campo **SSL** para descargar el certificado raíz o el paquete de certificados.

 Para obtener más información sobre cómo configurar una conexión SSL, consulte el documento oficial del controlador Java de MongoDB en https://www.mongodb.com/docs/drivers/java/sync/ current/fundamentals/connection/tls/#std-label-tls-ssl.

Si se conecta a una instancia de clúster mediante Java, el formato del código es el siguiente: mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>? authSource=admin&ssl=true

Parámetro	Descripción
<username></username>	Nombre de usuario actual.
<password></password>	Contraseña para el nombre de usuario actual
<instance_ip></instance_ip>	Si intenta obtener acceso a la instancia desde un ECS, establezca <i>instance_ip</i> en la dirección IP privada que se muestra en la página Basic Information de la instancia a la que desea conectarse.
	Si tiene la intención de acceder a la instancia a través de una EIP, establezca <i>instance_ip</i> en la EIP que se ha enlazado a la instancia.
	Si se requieren varias direcciones de host, enumere las direcciones en el formato de <instance_ip1>:<instance_port1>,<instance_ip2>:<instance_port2>. Ejemplo: mongodb:// username:****@127.***.***.1:8635,127.***.***.2:8635/? authSource=admin</instance_port2></instance_ip2></instance_port1></instance_ip1>
<instance_port></instance_port>	Puerto de la base de datos que se muestra en la página Basic Information. Valor predeterminado: 8635
<database_name></database_name>	Nombre de la base de datos que se va a conectar.
authSource	Base de datos de usuarios de autenticación. El valor es admin.
ssl	Modo de conexión. true indica que se utiliza el modo de conexión SSL.

Tabla 2-17 Descripción del parámetro

Utilice la herramienta keytool para configurar el certificado de CA. Para obtener más información sobre los parámetros, consulte **Tabla 2-18**.

keytool -importcert -trustcacerts -file <path to certificate authority file> keystore <path to trust store> -storepass <password>

Parámetro	Descripción
<pre><path authority="" certificate="" file="" to=""></path></pre>	Ruta para almacenar el certificado SSL.
<path store="" to="" trust=""></path>	Ruta para almacenar el truststore. Establezca este parámetro según sea necesario, por ejemplo, ./trust/ certs.keystore.
<password></password>	Contraseña personalizada.

Tabla 2-18 Descripción del parámetro

Configure las propiedades del sistema JVM en el programa para que apunten al truststore y keystore correctos:

- System.setProperty("javax.net.ssl.trustStore","path to trust store>");
- System.setProperty("javax.net.ssl.trustStorePassword","<password>");

Para obtener más información sobre el código Java, consulte el siguiente ejemplo: public class Connector {

```
public static void main(String[] args) {
        try {
            System.setProperty("javax.net.ssl.trustStore", "./trust/
certs.keystore");
            System.setProperty("javax.net.ssl.trustStorePassword",
"123456");
            ConnectionString connString = new
ConnectionString("mongodb://
<username>:<password>@<instance ip>:<instance port>/<database name>?
authSource=admin&ssl=true");
            MongoClientSettings settings = MongoClientSettings.builder()
                    .applyConnectionString(connString)
                    .applyToSslSettings(builder -> builder.enabled(true))
                    .applyToSslSettings(builder ->
builder.invalidHostNameAllowed(true))
                    .build();
            MongoClient mongoClient = MongoClients.create(settings);
            MongoDatabase database = mongoClient.getDatabase("admin");
            //Ping the database. If the operation fails, an exception
occurs.
            BsonDocument command = new BsonDocument("ping", new
BsonInt64(1));
            Document commandResult = database.runCommand(command);
            System.out.println("Connect to database successfully");
        } catch (Exception e) {
            e.printStackTrace();
            System.out.println("Test failed");
        }
    }
```

Conexión sin el certificado SSL

NOTA

No es necesario descargar el certificado SSL porque no se requiere la verificación del certificado en el servidor.

Si se conecta a una instancia de clúster mediante Java, el formato del código es el siguiente: mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>? authSource=admin

Parámetro	Descripción
<username></username>	Nombre de usuario actual.
<password></password>	Contraseña para el nombre de usuario actual
<instance_ip></instance_ip>	Si intenta obtener acceso a la instancia desde un ECS, establezca <i>instance_ip</i> en la dirección IP privada que se muestra en la página Basic Information de la instancia a la que desea conectarse.
	Si tiene la intención de acceder a la instancia a través de una EIP, establezca <i>instance_ip</i> en la EIP que se ha enlazado a la instancia.
	Si se requieren varias direcciones de host, enumere las direcciones en el formato de <instance_ip1>:<instance_port1>,<instance_ip2>:<instance_port2>. Ejemplo: mongodb:// username:*****@127.***.1:8635,127.***.***.2:8635/? authSource=admin</instance_port2></instance_ip2></instance_port1></instance_ip1>
<instance_port></instance_port>	Puerto de la base de datos que se muestra en la página Basic Information. Valor predeterminado: 8635
<database_name></database_name>	Nombre de la base de datos que se va a conectar.
authSource	Base de datos de usuarios de autenticación. El valor es admin.

Tabla 2-19 Descripción del parámetro

Para obtener más información sobre el código Java, consulte el siguiente ejemplo:

```
public class Connector {
    public static void main(String[] args) {
        try {
            ConnectionString connString = new
ConnectionString("mongodb://
<username>:<password>@<instance_ip>:<instance_port>/<database_name>?
authSource=admin");
            MongoClientSettings settings = MongoClientSettings.builder()
                    .applyConnectionString(connString)
                    .retryWrites(true)
                    .build();
            MongoClient mongoClient = MongoClients.create(settings);
            MongoDatabase database = mongoClient.getDatabase("admin");
            //Ping the database. If the operation fails, an exception
occurs.
            BsonDocument command = new BsonDocument("ping", new
BsonInt64(1));
            Document commandResult = database.runCommand(command);
            System.out.println("Connect to database successfully");
        } catch (Exception e) {
            e.printStackTrace();
            System.out.println("Test failed");
        }
```

}

}

2.2.5.2 Python

Esta sección describe cómo utilizar el cliente MongoDB en Python para conectarse a una instancia de clúster.

Prerrequisitos

1. Para conectar un ECS a una instancia, el ECS debe poder comunicarse con la instancia DDS. Puede ejecutar el siguiente comando para conectarse a la dirección IP y el puerto del servidor de instancia para probar la conectividad de red.

curl ip:port

Si se muestra el mensaje It looks like you are trying to access MongoDB over HTTP on the native driver port, la conectividad de red es normal.

- 2. Instale Python y el paquete de instalación de terceros **pymongo** en el ECS. Se recomienda Pymongo 2.8.
- 3. Si SSL está habilitado, debe descargar el certificado raíz y subirlo al ECS.

Código de conexión

```
    Habilitación de SSL
```

```
import ssl
from pymongo import MongoClient
conn_urls="mongodb://rwuser:rwuserpassword@ip:port/{mydb}?
authSource=admin"
connection = MongoClient(conn_urls,connectTimeoutMS=5000,ssl=True,
ssl_cert_reqs=ssl.CERT_REQUIRED,ssl_match_hostname=False,ssl_ca_certs
=${path to certificate authority file})
dbs = connection.database_names()
print "connect database success! database names is %s" % dbs
```

Desactivación de SSL

```
import ssl
from pymongo import MongoClient
conn_urls="mongodb://rwuser:rwuserpassword@ip:port/{mydb}?
authSource=admin"
connection = MongoClient(conn_urls,connectTimeoutMS=5000)
dbs = connection.database_names()
print "connect database success! database names is %s" % dbs
```


- La base de datos de autenticación en la URL debe ser admin. Eso significa configurar authSource a admin.
- En el modo SSL, es necesario generar manualmente el archivo trustStore.
- La base de datos de autenticación debe ser **admin** y, a continuación, cambiar a la base de datos de servicio.

3 Tareas iniciales con conjunto de réplicas

3.1 Compra de una instancia de conjunto de réplicas

3.1.1 Config rápido

Esta sección describe cómo comprar rápidamente una instancia de conjunto de réplicas en la consola de gestión. DDS proporciona varias configuraciones recomendadas para ayudarle a comprar una instancia de conjunto de réplicas en varios minutos.

Prerrequisitos

- Ha registrado un ID de Huawei y ha habilitado servicios de Huawei Cloud.
- El saldo de su cuenta es mayor o igual a \$0 USD.

Procedimiento

- Paso 1 Vaya a la página de Quick Config.
- Paso 2 En la página mostrada, seleccione un modo de facturación y configure la información sobre su instancia de base de datos. A continuación, haga clic en Next.

Figura 3-1 Configuraciones básicas



Tabla 3-1 Configuraciones básicas

Parámetro	Descripción
Billing Mode	Selecciona un modo de facturación: Yearly/Monthly o Pay-per-use.
	• Para instancias anuales/mensuales
	 Especifique Required Duration y el sistema deduce las tarifas incurridas de su cuenta en función del precio del servicio.
	 Si no espera seguir usando la instancia mucho después de que caduque, puede cambiar el modo de facturación de anual/ mensual a pago por uso. Para más detalles, consulte Cambio del modo de facturación de anual/mensual a de pago por uso.
	NOTA Las instancias facturadas anualmente/mensualmente no se pueden eliminar. Solo pueden darse de baja de. Para obtener más información, consulte Anulación de la suscripción a una instancia anual/mensual .
	• Para instancias de pago por uso
	 Se le factura el uso basado en el tiempo que el servicio está en uso.
	 Si espera usar el servicio ampliamente durante un largo período de tiempo, puede cambiar su modo de facturación de pago por uso a anual/mensual para reducir los costos. Para más detalles, consulte Cambio del modo de facturación de pago por uso a anual/mensual.
Region	La región donde se encuentra el recurso.
	NOTA Las instancias desplegadas en diferentes regiones no pueden comunicarse entre sí a través de una red privada y no se puede cambiar la región de una instancia una vez que se ha comprado. Tenga cuidado al seleccionar una región.
Project	El proyecto corresponde a la región actual y se puede cambiar.

Parámetro	Descripción
AZ	Una AZ es una parte de una región con su propia fuente de alimentación y red independiente. Las zonas de disponibilidad están físicamente aisladas pero pueden comunicarse a través de conexiones de red internas.
	Las instancias se pueden desplegar en una única zona de disponibilidad o en tres zonas de disponibilidad.
	 Si su servicio requiere baja latencia de red entre instancias, despliega los componentes de la instancia en la misma zona de disponibilidad. Si selecciona una única zona de disponibilidad para desplegar la instancia, se utiliza de forma predeterminada el despliegue antiafinidad. Con un despliegue antiafinidad, sus nodos primarios, secundarios y ocultos se despliegan en diferentes máquinas físicas para una alta disponibilidad.
	• Si desea desplegar una instancia en las zonas de disponibilidad para la recuperación ante desastres, seleccione tres zonas de disponibilidad. En este modo de despliegue, los nodos primario, secundario y oculto se distribuyen uniformemente en tres zonas de disponibilidad.
	NOTA El despliegue de 3-AZ no está disponible en todas las regiones. Si la opción de 3- AZ no se muestra en la página para comprar una instancia, pruebe con una región diferente.
DB Instance	Seleccione Replica set.
Туре	Un conjunto de réplicas consiste en el nodo primario, el nodo secundario y el nodo oculto. Si un nodo primario se cae o se vuelve defectuoso, un nodo secundario se asigna automáticamente al rol principal y continúa el funcionamiento normal. Si un nodo secundario no está disponible, un nodo oculto asumirá el papel del secundario para garantizar una alta disponibilidad.
Compatible MongoDB Version	 4.4 4.2 4.0 3.4

Parámetro	Descripción
СРU Туре	DDS admite arquitecturas de CPU x86 y Kunpeng. NOTA Este parámetro solo está disponible para MongoDB 4.0 y 3.4. El valor
	 x86 Las CPU x86 utilizan el conjunto de instrucciones de complejas de computación con Conjunto de Instrucciones Complejas (CISC). Cada instrucción se puede usar para ejecutar operaciones de hardware de bajo nivel. Las instrucciones CISC varían en longitud, y tienden a ser complicadas y lentas en comparación con la computación de conjunto reducido de instrucciones (RISC).
	 Kunpeng La arquitectura de CPU Kunpeng utiliza RISC. El conjunto de instrucciones RISC es más pequeño y más rápido que CISC, gracias a la arquitectura simplificada. Las CPU de Kunpeng también ofrecen un mejor equilibrio entre potencia y rendimiento que x86.
	Las CPU de Kunpeng ofrecen una opción de alta densidad y bajo consumo que es más rentable para cargas de trabajo pesadas.
Specifications	Con una arquitectura x86, tiene las siguientes opciones:
	 Uso general (s6): Las instancias S6 son adecuadas para aplicaciones que requieren un rendimiento moderado en general, pero ocasionales ráfagas de alto rendimiento, como servidores web de carga ligera, entornos de pruebas y R&D empresariales y bases de datos de bajo y mediano rendimiento.
	 Mejorado II (c6): Las instancias C6 tienen múltiples tecnologías optimizadas para proporcionar un rendimiento informático potente y estable. Las NIC inteligentes de alta velocidad de 25 GE se utilizan para proporcionar un ancho de banda y un rendimiento ultra altos, lo que las convierte en una excelente opción para escenarios de carga pesada. Es adecuado para sitios web, aplicaciones web, bases de datos generales y servidores de caché que tienen requisitos de rendimiento más altos para recursos informáticos y de red; y aplicaciones empresariales de carga media y pesada.
Recommended Specifications	Actualmente, se admiten especificaciones de bases de datos medianas y ligeras y especificaciones personalizadas. NOTA
	• Si una instancia tiene menos de 16 vCPU, el espacio de almacenamiento oscila entre 10 GB y 2000 GB.
	• Si una instancia tiene más de 16 vCPU, el espacio de almacenamiento oscila entre 10 GB y 4000 GB.

|--|

Network VPC :	default_type • C default_tydenet(192.168.0.0/24) • C Sps-default(b6f16cee-e856-47e2-a418 • C ▲ After the DOS instance is created, the VPC cannot be changed. Available private IP addresses in the subnet: 227 In a security group, rules that authorize connections to DB instances apply to all DB instances associated with the security group.
Enterprise Project Enterprise Project	Select • C Vew Project Management ③
Some settings are configured by de	elault during purchase, but can still be modified after the instance is created. If you do not see a setting listed for your instance, click Custom Config ns

 Tabla 3-2
 Ajustes de red

Parámetro	Descripción
VPC	La VPC donde se encuentran instancias de base de datos. Una VPC aísla las redes para diferentes servicios. Le permite gestionar y configurar fácilmente redes privadas y cambiar las configuraciones de red.
	Necesita crear o seleccionar la VPC requerida. Para obtener más información, consulte Creación de una VPC en la <i>Guía de usuario de</i> <i>Virtual Private Cloud</i> . Para obtener más información acerca de las restricciones en el uso de VPC, consulte Métodos de conexión .
	Si no hay VPC disponibles, DDS crea una para usted de manera predeterminada.
	NOTA Una vez creada la instancia de DDS, la VPC no podrá modificarse.
Enterprise Project	Solo los usuarios de empresa pueden utilizar esta función. Para utilizar esta función, póngase en contacto con el servicio de atención al cliente.
	Un proyecto empresarial es un modo de gestión de recursos en la nube, en el que los recursos y los miembros en la nube se gestionan de forma centralizada por proyecto.
	Seleccione un proyecto de empresa en la lista desplegable. El proyecto predeterminado es default . Para obtener más información acerca de los proyectos de empresa, consulte Gestión de proyecto en <i>Guía de usuario de Enterprise Management</i> .
	Para personalizar un proyecto de empresa, haga clic en Enterprise en la esquina superior derecha de la consola. Se muestra la página Enterprise Management . Para obtener más información, consulte Creación de un proyecto empresarial .

Tabla 3-3 Período de uso y cantidad

Parámetro	Descripción
Required Duration	El sistema calculará automáticamente la tarifa en función del período de validez que haya seleccionado.

Parámetro	Descripción
Auto-renew	 De forma predeterminada, esta opción no está seleccionada. Si selecciona esta opción, el ciclo de renovación automática viene determinado por la duración de la suscripción.
Quantity	La cantidad de compra depende de la cuota de instancia del conjunto de réplicas. Si su cuota actual no le permite comprar el número requerido de instancias, puede solicitar el aumento de la cuota según se le solicite. Las instancias anuales/mensuales que se compraron en lotes tienen las mismas especificaciones, excepto el nombre y el ID de la instancia.

Paso 3 En la página mostrada, confirme los detalles de la instancia.

- Para instancias anuales/mensuales
 - Si necesita modificar las especificaciones, haga clic en Previous para volver a la página anterior.
 - Si no necesita modificar las especificaciones, lea y acepte el contrato de servicio y haga clic en Pay Now para ir a la página de pago y completar el pago.
- Para instancias de pago por uso
 - Si necesita modificar las especificaciones, haga clic en Previous para volver a la página anterior.
 - Si no necesita modificar las especificaciones, lea y acepte el contrato de servicio y haga clic en Submit para comenzar a crear la instancia.
- **Paso 4** Haga clic en **Back to Instance List**. Después de crear una instancia DDS, puede ver y gestionarla en la página **Instances**.
 - Cuando se crea una instancia, el estado que se muestra en la columna Status es Creating. Este proceso dura unos 15 minutos. Una vez completada la creación, el estado cambia a Available.
 - DDS habilita la política de copia de respaldo automatizada de forma predeterminada. Después de crear una instancia, puede modificar o deshabilitar la política de copia de respaldo automatizada. Una copia de respaldo completa automatizada se activa inmediatamente después de la creación de una instancia.

----Fin

3.1.2 Config personalizado

En esta sección se describe cómo comprar una instancia de conjunto de réplicas en modo personalizado en la consola de gestión. Puede personalizar los recursos informáticos y el espacio de almacenamiento de una instancia de conjunto de réplicas en función de sus requisitos de servicio. Además, puede configurar ajustes avanzados, como el registro de consultas lentas y la copia de respaldo automatizada.

Precauciones

Cada cuenta puede crear hasta 50 instancias de conjuntos de réplicas.

Prerrequisitos

- Ha registrado un ID de Huawei y ha habilitado servicios de Huawei Cloud.
- El saldo de su cuenta es mayor o igual a \$0 USD.
- Para mostrar si el disco está cifrado en la lista de instancias de base de datos, envíe un ticket de servicio. En la esquina superior derecha de la consola de gestión, elija Service Tickets > Create Service Ticket.
- Si desea recursos informáticos y de red dedicados a su uso exclusivo, habilite un DeC y solicite recursos de DCC. A continuación, puede crear instancias DDS. Haga clic en

🕺 en la esquina superior izquierda, y seleccione una región y un proyecto.

NOTA

Se le cobrará adicionalmente por usar DeC. Solo se pueden comprar instancias de conjuntos de réplicas de pago por uso a través de DeC.

Procedimiento

- Paso 1 Vaya a la página Custom Config.
- Paso 2 En la página mostrada, seleccione un modo de facturación y configure la información sobre su instancia de base de datos. A continuación, haga clic en Next.

Figura 3-3 Configuraciones básicas


Parámetro	Descripción	
Billing Mode	Selecciona un modo de facturación: Yearly/Monthly o Pay-per-use.	
	Para instancias anuales/mensuales	
	 Especifique Required Duration y el sistema deduce las tarifas incurridas de su cuenta en función del precio del servicio. 	
	 Si no espera seguir usando la instancia mucho después de que caduque, puede cambiar el modo de facturación de anual/ mensual a pago por uso. Para más detalles, consulte Cambio del modo de facturación de anual/mensual a pago por uso. 	
	NOTA Las instancias facturadas anualmente/mensualmente no se pueden eliminar. Solo pueden darse de baja de. Para obtener más información, consulte Anulación de la suscripción a una instancia anual/mensual.	
	 Para instancias de pago por uso 	
	 Se le factura el uso basado en el tiempo que el servicio está en uso. 	
	 Si espera usar el servicio ampliamente durante un largo período de tiempo, puede cambiar su modo de facturación de pago por uso a anual/mensual para reducir los costos. Para más detalles, consulte Cambio del modo de facturación de pago por uso a anual/mensual. 	
Region	La región donde se encuentra el recurso.	
	NOTA Las instancias desplegadas en diferentes regiones no pueden comunicarse entre sí a través de una red privada y no se puede cambiar la región de una instancia una vez que se ha comprado. Tenga cuidado al seleccionar una región.	
Project	El proyecto corresponde a la región actual y se puede cambiar.	

Tabla 3-4 Modo de facturación

Parámetro	Descripción		
AZ	Una AZ es una parte de una región con su propia fuente de alimentación y red independiente. Las zonas de disponibilidad están físicamente aisladas pero pueden comunicarse a través de conexiones de red internas.		
	Las instancias se pueden desplegar en una única zona de disponibilidad o en tres zonas de disponibilidad.		
	 Si su servicio requiere baja latencia de red entre instancias, despliega los componentes de la instancia en la misma zona de disponibilidad. Si selecciona una única zona de disponibilidad para desplegar la instancia, se utiliza de forma predeterminada el despliegue antiafinidad. Con un despliegue antiafinidad, sus nodos primarios, secundarios y ocultos se despliegan en diferentes máquinas físicas para una alta disponibilidad. 		
	• Si desea desplegar una instancia en las zonas de disponibilidad para la recuperación ante desastres, seleccione tres zonas de disponibilidad. En este modo de despliegue, los nodos primario, secundario y oculto se distribuyen uniformemente en tres zonas de disponibilidad.		
	NOTA El despliegue de 3-AZ no está disponible en todas las regiones. Si la opción de 3- AZ no se muestra en la página para comprar una instancia, pruebe con una región diferente.		
DB Instance Name	• El nombre de instancia que especifique después de la compra. El nombre de instancia debe contener entre 4 y 64 caracteres y debe comenzar con una letra. Es sensible a mayúsculas y minúsculas y puede contener letras, dígitos, guiones (-) y guiones bajos (_). No puede contener otros caracteres especiales.		
	• El nombre de instancia puede ser el mismo que un nombre de instancia existente.		
	 Si compra un lote de instancias a la vez, se agregará un sufijo numérico de 4 dígitos a los nombres de las instancias, comenzando por -0001. Si más adelante realiza otra compra por lotes, los nombres de las nuevas instancias se numerarán primero utilizando los sufijos que falten en la secuencia de sus instancias existentes y, a continuación, continuando desde donde lo dejó su última compra por lotes. Por ejemplo, un lote de 3 instancias obtiene los sufijos -0001, -0002 y -0003. Si eliminó instancia 0002 y luego compró 3 instancias más, las nuevas instancias obtendrían los sufijos -0002, -0004 y -0005. 		
	 Después de crear la instancia de base de datos, puede cambiar su nombre. Para obtener más información, consulte Cambio del nombre de una instancia. 		

Parámetro	Descripción	
DB Instance Type	Seleccione Replica set . Un conjunto de réplicas consiste en el nodo primario, el nodo secundario y el nodo oculto. Si un nodo primario se cae o se vuelve defectuoso, un nodo secundario se asigna automáticamente al rol principal y continúa el funcionamiento normal. Si un nodo secundario no está disponible, un nodo oculto asumirá el papel del secundario para garantizar una alta disponibilidad.	
Compatible MongoDB Version	 4.4 4.2 4.0 3.4 	
Nodes	Puede crear una instancia de conjunto de réplicas de tres, cinco o siete nodos.	
CPU Type	 DDS admite arquitecturas de CPU x86 y Kunpeng. NOTA Este parámetro solo está disponible para MongoDB 4.0 y 3.4. El valor predeterminado es Kunpeng. x86 Las CPU x86 utilizan el conjunto de instrucciones CISC (Complex Instruction Set Computing). Cada instrucción se puede usar para ejecutar operaciones de hardware de bajo nivel. Las instrucciones CISC varían en longitud, y tienden a ser complicadas y lentas en comparación con la computación de conjunto reducido de instrucciones (RISC). Kunpeng La arquitectura de CPU Kunpeng utiliza RISC. El conjunto de instrucciones RISC es más pequeño y más rápido que CISC, gracias a la arquitectura simplificada. Las CPU de Kunpeng también ofrecen un mejor equilibrio entre potencia y rendimiento que x86. Las CPU de Kunpeng ofrecen una opción de alta densidad y bajo consumo que es más rentable para cargas de trabajo pesadas.	
Storage Type	 Si no utiliza DeC, el tipo de almacenamiento es Cloud SSD de forma predeterminada. Para los usuarios de DeC, los tipos de almacenamiento admitidos dependen del tipo de recurso seleccionado. Si selecciona EVS para Resource Type, Storage Type se establece en Cloud SSD 	
	 Si selecciona DSS para Resource Type, Storage Type se puede establecer en Common I/O, High I/O o Cloud SSD. 	

Parámetro	Descripción
Storage Engine	 WiredTiger WiredTiger es el motor de almacenamiento predeterminado de DDS 3.4 y 4.0. WiredTiger ofrece diferentes mecanismos de control de simultaneidad y compresión de granularidad para la gestión de datos. Puede proporcionar el mejor rendimiento y eficiencia de almacenamiento para diferentes tipos de aplicaciones.
	 RocksDB RocksDB es el motor de almacenamiento predeterminado de DDS 4.2. RocksDB admite búsqueda de puntos eficiente, escaneo de rango y escritura de alta velocidad. RocksDB se puede utilizar como el motor de almacenamiento de datos subyacente de MongoDB y es adecuado para escenarios con un gran número de operaciones de escritura.
Specifications	Con una arquitectura x86, tiene las siguientes opciones:
	• Uso general (s6): Las instancias S6 son adecuadas para aplicaciones que requieren un rendimiento moderado en general, pero ocasionales ráfagas de alto rendimiento, como servidores web de carga ligera, entornos de pruebas y R&D empresariales y bases de datos de bajo y mediano rendimiento.
	 Mejorado II (c6): Las instancias C6 tienen múltiples tecnologías optimizadas para proporcionar un rendimiento informático potente y estable. Las NIC inteligentes de alta velocidad de 25 GE se utilizan para proporcionar un ancho de banda y un rendimiento ultra altos, lo que las convierte en una excelente opción para escenarios de carga pesada. Es adecuado para sitios web, aplicaciones web, bases de datos generales y servidores de caché que tienen requisitos de rendimiento más altos para recursos informáticos y de red; y aplicaciones empresariales de carga media y pesada.
Node Class	Para obtener más información sobre las especificaciones de instancia, consulte Especificaciones de instancia
	Para obtener más información sobre los datos de rendimiento de instancias de bases de datos de diferentes especificaciones, consulte Libro blanco de rendimiento .
	Si la CPU o la memoria de una instancia de base de datos creada no pueden cumplir los requisitos de servicio, puede cambiarlos en la consola de gestión. Para obtener más información, consulte Cambio de una clase de instancia de conjunto de réplicas .

Parámetro	Descripción		
Storage Space	Si una instancia tiene menos de 16 vCPU, el espacio de almacenamiento oscila entre 10 GB y 2000 GB.		
	Si una instancia tiene más de 16 vCPU, el espacio de almacenamiento oscila entre 10 GB y 4000 GB.		
	El valor debe ser un múltiplo entero de 10.		
	Puede ampliar verticalmente una instancia después de crearla. Para obtener más información, consulte Ampliación vertical de una instancia de conjunto de réplicas .		
	NOTA		
	• Si el espacio de almacenamiento adquirido supera los 600 GB y el espacio de almacenamiento restante es de 18 GB, la instancia se convierte en sólo lectura.		
	• Si el espacio de almacenamiento que compró es inferior a 600 GB y el uso de espacio de almacenamiento alcanza el 97%, la instancia se convierte en sólo lectura.		
	En estos casos, elimine recursos innecesarios o amplíe la capacidad.		
Disk Encryption	• Disabled: Desactivar la encriptación.		
	 Enabled: Habilitar la encriptación. Esta característica mejora la seguridad de los datos, pero afecta ligeramente el rendimiento de lectura/escritura. Key Name: Seleccione o cree una clave privada, que es la clave del tenant. 		
	NOTA		
	 Después de crear una instancia, el estado de encriptación del disco y la clave no se pueden cambiar. La encriptación de disco no cifrará los datos de copia de respaldo almacenados en OBS. Para habilitar la encriptación de datos de copia de respaldo, póngase en contacto con el servicio de atención al cliente. 		
	• Para comprobar si el disco está cifrado, puede ver Disk Encrypted en la lista de instancias de base de datos.		
	 Si la encriptación de disco o la encriptación de datos de copia de respaldo están habilitados, mantenga la clave correctamente. Una vez que la clave está deshabilitada, eliminada o congelada, la base de datos no estará disponible y los datos no se restaurarán. Si la encriptación de disco está habilitado pero la encriptación de datos de 		
	copia de respaldo no está habilitado, puede restaurar datos a una nueva instancia desde copias de respaldo.		
	Si tanto la encriptación de disco como la encriptación de datos de copia de respaldo están habilitados, los datos no se pueden restaurar.		
	 Para obtener más información sobre cómo crear una clave, consulte "Creación de un CMK" en Guía de usuario de Data Encryption Workshop. 		

Administrator				
Password	Configure	Skip		
Administrator	rwuser			
Administrator Password			ø	Keep your password secure. The system cannot retrieve your password
Confirm Password			ίQ.	

Figura 3-4 Configuración del administrador

Tabla 3-5 Configuración del administrador

Parámetro	Descripción	
Password	 Configurar Introduzca y confirme la nueva contraseña de administrador. Después de crear una instancia, puede conectarse a la instancia mediante la contraseña. 	
	 Omitir Para iniciar sesión, tendrá que restablecer la contraseña más adelante en la página Basic Information. Si necesita conectarse a una instancia después de crearla, busque la instancia y elija More > Reset Password en la columna Operation para establecer primero una contraseña para la instancia. 	
Administrator	La cuenta predeterminada es rwuser.	
Administrator Password	Establezca una contraseña para el administrador. La contraseña debe tener entre 8 y 32 caracteres y contener letras mayúsculas, minúsculas, dígitos y al menos uno de los siguientes characters: ~!@#%^*=+?()\$ Mantenga esta contraseña segura. Si se pierde, el sistema no puede recuperarlo para usted.	
Confirm Password	Ingrese la contraseña de administrador de nuevo.	

Figura 3-5 Red, duración requerida y cantidad

Network	
VPC	default_upc Vew VPC
	A After the DDS instance is created, the VPC cannot be changed.
Subnet	default; subnet(192.1680.0.024) View Subnet
	Ausliable private IP addresses in the subnet: 227
Security Group	Sys-default;b611sicee-e859-4742-a418. + C View Security Group
	In a security group, rules that authorize connections to DB Instances apply to all DB Instances associated with the security group.
SSL.	D Ver Deals ()
	A To encrypt transmission, enable SSL
Database Port	Default port 8035
Gross-CIDR Access	Configure Skip
	Only configure roots-CIDR access if the CIDR blocks of the client and the replica set instance are different. For example, if the client CIDR block is 192.168.0.0/16 and the replica set instance's CIDR block is 172.165.0.0/4, add the
Enterprise Project	
Enterprise Project	Select • C Vew Project Management (2)

Tabla 3-6 Red

Parámetro	Descripción		
VPC	La VPC donde se encuentran instancias de base de datos. Una VPC aísla las redes para diferentes servicios. Le permite gestionar y configurar fácilmente redes privadas y cambiar las configuraciones de red.		
	Deberá crear o seleccionar la VPC requerida. Para obtener más información sobre cómo crear una VPC, consulte "Creación de una VPC" en la <i>Guía del usuario de Virtual Private Cloud</i> . Para obtener más información acerca de las restricciones en el uso de VPC, consulte Métodos de conexión .		
	Si no hay VPC disponibles, DDS crea una para usted de manera predeterminada.		
	Una vez creada la instancia de DDS, la VPC no podrá modificarse.		
Subnet	Una subred proporciona recursos de red dedicados que están lógicamente aislados de otras redes por razones de seguridad.		
	Una vez creada la instancia, puede cambiar la dirección IP privada asignada por la subred. Para obtener más información, consulte Cambio de una dirección IP privada .		
	No se admiten subredes IPv6. Se recomienda crear y seleccionar subredes IPv4.		
Security	Un grupo de seguridad controla el acceso entre DDS y otros servicios.		
Group	Si no hay grupos de seguridad disponibles, DDS crea una para usted de manera predeterminada.		
	NOTA Asegúrese de que haya una regla de grupo de seguridad configurada que permita a los clientes acceder a las instancias. Por ejemplo, seleccione una regla TCP entrante con el puerto predeterminado 8635 e introduzca una dirección IP de subred o seleccione un grupo de seguridad al que pertenece la instancia.		
SSL	Secure Sockets Layer (SSL) encripta las conexiones entre clientes y servidores, evitando que los datos sean manipulados o robados durante la transmisión.		
	Puede habilitar SSL para mejorar la seguridad de los datos. Después de crear una instancia, puede conectarse a ella mediante SSL.		
Database Port	El puerto DDS predeterminado es 8635, pero este puerto se puede modificar si es necesario. Si cambia el puerto, agregue una regla de grupo de seguridad correspondiente para permitir el acceso a la instancia.		

Parámetro	Descripción	
Cross-CIDR Access	 Configurar Si un cliente y una instancia de conjunto de réplicas se implementan en diferentes bloques de CIDR y el cliente no está en 192.168.0.0/16, 172.16.0.0/24 o 10.0.0.0/8, configure el acceso Cross-CIDR para que la instancia se comunique con el cliente. 	
	 Para asegurarse de que el ECS y la instancia de base de datos pueden comunicarse entre sí, configure la conexión haciendo referencia a Descripción general de la conexión de pares de VPC. 	
	 Se pueden configurar hasta 30 bloques CIDR, y cada uno de ellos puede superponerse pero no pueden ser los mismos. Es decir, los bloques CIDR de origen pueden solaparse pero no pueden ser los mismos. Los bloques CIDR no pueden comenzar con 127. La máscara IP permitida varía de 8 a 32. 	
	• Omitir Configurar el bloque CIDR del cliente más tarde. Después de crear una instancia de base de datos, puede configurar el acceso entre CIDR haciendo referencia a Configuración de acceso entre CIDR.	
Enterprise Project	Solo los usuarios de empresa pueden utilizar esta función. Para utilizar esta función, póngase en contacto con el servicio de atención al cliente.	
	Un proyecto empresarial es un modo de gestión de recursos en la nube, en el que los recursos y los miembros en la nube se gestionan de forma centralizada por proyecto.	
	Seleccione un proyecto de empresa en la lista desplegable. El proyecto predeterminado es default .	

Figura 3-6 Configuración avanzada

Advanced Settings	
Replica Set Parameter Template	Default-DDS-4.2-Replica
Automated Backup	0
Retention Period	- 7 + Enter an integer from 1 to 732.
Time Window	00:00 - 01:00 • GMT+08:00
Maintenance Window	Skip Configure ①
Tags	It is recommended that you use TMS's predefined tag function to add the same tags to different cloud resources. C View predefined tags
	Tag key Tag value
	You can add 20 more tags.

Parámetro	Descripción	
Replica Set Parameter Template	Parámetros que se aplican a las instancias del conjunto de réplicas. Después de crear una instancia, puede cambiar la plantilla de parámetros que configuró para la instancia para obtener el mejor rendimiento.	
	Para obtener más información, consulte Edición de una plantilla de parámetro.	
Automated Backup	DDS habilita una política de copia de respaldo automatizada de forma predeterminada, pero puede deshabilitarla después de crear una instancia. Una copia de respaldo completa automatizada se activa inmediatamente después de la creación de una instancia.	
	Para obtener más información, consulte Configuración de una copia de respaldo automatizada.	
Retention Period (days)	Retention Period se refiere al número de días que se conservan los datos. Puede aumentar el período de retención para mejorar la confiabilidad de los datos. El período de retención de copias de respaldo es de 1 a 732 días.	
Time Window	El intervalo de copia de respaldo es de 1 hora.	

Tabla 3-7 Configuración avanzada

Parámetro	Descripción
Tags	(Opcional) Puede agregar etiquetas a instancias DDS para que pueda buscar y filtrar rápidamente instancias especificadas por etiqueta. Cada instancia de DDS puede tener hasta 20 etiquetas.
	• Crear una etiqueta. Puede crear etiquetas en la consola DDS y configurar la etiqueta key y value .
	Key: Este parámetro es obligatorio.
	 Cada clave de etiqueta debe ser única para cada instancia.
	– Una clave de etiqueta consta de hasta 36 caracteres.
	 La clave debe consistir únicamente en dígitos, letras, guiones bajos (_), y guiones (-).
	Valor: Este parámetro es opcional.
	 El valor consta de hasta 43 caracteres.
	 El valor debe consistir únicamente en dígitos, letras, guiones bajos (_), puntos y guiones (-).
	 Agregar una etiqueta predefinida. Las etiquetas predefinidas se pueden utilizar para identificar múltiples recursos en la nube.
	Para etiquetar un recurso en la nube, puede seleccionar una etiqueta predefinida creada en la lista desplegable, sin introducir una clave y un valor para la etiqueta.
	Por ejemplo, si se ha creado una etiqueta predefinida, su clave es Usage y valor es Project1. Cuando configura la clave y el valor de un recurso en la nube, la etiqueta predefinida creada se mostrará en la página.
	Después de crear una instancia, puede hacer clic en el nombre de la instancia para ver sus etiquetas. En la página Tags , también puede modificar o eliminar las etiquetas . Además, puede buscar y filtrar rápidamente instancias especificadas por etiqueta .
	Puede agregar una etiqueta a una instancia después de crearla. Para obtener más información, consulte Adición de una etiqueta.

Si tiene alguna pregunta sobre el precio, haga clic en Price Details.

NOTA

El rendimiento de la instancia depende de las especificaciones que seleccione durante la creación. Los elementos de configuración de hardware que se pueden seleccionar incluyen la clase de instancia y el espacio de almacenamiento.

Paso 3 En la página mostrada, confirme los detalles de la instancia.

- Para instancias anuales/mensuales
 - Si necesita modificar las especificaciones, haga clic en Previous para volver a la página anterior.

- Si no necesita modificar las especificaciones, lea y acepte el contrato de servicio y haga clic en **Pay Now** para ir a la página de pago y completar el pago.
- Para instancias de pago por uso
 - Si necesita modificar las especificaciones, haga clic en **Previous** para volver a la página anterior.
 - Si no necesita modificar las especificaciones, lea y acepte el contrato de servicio y haga clic en Submit para comenzar a crear la instancia.
- **Paso 4** Haga clic en **Back to Instance List**. Después de crear una instancia DDS, puede ver y gestionarla en la página **Instances**.
 - Cuando se crea una instancia, el estado que se muestra en la columna **Status** es **Creating**. Este proceso dura unos 15 minutos. Una vez completada la creación, el estado cambia a **Available**.
 - Las instancias anuales/mensuales que se compraron en lotes tienen las mismas especificaciones, excepto el nombre y el ID de la instancia.

----Fin

3.2 Conexión a una instancia de conjunto de réplicas

3.2.1 Métodos de conexión

You can access DDS over private or public networks.

Método	Dirección IP	Escenario	Descripción
DAS	No requerido	DAS proporciona una GUI y le permite realizar operaciones visualizadas en la consola. La ejecución SQL, la gestión avanzada de bases de datos y la operación inteligente están disponibles para hacer que la gestión de bases de datos sea simple, segura e inteligente.	 Fácil de usar, seguro, avanzado e inteligente Recomendada
Red privada	Dirección IP privada	DDS proporciona una dirección IP privada de forma predeterminada. Si sus aplicaciones se ejecutan en un ECS en la misma subred de región, zona de disponibilidad y VPC que su instancia DDS, se recomienda utilizar una dirección IP privada para conectar el ECS a sus instancias DDS.	Rendimiento seguro y excelente

|--|

Método	Dirección IP	Escenario	Descripción
Red pública	EIP	 Si sus aplicaciones se ejecutan en un ECS que se encuentra en una región diferente de la donde se encuentra la instancia de base de datos, utilice una EIP para conectar el ECS a las instancias de base de datos de DDS. Si sus aplicaciones se despliegan en otra plataforma en la nube, se recomienda EIP. 	 Bajo nivel de seguridad Para una transmisión más rápida y una seguridad mejorada, se recomienda migrar sus aplicaciones a un ECS que esté en la misma subred que su instancia de DDS y utilizar una dirección IP privada para acceder a la instancia.

3.2.2 (Recomendado) Conexión a instancias de conjunto de réplicas mediante DAS

3.2.2.1 Descripción

DAS proporciona una GUI y le permite realizar operaciones visualizadas en la consola. La ejecución SQL, la gestión avanzada de bases de datos y la operación inteligente están disponibles para hacer que la gestión de bases de datos sea simple, segura e inteligente. Se recomienda utilizar DAS para conectarse a instancias de base de datos.

Esta sección describe cómo comprar una instancia de conjunto de réplicas en la consola de gestión y cómo conectarse a la instancia de conjunto de réplicas a través de DAS.

Proceso

Para comprar y conectarse a una instancia de conjunto de réplicas, realice los siguientes pasos:

- 1. Comprar una instancia de conjunto de réplicas.
- 2. Conectar a la instancia del conjunto de réplicas mediante DAS.

3.2.2.2 Conexión a una instancia de conjunto de réplicas mediante DAS

Data Admin Service (DAS) le permite gestionar instancias de bases de datos en una consola basada en web, simplificando la gestión de bases de datos y mejorando la eficiencia del trabajo. Puede conectar y gestionar instancias a través de DAS. De forma predeterminada, tiene el permiso necesario para el inicio de sesión remoto. Se recomienda utilizar el servicio DAS para conectarse a instancias. DAS es seguro y conveniente.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic 🔍 en la esquina superior izquierda y seleccione una región y un proyecto.

Si desea recursos informáticos y de red dedicados a su uso exclusivo, **habilite un DeC** y **solicite recursos de DCC**. Después de habilitar un DeC, puede seleccionar la región y el proyecto de DeC.

- **Paso 3** Haga clic = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.
- Paso 4 En la página Instances, busque la instancia de base de datos de destino y haga clic en Log In en la columna Operation.

También puede hacer clic en la instancia de base de datos de destino en la página **Instances**. En la página **Basic Information** mostrada, haga clic en **Log In** en la esquina superior derecha de la página.

Figura 3-7 Gestión de instancias

Renew Change to Yearly/Monthly			All DB in	tances 🔻 Enter a D	B instance name, a DB instan	ce ID, or an address. Q Search by Tag 😸 C 🖸
Name/ID ↓≡	DB Instance Type	DB Engine Version	Status ↓Ξ	Billing Mode	Address	Operation
dds-5099 70b2feaf6d76437a9bc28a09ca385dcdin02	Replica set	Community Edition 4.0	 Available 	Yearly/Monthly 31 days until expiration	mongodb://rwuser.****	Log In View Metric More 👻
e3d6949593814c46a89e0c95eebafbc3in02	Replica set	Community Edition 3.4	 Available 	Pay-per-use Created on Jan 20, 2020	mongodb://rwuser.****	Log In View Metric More 👻
97ecaf5ce9374c98a4a2d8b337b3da03in02	Replica set	Community Edition 3.4	 Available 	Pay-per-use Created on Jan 20, 2020	mongodb://rwuser.****	Log In View Metric More 👻
dds-3968 9b40c8c0ef9b4038b7b5327b13374ed7in02	Cluster	Community Edition 4.0	 Available 	Pay-per-use Created on Jan 19, 2020	mongodb://rwuser.****	Log In View Metric More 👻

Paso 5 En la página de inicio de sesión mostrada, introduzca el nombre de usuario y la contraseña del administrador y haga clic en Log In.

Para obtener más información acerca de cómo gestionar bases de datos a través de DAS, consulte **Gestión de instancias de DDS**.

----Fin

3.2.3 Conexión a una instancia de conjunto de réplicas a través de una red privada

3.2.3.1 Configuración de reglas de grupo de seguridad

Un grupo de seguridad es una colección de reglas de control de acceso para ECS e instancias de DDS que tienen los mismos requisitos de protección de seguridad y son de confianza mutua en una VPC.

Para garantizar la seguridad y confiabilidad de la base de datos, debe configurar reglas de grupo de seguridad para permitir que las direcciones IP y los puertos específicos accedan a instancias de DDS.

Puede conectarse a una instancia mediante la configuración de las reglas de grupo de seguridad de las dos maneras siguientes:

• Si el ECS y la instancia están en el mismo grupo de seguridad, pueden comunicarse entre sí de forma predeterminada. No es necesario configurar ninguna regla de grupo de seguridad. Vaya a Conexión a una instancia de conjunto de réplicas mediante Mongo Shell (red privada).

Figura 3-8 Mismo grupo de seguridad



• Si el ECS y la instancia están en diferentes grupos de seguridad, debe configurar las reglas de grupo de seguridad para ellos, por separado.





- Instancia: configura una inbound rule para el grupo de seguridad asociado a la instancia.
- ECS: La regla de grupo de seguridad predeterminada permite todos los paquetes de datos salientes. En este caso, no es necesario configurar una regla de grupo de seguridad para el ECS. Si no se permite que todo el tráfico llegue a la instancia, configure una regla de **outbound** para el ECS.

Esta sección describe cómo configurar una regla de entrada para una instancia.

Precauciones

- De forma predeterminada, una cuenta puede crear hasta 500 reglas de grupo de seguridad.
- Demasiadas reglas de grupo de seguridad aumentarán la latencia del primer paquete, por lo que se recomienda un máximo de 50 reglas para cada grupo de seguridad.
- Una instancia DDS solo puede asociarse a un grupo de seguridad.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

- Paso 2 Haga clic en 🔍 en la esquina superior izquierda, y seleccione una región y un proyecto.
- **Paso 3** Haga clic en = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia. Se muestra la página Basic Information.
- **Paso 5** En el área **Network Information** de la página **Basic Information**, haga clic en el grupo de seguridad.

Figura 3-10 Grupo de seguridad

Network Information			
VPC	dds-st-test-vpc	Subnet	dds-st-test-subnet-2 (1)
Security Group	Sys-default 🖉	Database Port	8635 🖉

También puede elegir **Connections** en el panel de navegación de la izquierda. En la pestaña **Private Connection**, en el área **Security Group**, haga clic en el nombre del grupo de seguridad.

Figura 3-11 Grupo de seguridad

Security Group				
Security Group	Sys-default 🖉			
Add Rule	Delete			С
Inbound Rules(1)	Outbound Rules	(1)		
Protocol & Port (?)		Source (?)	Description	
All		Sys-default		

- Paso 6 En la página Security Group, busque el grupo de seguridad de destino y haga clic en Manage Rule en la columna Operation.
- Paso 7 En la pestaña Inbound Rules, haga clic en Add Rule. Aparece el cuadro de diálogo Add Inbound Rule.
- Paso 8 Agregue una regla de grupo de seguridad como se le solicite.

Figura 3-12 Agregar regla de entrada

Add Inbound Rule Learn more about security group configuration.					×
i Inbound rules allow incoming traffic	to instances associated wi	h the security group.			
Security Group Sys-default You can import multiple rules in a batch.					
Protocol & Port ⑦	Туре	Source 🕐	Description	Operation	
TCP Example: 22 or 22-30	IPv4 💌	IP address 0.0.0.0/0	•	Operation v	
		🕀 Add Rule			
		OK Cancel			

Tabla 3-9 Configuración de reglas entrantes

Parámetro	Descripción	Ejemplo
Priority	Prioridad de regla de grupo de seguridad. El valor de prioridad varía de 1 a 100. La prioridad predeterminada es 1 y tiene la prioridad más alta. La regla de grupo de seguridad con un valor menor tiene mayor	1
	prioridad.	
Action	Las acciones de la regla del grupo de seguridad.	Allow
	Una regla con una acción de denegación invalida a otra con una acción de permiso si las dos reglas tienen la misma prioridad.	
Protocol & Port	El protocolo de red requerido para el acceso. Opciones disponibles: TCP, UDP, ICMP, o GRE	ТСР
	Puerto: el puerto en el que desea permitir el acceso a DDS. El puerto predeterminado es 8635. El puerto oscila entre 2100 y 9500 o puede ser 27017, 27018, o 27019.	8635
Туре	Tipo de dirección IP. Solo IPv4 y IPv6 son compatibles.	IPv4

Parámetro	Descripción	Ejemplo
Source	Especifica la dirección IP, el grupo de seguridad y el grupo de direcciones IP compatibles, que permiten el acceso desde direcciones IP o instancias de otro grupo de seguridad. Ejemplo:	0.0.0/0
	• Dirección IP única: 192.168.10.10/32	
	 Segmento de dirección IP: 192.168.1.0/24 	
	• Todas las direcciones IP: 0.0.0/0	
	• Grupo de seguridad: sg-abc	
	• Grupo de direcciones IP: ipGroup-test	
	Si introduce un grupo de seguridad, todos los ECS asociados al grupo de seguridad cumplen con la regla creada.	
	Para obtener más información acerca de los grupos de direcciones IP, consulte Grupo de direcciones IP .	
Description	(Opcional) Proporciona información adicional acerca de la regla del grupo de seguridad. Este parámetro es opcional.	-
	La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	

Paso 9 Haga clic en OK.

----Fin

3.2.3.2 Conexión a una instancia de conjunto de réplicas mediante Mongo Shell (red privada)

Mongo shell es el cliente por defecto para el servidor de base de datos MongoDB. Puede utilizar Mongo Shell para conectarse a instancias de base de datos y consultar, actualizar y gestionar datos en bases de datos. Para usar Mongo Shell, descargue e instale primero el cliente MongoDB y, a continuación, use el shell Mongo para conectarse a la instancia de base de datos.

De forma predeterminada, una instancia DDS proporciona una dirección IP privada. Si sus aplicaciones se despliegan en un ECS y están en la misma región y VPC que las instancias DDS, puede conectarse a las instancias DDS mediante una dirección IP privada para lograr una velocidad de transmisión rápida y una alta seguridad.

En esta sección se describe cómo utilizar Mongo Shell para conectarse a una instancia de conjunto de réplicas a través de una red privada.

El cliente MongoDB puede conectarse a una instancia con una conexión no cifrada o una conexión cifrada (SSL). Para mejorar la seguridad de la transmisión de datos, conéctese a instancias mediante SSL.

Prerrequisitos

- 1. Para obtener más información acerca de cómo crear e iniciar sesión en un ECS, consulte Comprar un ECS e iniciar sesión en un ECS.
- 2. Instale el cliente MongoDB en el ECS. Para garantizar la autenticación correcta, instale el cliente MongoDB de la misma versión que la instancia de destino.

Para obtener más información sobre cómo instalar un cliente MongoDB, consulte ¿Cómo puedo instalar un cliente MongoDB?

3. El ECS puede comunicarse con la instancia DDS. Para obtener más información, véase **Configuración de reglas de grupo de seguridad**.

Conexión SSL

AVISO

Si se conecta a una instancia a través de la conexión SSL, habilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo habilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

- Paso 1 Inicie sesión en la consola de gestión.
- Paso 2 Haga clic en 🔍 en la esquina superior izquierda, y seleccione una región y un proyecto.
- Paso 3 Haga clic en = en la esquina superior izquierda de la página y elija Databases > Document Database Service.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia.
- Paso 5 En el panel de navegación de la izquierda, elija Connections.
- Paso 6 En el área Basic Information, haga clic en 📥 junto al campo SSL.
- Paso 7 Cargue el certificado raíz al ECS para conectarse a la instancia.

A continuación se describe cómo cargar el certificado en un ECS de Linux y Windows:

 En Linux, ejecute el siguiente comando:
 scp<IDENTITY_FILE><REMOTE_USER>@<REMOTE_ADDRESS>:<REMOTE_DI R>

D NOTA

- IDENTITY_FILE es el directorio donde reside el certificado raíz. El permiso de acceso al archivo es 600.
- **REMOTE_USER** es el usuario del sistema operativo de ECS.
- **REMOTE_ADDRESS** es la dirección de ECS.
- **REMOTE_DIR** es el directorio del ECS al que se carga el certificado raíz.
- En Windows, cargue el certificado raíz mediante una herramienta de conexión remota.
- Paso 8 Conéctese a una instancia DDS.

Método 1: Uso de la dirección de conexión HA privada (recomendado)

DDS proporciona la dirección de conexión HA. El uso de esta dirección para conectarse a una instancia de conjunto de réplicas mejora el rendimiento de lectura/escritura de datos y evita que se notifiquen errores cuando se escriben datos desde el cliente después de una conmutación principal/en espera.

Ejemplo de comando:

```
./mongo "<Private HA connection address>" --ssl --sslCAFile<FILE_PATH> -- sslAllowInvalidHostnames
```

Descripción de parámetros:

 Private HA Connection Address: En la página Instances, haga clic en el nombre de la instancia. Se muestra la página Basic Information. Elija Connections. Haga clic en la pestaña Private Connection y obtenga la dirección de conexión de la instancia actual en el campo Private HA Connection Address.

Figura 3-13 Obtención de la dirección de conexión HA privada

Private Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	⊂ ₹	Subnet	dds-st-test-subnet-2 ()
Auto-switch Private IP Address			
Address			
Cross-CIDR Access	Disabled Enable		
Private HA Connection A	Address mongodb://rwuser: <password>@^</password>		/test?authSource=admin&replicaSet=replica 🗇 Learn more

El formato de la dirección de conexión HA privada es el siguiente. El nombre de usuario de la base de datos **rwuser** y la base de datos de autenticación **admin** no se pueden cambiar.

mongodb://**rwuser:**<*password*>@192.168.xx.xx:8635,192.168.xx.xx:8635/**test? authSource=admin&replicaSet=replica**

Preste atención a los siguientes parámetros en la dirección HA privada:

Tabla 3-10 Descripción del parámetro

Parámetro	Descripción
rwuser	Nombre de cuenta, es decir, el nombre de usuario de la base de datos.

Parámetro	Descripción		
<password></password>	Contraseña para la cuenta de la base de datos. Reemplácelo con la contraseña real.		
	Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcent (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.		
	Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25*** %21%24 .		
192.168.xx.xx:8635,192.168. xx.xx:8635	Dirección IP y puerto del nodo de la instancia del conjunto de réplicas		
test	El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.		
authSource=admin&replicaS et=replica	 La base de datos de autenticación del usuario rwuser debe ser admin. authSource=admin está fijo en el comando. 		
	 replica en replicaSet=replica es el nombre de un conjunto de réplicas. El conjunto de réplicas predeterminado de Huawei Cloud DDS es replica. 		

- FILE_PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: El certificado del conjunto de réplicas se genera utilizando la dirección IP de gestión interna para garantizar que la comunicación interna no ocupe recursos como la dirección IP del usuario y el ancho de banda. -sslAllowInvalidHostnames es necesario para la conexión SSL a través de una red privada.

Ejemplo de comandos:

./mongo "mongodb://rwuser:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/test? authSource=admin&replicaSet=replica" --ssl --sslCAFile/tmp/ca.crt -sslAllowInvalidHostnames

NOTA

- Si se conecta a una instancia a través de una dirección HA privada, agregue comillas dobles antes y después de la información de conexión.
- Para obtener más información sobre la conexión HA, consulte Conexión a una instancia de conjunto de réplicas para separación de lectura y escritura y alta disponibilidad.

Si se muestra la siguiente información, la instancia se conecta correctamente: replica:PRIMARY>

Ejecute el siguiente comando para acceder a la base de datos local:

use local

La información que aparecerá en pantalla será similar a la información siguiente:

```
switched to db local
```

Ejecute el siguiente comando para consultar oplog de conjunto de réplicas:

db.oplog.rs.find()

Método 2: Uso de la dirección de conexión HA privada (base de datos y cuenta definidas por el usuario)

Ejemplo de comando:

```
./mongo "<Private HA connection address>" --ssl --sslCAFile<FILE_PATH> --
sslAllowInvalidHostnames
```

Descripción de parámetros:

 Private HA Connection Address: En la página Instances, haga clic en el nombre de la instancia. Se muestra la página Basic Information. Elija Connections. Haga clic en la pestaña Private Connection y obtenga la dirección de conexión de la instancia actual en el campo Private HA Connection Address.

Figura 3-14 Obtención de la dirección de conexión HA privada

Private Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	Ť	Subnet	dds-st-test-subnet-2 ()
Auto-switch Private IP Address			
Address			
Cross-CIDR Access	Disabled Enable		
Private HA Connection	Address mongodb://rwuser: <password>@*</password>	/	test?authSource=admin&replicaSet=replica 🗇 Learn more

El formato de la dirección de conexión HA privada obtenida es el siguiente:

mongodb://**rwuser:**<*password*>@192.168.xx.xx:8635,192.168.xx.xx:8635/**test? authSource=admin&replicaSet=replica**

La siguiente tabla muestra los parámetros requeridos en la dirección de HA privada.

 Tabla 3-11 Información de parámetros

Parámetro	Descripción
rwuser	Nombre de usuario de base de datos. El valor predeterminado es rwuser . Puede cambiar el valor por el nombre de usuario en función de sus requisitos de servicio.

Parámetro	Descripción	
<password></password>	Contraseña para el nombre de usuario de la base de datos. Reemplácelo con la contraseña real.	
	Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.	
	Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25*** %21%24.	
192.168.xx.xx:8635,192.16 8.xx.xx:8635	Dirección IP y puerto del nodo de la instancia del conjunto de réplicas	
test	El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.	
authSource=admin&replic aSet=replica	 La base de datos de autenticación de usuario rwuser es admin. 	
	 En replica in replicaSet=replica, replica indica que el tipo de instancia es un conjunto de réplicas y que el formato no se puede cambiar. 	
	NOTA Si utiliza una base de datos definida por el usuario para la autenticación, cambie la base de datos de autenticación en la dirección de conexión HA por el nombre de la base de datos definida por el usuario. Además, reemplace rwuser con el nombre de usuario creado en la base de datos definida por el usuario.	

- FILE_PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: El certificado del conjunto de réplicas se genera utilizando la dirección IP de gestión interna para garantizar que la comunicación interna no ocupe recursos como la dirección IP del usuario y el ancho de banda. -sslAllowInvalidHostnames es necesario para la conexión SSL a través de una red privada.

Por ejemplo, si crea una base de datos definida por el usuario **Database** y un usuario **test1** en la base de datos, el comando de conexión es el siguiente:

./mongo "mongodb://test1:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/ Database?authSource=Database&replicaSet=replica" --ssl --sslCAFile/tmp/ca.crt -sslAllowInvalidHostnames

Method 3: Conéctese a un nodo único.

También puede utilizar la dirección IP privada de un nodo primario o secundario para acceder a la instancia del conjunto de réplicas. Este método afecta al rendimiento de lectura/escritura cuando se produce **una conmutación primaria/en espera**.

Ejemplo de comando:

./mongo --host <DB_HOST> --port <DB_PORT> -u <DB_USER> -p -authenticationDatabase admin --ssl --sslCAFile<FILE_PATH> -sslAllowInvalidHostnames

Descripción de parámetros:

Private Connection

• **DB_HOST** es la dirección IP privada del nodo primario o en espera de la instancia que se va a conectar.

Nodo primario: Puede leer y escribir datos en él.

Nodo secundario: Solo puede leer datos de él.

Public Connection

En la página **Instances**, haga clic en la instancia para ir a la página **Basic Information**. Elija **Connections**. En la pestaña **Private Connection**, obtenga la dirección IP del nodo correspondiente.

Figura 3-15 Obtención de la dirección IP de un nodo

	r dotte conne	ction				
Basic Information						
Database Port	8635 🖉			VI	PC	dds-st-test-vpc
SSL	1			Su	ıbnet	dds-st-test-subnet-2 ()
Auto-switch Private IP Address						
Address						
Cross-CIDR Access	Disab	led Enab	e			
Private HA Connection A	Address mong	odb://rwus	er: <password>@</password>		/te	est?authSource=admin&replicaSet=replica 🗇 Learn more
	Note	The par	ameters in orange are va	ariables and need	to be modified ba	sed on service requirements. For details, click Learn more.
Name/ID	Role	AZ	Private IP Address	Private Dom	EIP	Operation
dds-cc16_replica_n 9d5f8e0715fd48f8	Primary	az2	192.	9d5f8e0715f	Our Contract Output	Change Private IP Address More 👻
dds-cc16_replica_n 9f5c3b450cdc42fb	Secondary	az2	192.	9f5c3b450cd	Our Unbound	Change Private IP Address More 💌
dds-cc16_replica_n 232051a2bcc74d2	Hidden	az2	192.168.18.172			Change Private IP Address

• **DB_PORT** es el puerto de la base de datos. El valor predeterminado es 8635.

Puede hacer clic en la instancia para ir a la página **Basic Information**. En el panel de navegación de la izquierda, elija **Connections**. En la página mostrada, haga clic en la pestaña **Private Connection** y obtenga el puerto del **Database Port** en el área **Basic Information**.

Figura 3-16 Obtención del puerto

Private Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	F	Subnet	dds-st-test-subnet (

- **DB USER** es el usuario de la base de datos. El valor predeterminado es **rwuser**.
- FILE_PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: El certificado del conjunto de réplicas se genera utilizando la dirección IP de gestión interna para garantizar que la comunicación interna no ocupe recursos como la dirección IP del usuario y el ancho de banda. -sslAllowInvalidHostnames es necesario para la conexión SSL a través de una red privada.

Introduzca la contraseña de la cuenta de la base de datos cuando se le solicite:

Enter password:

Ejemplo de comandos:

./mongo --host 192.168.xx.xx --port 8635 -u rwuser -p --authenticationDatabase admin -ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames

Si se muestra la siguiente información, el nodo correspondiente se conecta correctamente:

- El nodo principal del conjunto de réplicas está conectado. replica: PRIMARY>
- El nodo en espera del conjunto de réplicas está conectado. replica: SECONDARY>

----Fin

Conexión sin encriptar

AVISO

Si se conecta a una instancia a través de una conexión no cifrada, deshabilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo deshabilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

- **Paso 1** Inicie sesión en el ECS.
- Paso 2 Conéctese a una instancia DDS.

Método 1: Conexión de alta disponibilidad (recomendado)

DDS proporciona la dirección de conexión HA. El uso de esta dirección para conectarse a una instancia de conjunto de réplicas mejora el rendimiento de lectura/escritura y evita que se notifiquen errores cuando se escriben datos desde el cliente después de una conmutación principal/en espera.

Ejemplo de comando:

./mongo "<Private HA Connection Address>"

Private HA Connection Address: En la página **Instances**, haga clic en el nombre de la instancia. Se muestra la página **Basic Information**. Elija **Connections**. Haga clic en la pestaña **Private Connection** y obtenga la dirección de conexión de la instancia actual en el campo **Private HA Connection Address**.

Figura 3-17 Obtención de la dirección de conexión HA privada

Private Connection	Public Connection			
Basic Information				
Database Port	8635 🖉	VPC	dds-st-test-vpc	
SSL	ج ج	Subnet	dds-st-test-subnet-2 ()	
Auto-switch Private IP Address				
Address				
Cross-CIDR Access	Disabled Enable			
Private HA Connection	n Address mongodb://rwuser: <password>@'</password>		/test?authSource=admin&replicaSet=replica 🗇 Learn more	

El formato de la dirección de conexión HA privada es el siguiente. El nombre de usuario de la base de datos **rwuser** y la base de datos de autenticación **admin** no se pueden cambiar.

mongodb://**rwuser:**<*password*>@192.168.xx.xx:8635,192.168.xx.xx:8635/**test? authSource=admin&replicaSet=replica**

Preste atención a los siguientes parámetros en la dirección HA privada:

Parámetro	Descripción
rwuser	Nombre de cuenta, es decir, el nombre de usuario de la base de datos.
<password></password>	Contraseña para la cuenta de la base de datos. Reemplácelo con la contraseña real.
	Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.
	Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25***%21%24 .
192.168.xx.xx:8635,192.168.x x.xx:8635	Dirección IP y puerto del nodo de la instancia del conjunto de réplicas
test	El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.
authSource=admin&replicaSet =replica	• La base de datos de autenticación del usuario rwuser debe ser admin . authSource=admin está fijo en el comando.
	• replica en replicaSet=replica es el nombre de un conjunto de réplicas. El conjunto de réplicas predeterminado de Huawei Cloud DDS es replica.

Tabla 3-12 Descripción del parámetro

Ejemplo de comandos:

./mongo "mongodb://rwuser:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/test? authSource=admin&replicaSet=replica"

Si se muestra la siguiente información, la instancia se conecta correctamente: replica:PRIMARY>

Ejecute el siguiente comando para acceder a la base de datos local:

use local

La información que aparecerá en pantalla será similar a la información siguiente:

switched to db local

Ejecute el siguiente comando para consultar oplog de conjunto de réplicas:

db.oplog.rs.find()

Método 2: Conexión HA privada (base de datos y cuenta definidas por el usuario)

Ejemplo de comando:

./mongo "<Private HA Connection Address>"

Private HA Connection Address: En la página **Instances**, haga clic en el nombre de la instancia. Se muestra la página **Basic Information**. Elija **Connections**. Haga clic en la pestaña **Private Connection** y obtenga la dirección de conexión de la instancia actual en el campo **Private HA Connection Address**.

Figura 3-18 Obtención de la dirección de conexión HA privada

Private Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	7	Subnet	dds-st-test-subnet-2 ()
Auto-switch Private IP Address			
Address			
Cross-CIDR Access	Disabled Enable		
Private HA Connection A	address mongodb://rwuser: <password>@"</password>		/test?authSource=admin&replicaSet=replica ☐ Learn more

El formato de la dirección de conexión HA privada obtenida es el siguiente:

mongodb://**rwuser:**<*password*>@192.168.xx.xx:8635,192.168.xx.xx:8635/**test? authSource=admin&replicaSet=replica**

La siguiente tabla muestra los parámetros requeridos en la dirección de HA privada.

Tabla 3-13 Información de parámetros

Parámetro	Descripción
rwuser	Nombre de usuario de base de datos. El valor predeterminado es rwuser . Puede cambiar el valor por el nombre de usuario en función de sus requisitos de servicio.

Parámetro	Descripción	
<password></password>	Contraseña para el nombre de usuario de la base de datos. Reemplácelo con la contraseña real.	
	Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.	
	Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25***%21%24.	
192.168.xx.xx:8635,192.168 .xx.xx:8635	Dirección IP y puerto del nodo de la instancia del conjunto de réplicas	
test	El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.	
authSource=admin&replica Set=replica	 La base de datos de autenticación de usuario rwuser es admin. 	
	• En replica in replicaSet=replica , replica indica que el tipo de instancia es un conjunto de réplicas y que el formato no se puede cambiar.	
	NOTA Si utiliza una base de datos definida por el usuario para la autenticación, cambie la base de datos de autenticación en la dirección de conexión HA por el nombre de la base de datos definida por el usuario. Además, reemplace rwuser con el nombre de usuario creado en la base de datos definida por el usuario.	

Por ejemplo, si crea una base de datos definida por el usuario **Database** y un usuario **test1** en la base de datos, el comando de conexión es el siguiente:

./mongo "mongodb://test1:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/ Database?authSource=Database&replicaSet=replica"

Method 3: Conéctese a un nodo único.

También puede utilizar la dirección IP privada de un nodo primario o secundario para acceder a la instancia del conjunto de réplicas. Este método afecta al rendimiento de lectura/escritura cuando se produce una conmutación primaria/en espera.

Ejemplo de comando:

./mongo --host <*DB_HOST*> --port <*DB_PORT*> -u <*DB_USER*> -p -authenticationDatabase admin

Descripción de parámetros:

• **DB_HOST** es la dirección IP privada del nodo primario o en espera de la instancia que se va a conectar.

Nodo primario: Puede leer y escribir datos en él.

Nodo secundario: Solo puede leer datos de él.

En la página **Instances**, haga clic en la instancia para ir a la página **Basic Information**. Elija **Connections**. En la pestaña **Private Connection**, obtenga la dirección IP del nodo correspondiente.

ate Connection	Public Conne	ction				
Basic Information						
Database Port	8635 🖉			VI	PC	dds-st-test-vpc
SSL	○ ±			Su	ıbnet	dds-st-test-subnet-2 ()
Auto-switch Private IP Address						
Address						
Cross-CIDR Access	Disab	led Enab	le			
Private HA Connection A	Address mong	odb://rwus	er: <password>@</password>		/t	est?authSource=admin&replicaSet=replica 🗇 Learn more
	Note	The par	ameters in orange are va	riables and need	to be modified ba	sed on service requirements. For details, click Learn more.
Name/ID	Role	AZ	Private IP Address	Private Dom	EIP	Operation
dds-cc16_replica_n 9d5f8e0715fd48f8	Primary	az2	192.	9d5f8e0715f	Onbound	Change Private IP Address More 👻
dds-cc16_replica_n 9f5c3b450cdc42fb	Secondary	az2	192.	9f5c3b450cd	Our Unbound	Change Private IP Address More 👻
dds-cc16_replica_n	Hidden	az2	192.168.18.172			Change Private IP Address

Figura 3-19 Obtención de la dirección IP de un nodo

• **DB PORT** es el puerto de la base de datos. El valor predeterminado es 8635.

Puede hacer clic en la instancia para ir a la página **Basic Information**. En el panel de navegación de la izquierda, elija **Connections**. En la página mostrada, haga clic en la pestaña **Private Connection** y obtenga el puerto del **Database Port** en el área **Basic Information**.

Figura 3-20 Obtención del puerto

Private Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	Ŧ	Subnet	dds-st-test-subnet (

• **DB_USER** es el usuario de la base de datos. El valor predeterminado es **rwuser**.

Ejemplo de comandos:

```
./mongo --host 192.168.xx.xx --port 8635 -u rwuser -p --authenticationDatabase admin
```

Introduzca la contraseña de la cuenta de la base de datos cuando se le solicite:

Enter password:

Si se muestra la siguiente información, el nodo correspondiente se conecta correctamente:

• El nodo principal del conjunto de réplicas está conectado. replica: PRIMARY> • El nodo en espera del conjunto de réplicas está conectado. replica:SECONDARY>

----Fin

3.2.3.3 Conexión a réplicas de lectura mediante Mongo Shell

Mongo shell es el cliente por defecto para el servidor de base de datos MongoDB. Puede utilizar Mongo Shell para conectarse a instancias de base de datos y consultar, actualizar y gestionar datos en bases de datos. Para usar Mongo Shell, descargue e instale primero el cliente MongoDB y, a continuación, use el shell Mongo para conectarse a la instancia de base de datos.

De forma predeterminada, una instancia DDS proporciona una dirección IP privada. Si sus aplicaciones se despliegan en un ECS y están en la misma región y VPC que las instancias DDS, puede conectarse a las instancias DDS mediante una dirección IP privada para lograr una velocidad de transmisión rápida y una alta seguridad.

En esta sección se describe cómo utilizar Mongo Shell para conectarse a una réplica de lectura a través de una red privada.

Puede conectarse a una réplica de lectura mediante una conexión SSL o una conexión sin cifrar. La conexión SSL es encriptada y más segura. Para mejorar la seguridad de la transmisión de datos, conéctese a instancias mediante SSL.

Prerrequisitos

- 1. Para obtener más información acerca de cómo crear e iniciar sesión en un ECS, consulte Comprar un ECS e iniciar sesión en un ECS.
- 2. Instale el cliente MongoDB en el ECS. Para garantizar la autenticación correcta, instale el cliente MongoDB de la misma versión que la instancia de destino.

Para obtener más información sobre cómo instalar un cliente MongoDB, consulte ¿Cómo puedo instalar un cliente MongoDB?

3. El ECS puede comunicarse con la instancia DDS. Para obtener más información, véase **Configuración de reglas de grupo de seguridad**.

Conexión SSL

AVISO

Si se conecta a una instancia a través de la conexión SSL, habilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo habilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

- Paso 1 En la página Instances, haga clic en el nombre de la instancia.
- Paso 2 En el panel de navegación de la izquierda, elija Connections.
- Paso 3 En el área Basic Information, haga clic en 📥 junto al campo SSL.
- Paso 4 Cargue el certificado raíz al ECS para conectarse a la instancia.

A continuación se describe cómo cargar el certificado en un ECS de Linux y Windows:

 En Linux, ejecute el siguiente comando:
 scp<IDENTITY_FILE><REMOTE_USER>@<REMOTE_ADDRESS>:<REMOTE_DI R>

NOTA

- IDENTITY_FILE es el directorio donde reside el certificado raíz. El permiso de acceso al archivo es 600.
- **REMOTE_USER** es el usuario del sistema operativo de ECS.
- **REMOTE_ADDRESS** es la dirección de ECS.
- **REMOTE_DIR** es el directorio del ECS al que se carga el certificado raíz.
- En Windows, cargue el certificado raíz mediante una herramienta de conexión remota.
- **Paso 5** Conéctese a una instancia DDS. La consola DDS proporciona la dirección de conexión de réplica de lectura. Puede utilizar esta dirección para conectarse a la réplica de lectura.

Ejemplo de comando:

```
./mongo "<Read replica connection address>" --ssl --sslCAFile<FILE_PATH> --
sslAllowInvalidHostnames
```

Descripción de parámetros:

• Read Replica Connection Address: En la página Instances, haga clic en la instancia para ir a la página Basic Information. Elija Connections. Haga clic en la pestaña Private Connection. En el área Address, obtenga la dirección de conexión de la instancia de réplica de lectura.

Figura 3-21 Obtención de la dirección de conexión de réplica de lectura

Private Connection	Public Conr	lection				
Basic Information						
Database Port	8635 🖉		VPC	dds-st	-test-vpc	
SSL	<u> </u>		Subnet	dds-st	-test-subnet-2	
Auto-switch Private IP A	ddress					
Address						
Cross-CIDR Access		Disabled Enable				
Private HA Connection A	Address	mongodb://rwuser: <password>@</password>		1:8635/test?auth	nSource=admin&replicaSet=replic	a 🗇 Learn more
Read replica {1} Connec	ction Address	mongodb://rwuser: <password>@</password>	est?authSource	e=admin 🗇		
Read replica {2} Connec	ction Address	mongodb://rwuser: <password>@</password>	'test?authSour	ce=admin 🗇		

El formato de la dirección de conexión de réplica de lectura es el siguiente. El nombre de usuario de la base de datos **rwuser** y la base de datos de autenticación **admin** no se pueden cambiar.

mongodb://rwuser:<*password*>@192.168.xx.xx:8635/test?authSource=admin

Preste atención a los siguientes parámetros en la dirección de conexión de réplica de lectura:

Parámetro	Descripción	
rwuser	Nombre de cuenta, es decir, el nombre de usuario de la base de datos.	
<password></password>	Contraseña para la cuenta de la base de datos. Reemplácelo con la contraseña real.	
	Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.	
	Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25*** %21%24.	
192.168.xx.xx:8635	Dirección IP y puerto de la réplica de lectura de la instancia del conjunto de réplicas	
test	El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.	
authSource=admin	La base de datos de autenticación del usuario rwuser debe ser admin . authSource=admin está fijo en el comando.	

 Tabla 3-14 Descripción del parámetro

- FILE_PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: El certificado del conjunto de réplicas se genera utilizando la dirección IP de gestión interna para garantizar que la comunicación interna no ocupe recursos como la dirección IP del usuario y el ancho de banda. -sslAllowInvalidHostnames es necesario para la conexión SSL a través de una red privada.

Ejemplo de comandos:

./mongo "mongodb://rwuser:<*password*>@192.168.xx.xx:8635/test?authSource=admin" --ssl --sslCAFile/tmp/ca.crt --sslAllowInvalidHostnames

NOTA

Cuando se conecte a una instancia mediante la dirección de conexión de réplica de lectura, agregue comillas dobles (") antes y después de la información de conexión.

Si se muestra la siguiente información, la instancia se conecta correctamente: replica:SECONDARY>

----Fin

Conexión sin encriptar

AVISO

Si se conecta a una instancia a través de una conexión no cifrada, deshabilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo deshabilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

- Paso 1 Inicie sesión en el ECS.
- Paso 2 Conéctese a una instancia DDS. La consola DDS proporciona la dirección de conexión de réplica de lectura. Puede utilizar esta dirección para conectarse a la réplica de lectura.

Ejemplo de comando:

./mongo "<Read replica connection address>"

Read Replica Connection Address: En la página **Instances**, haga clic en la instancia para ir a la página **Basic Information**. Elija **Connections**. Haga clic en la pestaña **Private Connection**. En el área **Address**, obtenga la dirección de conexión de la instancia de réplica de lectura.

Figura 3-22 Obtención de la dirección de conexión de réplica de lectura

Private Connection	Public Conn	ection			
Basic Information					
Database Port	8635 🖉		VPC	dds-st-test-vpc	
SSL	● ₹		Subnet	dds-st-test-subnet-2	
Auto-switch Private IP A	Address				
Address					
Cross-CIDR Access		Disabled Enable			
Private HA Connection	Address	mongodb://rwuser: <password>@</password>		1:8635/test?authSource=admin&replicaSet=replica 🗇 Learn	more
Read replica {1} Conne	ction Address	mongodb://rwuser: <password>@</password>	est?authSource	ze=admin ⊡	
Read replica {2} Conne	ction Address	mongodb://rwuser: <password>@</password>	'test?authSour	rce=admin 🗇	

El formato de la dirección de conexión de réplica de lectura es el siguiente. El nombre de usuario de la base de datos **rwuser** y la base de datos de autenticación **admin** no se pueden cambiar.

mongodb://rwuser:<password>@192.168.xx.xx:8635/test?authSource=admin

Preste atención a los siguientes parámetros en la dirección HA privada:

Parámetro	Descripción
rwuser	Nombre de cuenta, es decir, el nombre de usuario de la base de datos.
<password></password>	Contraseña para la cuenta de la base de datos. Reemplácelo con la contraseña real.
	Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.
	Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25***%21%24.
192.168.xx.xx:8635	Dirección IP y puerto de la réplica de lectura de la instancia del conjunto de réplicas
test	El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.
authSource=admin	La base de datos de autenticación del usuario rwuser debe ser admin . authSource=admin está fijo en el comando.

Ejemplo de comandos:

./mongo "mongodb://rwuser:password>@192.168.xx.xx:8635/test?authSource=admin"

Si se muestra la siguiente información, la instancia se conecta correctamente: replica:SECONDARY>

----Fin

3.2.4 Conexión a una instancia de conjunto de réplicas a través de una red pública

3.2.4.1 Vinculación y desvinculación de una EIP

Después de crear una instancia, puede enlazar una EIP a ella para permitir el acceso externo. Si más adelante desea prohibir el acceso externo, también puede desvincular la EIP de la instancia de base de datos.

Precauciones

- La supresión de una EIP vinculada no significa que la EIP no esté vinculada.
- Antes de acceder a una base de datos, solicite una EIP en la consola de VPC. A continuación, agregue una regla de entrada para permitir las direcciones IP o los intervalos de direcciones IP de los ECS. Para obtener más información, véase Configuración de reglas de grupo de seguridad.

• En la instancia de conjunto de réplicas, solo los nodos primarios y secundarios pueden tener una EIP enlazada. Para cambiar la EIP que se ha enlazado a un nodo, primero debe desvincularlo del nodo.

Vinculación de una EIP

Paso 1 Inicie sesión en la consola de gestión.

- **Paso 2** Haga clic en 🔍 en la esquina superior izquierda y seleccione una región y un proyecto.
- **Paso 3** Haga clic en = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.
- Paso 4 En la página Instances, haga clic en el nombre de instancia del conjunto de réplicas.
- Paso 5 En el panel de navegación de la izquierda, elija Connections. Haga clic en la pestaña Public Connection. En el área Basic Information, localice el nodo al que desea enlazar una EIP y haga clic en Bind EIP en la columna Operation.

Figura 3-23 Vinculación de una EIP

Basic Informatio	on					
Database Port	86	i35 🖉			SSL	▲
Auto-switch Privat Address	e IP					
Address						
Public Network Co	nnection A	ddress	Unbound			
Name/ID	Role	AZ	Private	EIP	Operation	
dds-df26_r	Second	az4	19	🕲 Un	Change Private IP Address	Bind EIP
dds-df26_r	Primary	az4	1 .	🕲 Un	Change Private IP Address	Bind EIP

También puede localizar el nodo en el **Node Information area** de la página **Basic Information** y hacer clic en **Bind EIP** en la columna **Operation**.

Figura 3-24 Vinculación de una EIP

Node Information						
Add Secondary Nodes	Switch Add R	ead Replicas				
Replica set nodes Rea	d replicas					
Name/ID	Role	Status	AZ	Private IP Address	EIP	Operation
dds-df26_replica_node_1 6b	Secondary	Available	az4	192.16	O Unbound	View Metric Change Private IP Address Bind EIP

Paso 6 En el cuadro de diálogo que se muestra, se muestran todos las EIP independientes disponibles. Seleccione la EIP requerido y haga clic en OK. Si no se muestran EIPs disponibles, haga clic en View EIP y cree una EIP en la consola de VPC.

Figura 3-25 Selección de una EIP

For out	security purpo bound and inb	oses, after bindi ound rules in th	ng the EIP, use <mark>SSL</mark> to co e security group.	onnect to	the database and add	
lode	Information	Node Name		Statu	S	
				Ə A	Available	
elect	EIP					(
	EIP		Status		Bandwidth	
۲			⊗ Unbound		5 Mbit/s	
0			🕲 Unbound		5 Mbit/s	
0			🕲 Unbound		88 Mbit/s	

Paso 7 Localice el nodo de destino. En la columna EIP, puede ver la EIP que estaba enlazada.
Para desvincular una EIP de la instancia, consulte Desvinculación de una EIP.
----Fin

Desvinculación de una EIP

- Paso 1 Inicie sesión en la consola de gestión.
- **Paso 2** Haga clic en 🔍 en la esquina superior izquierda y seleccione una región y un proyecto.
- Paso 3 Haga clic en = en la esquina superior izquierda de la página y elija Databases > Document Database Service.
- **Paso 4** En la página **Instances**, haga clic en la instancia del conjunto de réplicas que se ha enlazado con una EIP.
- Paso 5 En el panel de navegación de la izquierda, elija Connections. Haga clic en la pestaña Public Connection. En el área Basic Information, localice el nodo y haga clic en Unbind EIP en la columna Operation.

Figura 3-26 Desvinculación de una EIP

Nam	Role	AZ	Private I	EIP	Operation
31f3	Secondary	az1p	192.168	🕲 Unbou	Change Private IP Address Bind EIP
e328	Primary	az1p	192.168		Change Private IP Address Unbind EIP
40fc	Hidden	az1p	192.168		Change Private IP Address

También puede localizar el nodo en el **Node Information area** de la página **Basic Information** y hacer clic en **Unbind EIP** en la columna **Operation**.

Paso 6 En el cuadro de diálogo que se muestra, haga clic en Yes.

Para enlazar una EIP a la instancia de nuevo, consulte Vinculación de una EIP.

----Fin

3.2.4.2 Configuración de reglas de grupo de seguridad

Un grupo de seguridad es una colección de reglas de control de acceso para ECS e instancias de DDS que tienen los mismos requisitos de protección de seguridad y son de confianza mutua en una VPC.

Para garantizar la seguridad y confiabilidad de la base de datos, debe configurar reglas de grupo de seguridad para permitir que las direcciones IP y los puertos específicos accedan a la instancia.

Si intenta conectarse a una instancia a través de una EIP, debe configurar una regla de entrada para el grupo de seguridad asociado a la instancia.

Precauciones

- De forma predeterminada, una cuenta puede crear hasta 500 reglas de grupo de seguridad.
- Demasiadas reglas de grupo de seguridad aumentarán la latencia del primer paquete, por lo que se recomienda un máximo de 50 reglas para cada grupo de seguridad.
- Una instancia DDS solo puede asociarse a un grupo de seguridad.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en 🔍 en la esquina superior izquierda y seleccione una región y un proyecto.

Paso 3 Haga clic en = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia. Se muestra la página Basic Information.
- **Paso 5** En el área Network Information de la página Basic Information, haga clic en el grupo de seguridad.

Figura 3-27 Grupo de seguridad

Network Information			
VPC	dds-st-test-vpc	Subnet	dds-st-test-subnet-2 (1)
Security Group	Sys-default 🖉	Database Port	8635 🖉

También puede elegir **Connections** en el panel de navegación de la izquierda. En la pestaña **Public Connection**, en el área **Security Group**, haga clic en el nombre del grupo de seguridad.

Figura 3-28 Grupo de seguridad

Security Group		
Security Group Sys-default 🖉		
Add Rule Delete		C
Inbound Rules(1) Outbound Rules	(1)	
Protocol & Port ⑦	Source ⑦	Description
All	Sys-default	-

- Paso 6 En la página Security Group, busque el grupo de seguridad de destino y haga clic en Manage Rule en la columna Operation.
- Paso 7 En la pestaña Inbound Rules, haga clic en Add Rule. Aparece el cuadro de diálogo Add Inbound Rule.
- Paso 8 Agregue una regla de grupo de seguridad como se le solicite.

Figura 3-29 Agregar regla de entrada

dd Inbound Rule Learn more about security group configuration.									
() Inbound rules allow incoming traffic to instances associated with the security group.									
Security Group Sys-default You can import multiple rules in a batch.									
Protocol & Port ⑦	Туре	Source ⑦	Description	Operation					
TCP • Example: 22 or 22-30 •	IPv4 v	IP address 0.0.0.0/0	•	Operation 🗸					
Add Rule									
		OK Cancel							

Parámetro	Descripción	Valor de ejemplo
Priority	Prioridad de regla de grupo de seguridad. El valor de prioridad varía de 1 a 100. La prioridad predeterminada es 1 y tiene la prioridad más alta. La regla de grupo de seguridad con un valor menor tiene mayor prioridad.	1
Action	Las acciones de la regla del grupo de seguridad. Una regla con una acción de denegación invalida a otra con una acción de permiso si las dos reglas tienen la misma prioridad.	Allow
Protocol & Port	El protocolo de red requerido para el acceso. La opción puede ser All, TCP, UDP, ICMP, o GRE.	ТСР
	Puerto: el puerto en el que desea permitir el acceso a DDS. El puerto predeterminado es 8635. El puerto oscila entre 2100 y 9500 o puede ser 27017, 27018, o 27019.	8635
Туре	Tipo de dirección IP. Solo IPv4 y IPv6 son compatibles.	IPv4
Source	 Especifica la dirección IP, el grupo de seguridad y el grupo de direcciones IP compatibles, que permiten el acceso desde direcciones IP o instancias de otro grupo de seguridad. Ejemplo: Dirección IP única: 192.168.10.10/32 Segmento de dirección IP: 	0.0.0/0
	192.168.1.0/24	
	 Iodas las direcciones IP: 0.0.0.0/0 Grupo de seguridad: sg-abc 	
	 Grupo de seguridad. sg-abe Grupo de direcciones IP: ipGroup-test 	
	Si introduce un grupo de seguridad, todos los ECS asociados al grupo de seguridad cumplen con la regla creada.	
	Para obtener más información acerca de los grupos de direcciones IP, consulte Grupo de direcciones IP .	

Tabla 3-16 Configuración de reglas entrantes

Parámetro	Descripción	Valor de ejemplo
Description	(Opcional) Proporciona información adicional acerca de la regla del grupo de seguridad. Este parámetro es opcional.	-
	La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	

Paso 9 Haga clic en OK.

----Fin

3.2.4.3 Conexión a una instancia de conjunto de réplicas mediante Mongo Shell (Red pública)

En los siguientes escenarios, puede acceder a una instancia DDS desde Internet vinculando una EIP a la instancia.

Escenario 1: Las aplicaciones se despliegan en un ECS y no están en la misma región que la instancia DDS.





Escenario 2: Sus aplicaciones se despliegan en un servidor en la nube proporcionado por otros proveedores.

Figura 3-31 Acceso a DDS desde otros servidores en la nube



En esta sección se describe cómo utilizar Mongo Shell para conectarse a una instancia de conjunto de réplicas a través de una EIP.

Puede conectarse a una instancia mediante una conexión SSL o una conexión sin cifrar. La conexión SSL es encriptada y más segura. Para mejorar la seguridad de la transmisión de datos, conéctese a instancias mediante SSL.

Prerrequisitos

- 1. Para obtener más información acerca de cómo crear e iniciar sesión en un ECS, consulte Comprar un ECS e iniciar sesión en un ECS.
- 2. Vincule una **EIP** a la instancia del conjunto de réplicas y configure las reglas del grupo de seguridad para garantizar que se pueda acceder a la instancia del conjunto de réplicas desde un ECS.
- 3. Instale el cliente MongoDB en el ECS.

Para obtener más información sobre cómo instalar un cliente MongoDB, consulte ¿Cómo puedo instalar un cliente MongoDB?

D NOTA

La versión del cliente MongoDB instalado debe ser la misma que la versión de instancia.

Conexión de SSL

AVISO

Si se conecta a una instancia a través de la conexión SSL, habilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo habilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

- Paso 1 Inicie sesión en la consola de gestión.
- **Paso 2** Haga clic en 🔍 en la esquina superior izquierda, y seleccione una región y un proyecto.
- **Paso 3** Haga clic en = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia.
- Paso 5 En el panel de navegación de la izquierda, elija Connections.
- Paso 6 En el área Basic Information, haga clic en 📥 junto al campo SSL.
- Paso 7 Cargue el certificado raíz al ECS para conectarse a la instancia.

A continuación se describe cómo cargar el certificado en un ECS de Linux y Windows:

 En Linux, ejecute el siguiente comando:
 scp<IDENTITY_FILE><REMOTE_USER>@<REMOTE_ADDRESS>:<REMOTE_DI R>

D NOTA

- IDENTITY_FILE es el directorio donde reside el certificado raíz. El permiso de acceso al archivo es 600.
- **REMOTE_USER** es el usuario del sistema operativo de ECS.
- **REMOTE_ADDRESS** es la dirección de ECS.
- **REMOTE_DIR** es el directorio del ECS al que se carga el certificado raíz.
- En Windows, cargue el certificado raíz mediante una herramienta de conexión remota.

Paso 8 Conéctese a la instancia en el directorio donde se encuentra el cliente MongoDB.

Método 1: Uso de una dirección de conexión de red pública

Ejemplo de comando:

./mongo "<*Public network connection address*>" --ssl --sslCAFile<*FILE_PATH*> -sslAllowInvalidHostnames

Descripción de parámetros:

• Public Network Connection Address: En la página Instances, haga clic en la instancia para cambiar a la página Basic Information. En el panel de navegación de la izquierda, elija Connections. Haga clic en la pestaña Public Connection y obtenga la dirección de conexión de red pública.

Figura 3-32 Obtención de la dirección de conexión de red pública

Basic Information		
Database Port 8635 🖉	SSL	▲
Auto-switch Private IP Address		
Address		
Public Network Connection Address	mongodb://rwuser: <password>@10.1</password>	t?authSource=admin 🗗 Learn more
	Note The parameters in orange are variate uirements. For details, click Learn more.	ables and need to be modified based on service req

El formato de la dirección de conexión pública es el siguiente. El nombre de usuario de la base de datos **rwuser** y la base de datos de autenticación **admin** no se pueden cambiar.

mongodb://**rwuser:**<*password*>@192.168.xx.xx:8635/**test?authSource=admin** Preste atención a los siguientes parámetros en la dirección de conexión de red pública:

 Tabla 3-17 Descripción del parámetro

Parámetro	Descripción
rwuser	Nombre de cuenta, es decir, el nombre de usuario de la base de datos.

Parámetro	Descripción
<pre><password></password></pre>	Contraseña para la cuenta de la base de datos. Reemplácelo con la contraseña real.
	Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.
	Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25*** %21%24.
192.168.xx.xx:8635	La EIP y el puerto enlazados al nodo de la instancia del conjunto de réplicas.
authSource=admin	La base de datos de autenticación del usuario rwuser debe ser admin . authSource=admin está fijo en el comando.

- FILE_PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: El certificado del conjunto de réplicas se genera utilizando la dirección IP de gestión interna para garantizar que la comunicación interna no ocupe recursos como la dirección IP del usuario y el ancho de banda. -sslAllowInvalidHostnames es necesario para la conexión SSL a través de una red pública.

Ejemplo de comandos:

./mongo "mongodb://rwuser:<*password*>@192.168.xx.xx:8635/test?authSource=admin" --ssl --sslCAFile/tmp/ca.crt --sslAllowInvalidHostnames

D NOTA

- Si se conecta a una instancia a través de una dirección HA pública, agregue comillas dobles antes y después de la información de conexión.
- Mejorar el rendimiento de lectura y escritura y evitar que se notifiquen errores cuando se escriben datos desde el cliente después de una conmutación principal/en espera. Para obtener más información acerca de cómo conectarse a una instancia en modo HA, consulte Conexión a una instancia de conjunto de réplicas para separación de lectura y escritura y alta disponibilidad.

Método 2: Uso de una EIP

Ejemplo de comando:

```
./mongo --host <DB_HOST> --port <DB_PORT> -u <DB_USER> -p --
authenticationDatabaseadmin --ssl --sslCAFile<FILE_PATH> --
sslAllowInvalidHostnames
```

Descripción de parámetros:

• **DB_HOST** es la EIP enlazada al nodo de instancia que se va a conectar.

En la página **Instances**, haga clic en la instancia para ir a la página **Basic Information**. Elija **Connections**> **Public Connection** y obtenga la EIP del nodo correspondiente.

• **DB_PORT** es el puerto de la base de datos. El número de puerto predeterminado es 8635.

Puede hacer clic en la instancia para ir a la página **Basic Information**. En el panel de navegación de la izquierda, elija **Connections**. En la página mostrada, haga clic en la pestaña **Public Connection** y obtenga el puerto del campo **Database Port** en el área **Basic Information**.

Figura 3-33 Obtención del puerto

Basic Information							
Database Port	8635	2		SSL			
Address							
Public Network	Connection Add	ress r a	nongodb://rv idmin 🗇	wuser: <password>6</password>	8635/test?authSource=		
Name/ID	AZ	Private I	EIP	Operation			
dds-ce25_mor 000e813fb557	ng az4	192.168		Change Private IP A	Address Unbind EIP		
dds-ce25_mor bad06d1cf259	ng az4	192.168		Change Private IP A	Address Bind EIP		

- **DB_USER** es el usuario de la base de datos. El valor predeterminado es **rwuser**.
- FILE PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: El certificado del conjunto de réplicas se genera utilizando la dirección IP de gestión interna para garantizar que la comunicación interna no ocupe recursos como la dirección IP del usuario y el ancho de banda. -sslAllowInvalidHostnames es necesario para la conexión SSL a través de una red pública.

Introduzca la contraseña de la cuenta de la base de datos cuando se le solicite:

Enter password:

Ejemplo de comandos:

./mongo --host *192.168.xx.xx* --port **8635** -u rwuser -p --authenticationDatabase admin -ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames

- Paso 9 Compruebe el resultado de la conexión. Si se muestra la siguiente información, la conexión se realiza correctamente.
 - El nodo principal del conjunto de réplicas está conectado. replica: PRIMARY>
 - El nodo en espera del conjunto de réplicas está conectado. replica: SECONDARY>

----Fin

Conexión sin encriptar

AVISO

Si se conecta a una instancia a través de una conexión no cifrada, deshabilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo deshabilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

- Paso 1 Inicie sesión en el ECS.
- Paso 2 Conéctese a una instancia DDS.

Método 1: Uso de una dirección de conexión de red pública

Ejemplo de comando:

./mongo "<Public network address>"

Public Network Connection Address: En la página **Instances**, haga clic en la instancia para cambiar a la página **Basic Information**. En el panel de navegación de la izquierda, elija **Connections**. Haga clic en la pestaña **Public Connection** y obtenga la dirección de conexión de red pública.

Figura 3-34 Obtención de la dirección de conexión de red pública

Basic Information								
Database Port	8635 🖉			SSL	•	▲		
Auto-switch Private IP Address								
Address								
Public Network Connection	on Address	mongo	db://rwuser:< <mark>passw</mark>	ord>@10.1	0 heidens	t?authSource=	admin 🗖 Lea	rn more
		Note	The parameters in	n orange are varia	ables and nee	ed to be modif	ied based on s	ervice req
		uireme	nts. For details, clic	k Learn more.				

El formato de la dirección de conexión pública es el siguiente. El nombre de usuario de la base de datos **rwuser** y la base de datos de autenticación **admin** no se pueden cambiar.

mongodb://rwuser:password>@192.168.xx.xx:8635/test?authSource=admin

Preste atención a los siguientes parámetros en la dirección de conexión pública:

Parámetro	Descripción
rwuser	Nombre de cuenta, es decir, el nombre de usuario de la base de datos.
<password></password>	Contraseña para la cuenta de la base de datos. Reemplácelo con la contraseña real.
	Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.
	Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25***%21%24 .
192.168.xx.xx:8635	La EIP y el puerto enlazados al nodo de la instancia del conjunto de réplicas.
authSource=admin	La base de datos de autenticación del usuario rwuser debe ser admin . authSource=admin está fijo en el comando.

Tabla 3-18 Descripción del parámetro

Ejemplo de comandos:

./mongo "mongodb://rwuser:password>@192.168.xx.xx:8635/test?authSource=admin"

D NOTA

- Si se conecta a una instancia a través de una dirección HA pública, agregue comillas dobles antes y
 después de la información de conexión.
- Para mejorar el rendimiento de lectura y escritura y evitar que se notifiquen errores cuando se escriben datos desde el cliente después de una conmutación principal/en espera, se recomienda conectarse a una instancia mediante la dirección de conexión HA. Para obtener más información, consulte Conexión a una instancia de conjunto de réplicas para separación de lectura y escritura y alta disponibilidad.

Método 2: Uso de una EIP

Ejemplo de comando:

./mongo --host <*DB_HOST*> --port <*DB_PORT*> -u <*DB_USER*> -p -authenticationDatabase admin

Descripción de parámetros:

• **DB_HOST** es la EIP enlazada al nodo de instancia que se va a conectar.

En la página **Instances**, haga clic en la instancia para ir a la página **Basic Information**. Elija **Connections**> **Public Connection** y obtenga la EIP del nodo correspondiente.

• **DB_PORT** es el puerto de la base de datos. El número de puerto predeterminado es 8635.

Puede hacer clic en la instancia para ir a la página **Basic Information**. En el panel de navegación de la izquierda, elija **Connections**. En la página mostrada, haga clic en la pestaña **Public Connection** y obtenga el puerto del campo **Database Port** en el área **Basic Information**.

Figura 3-35 Obtención del puerto

Basic Information								
Database Port	8635	2		SSL	 *			
Address								
Public Network Conne	ection Add	ress r	nongodb://rw	user: <password>@</password>	8635/test?authSource=			
		-	idmin 🗇					
Name/ID	AZ	Private I	EIP	Operation				
dds-ce25_mong 000e813fb5574c	az4	192.168		Change Private IP A	ddress Unbind EIP			
dds-ce25_mong bad06d1cf2594e	az4	192.168		Change Private IP A	ddress Bind EIP			

• **DB_USER** es el usuario de la base de datos. El valor predeterminado es **rwuser**.

Introduzca la contraseña de la cuenta de la base de datos cuando se le solicite:

Enter password:

Ejemplo de comandos:

./mongo --host 192.168.xx.xx --port 8635 -u rwuser -p --authenticationDatabase admin

- Paso 3 Compruebe el resultado de la conexión. Si se muestra la siguiente información, la conexión se realiza correctamente.
 - El nodo principal del conjunto de réplicas está conectado. replica: PRIMARY>
 - El nodo en espera del conjunto de réplicas está conectado. replica: SECONDARY>

----Fin

3.2.4.4 Conexión a una instancia de conjunto de réplicas mediante Robo 3T

Para conectarse a una instancia desde un dispositivo local, puede usar Robo 3T para acceder a la instancia desde Internet.

Esta sección describe cómo usar Robo 3T para conectarse a una instancia de clúster desde un dispositivo local. En esta sección, se utiliza como ejemplo el sistema operativo Windows utilizado por el cliente.

Robo 3T puede conectarse a una instancia con una conexión no cifrada o una conexión cifrada (SSL). Para mejorar la seguridad de la transmisión de datos, conéctese a instancias mediante SSL.

Diagrama de conexión



Figura 3-36 Diagrama de conexión

Prerrequisitos

- 1. Vincular una EIP al ECS y configurar las reglas de grupo de seguridad.
 - a. Vincule una EIP a la instancia del conjunto de réplicas.
 - Para obtener más información sobre cómo vincular una EIP, consulte Vinculación y desvinculación de una EIP.
 - b. Obtenga la dirección IP de un dispositivo local.
 - c. Configure reglas de grupo de seguridad.

Agregue la dirección IP obtenida en **1.b** y el puerto de instancia a la regla de entrada del grupo de seguridad.

Para obtener más información acerca de cómo configurar reglas de grupo de seguridad, consulte **Configuración de reglas de grupo de seguridad**.

- d. Ejecute el comando ping para hacer ping a la EIP enlazado en **1.**a para asegurarse de que la EIP es accesible a través de su dispositivo local.
- 2. Instalar Robo 3T.
 - a. Para obtener más información, consulte Instalación de Robo 3T.

SSL

AVISO

Si se conecta a una instancia a través de la conexión SSL, habilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo habilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

Paso 1 Ejecute el Robo 3T instalado. En el cuadro de diálogo mostrado, haga clic en Create.

Figura 3-37 Conexiones

!	A MongoDB Connections X					
C	<u>Create</u> , <u>edit</u> , <u>remove</u> , <u>clone</u> or	reorder connections via drag'n'	drop.			
	Name	Address	Attributes	Auth.	Database / User	
					📃 Connect 🛛 Car	ncel

- Paso 2 En el cuadro de diálogo Connection Settings, establezca los parámetros de la nueva conexión.
 - 1. En la pestaña **Connection**, escriba el nombre de la nueva conexión en el cuadro de texto **Name** e introduzca el puerto EIP y la base de datos enlazados a la instancia de base de datos DDS en el cuadro de texto **Name**.

Figura 3-38 Conexión

Connection Settings ×					
Connection	Authentication SSH TLS Advanced				
Туре:	Direct Connection	\sim			
Name:	test				
Address:	: 8635				
	Specify host and port of MongoDB server. Host can be either IPv4, IPv6 or domain name.	r			
From URI	Import connection details from MongoDB URI connection stri	ng			
<u>1</u> est	Save Can	cel			

2. En la pestaña Authentication, establezca Database en admin, User Name en rwuser y Password en la contraseña de administrador establecida durante la creación de la instancia de clúster.

Figura 3-39 Autenticación

Connection Se	ettings						×
Connection	Authentication	SSH	TLS	Advance	d		
🗹 Perform aut	hentication						
Database	admin						
	The admin data	base i 11	is unio 1.:_ 1	que in 1	MongoDB. U:	sers with ,	
User Name	rwuser						
Password	•••••					Ś	
Auth Mechanism	SCRAM-SHA-1					~	•
🗌 Manually specify visible databases							
i <u>T</u> est				E	Save	Cancel	

3. En la pestaña TLS, seleccione Use TLS protocol y seleccione Self-signed Certificate para Authentication Method.

Figura 3-40 SSL

📃 Connection Settings		×
Connection Authentic	cation SSH TLS Advanced	
🗹 Use TLS protocol		
Authentication Method:	Self-signed Certificate	\sim
	In general, avoid using self-signed certificates unless the network is trusted. If self-signed certificate is used, the communications channel will be encrypted however there will be no validation of server identity.	
🗌 Use PEM Cert./Key:	Enable this option to connect to a MongoDB that requires CA-signed client certificates/key file.	
Advanced Options		
<u>i</u> est	Save Cance	<u>1</u>

- 4. Haga clic en Save.
- Paso 3 En la página MongoDB Connections, haga clic en Connect para conectarse a la instancia del conjunto de réplicas.

Figura 3-41	Infor	nación	de	conexión	de	clúster
-------------	-------	--------	----	----------	----	---------

🛃 MongoDB Connections				×
<u>Create</u> , <u>edit</u> , <u>remove</u> , <u>clone</u> or	reorder connections via drag´n´	drop.		
Name	Address	Attributes	Auth. Database / User	
📃 test	:8635	TLS	🔎 admin / rwuser	
			Connect Cance	1

Paso 4 Si la instancia del conjunto de réplicas se conecta correctamente, se muestra la página mostrada en Figura 3-42.

Figura 3-42 Conexión correcta



----Fin

Conexión sin encriptar

AVISO

Si se conecta a una instancia a través de una conexión no cifrada, deshabilite SSL primero. De lo contrario, se notifica un error. Para obtener más información, consulte Habilitar y deshabilitar SSL.

Paso 1 Ejecute el Robo 3T instalado. En el cuadro de diálogo mostrado, haga clic en Create.

Figura 3-43 Conexiones

🛃 MongoDB Connections				×
Create, edit, remove, clone or	reorder connections via drag'n'	drop.		
Name	Address	Attributes A	uth. Database / User	
			📃 C <u>o</u> nnect Can	cel

Paso 2 En el cuadro de diálogo Connection Settings, establezca los parámetros de la nueva conexión.

1. En la pestaña **Connection**, escriba el nombre de la nueva conexión en el cuadro de texto **Name** e introduzca el puerto EIP y la base de datos enlazados a la instancia de base de datos DDS en el cuadro de texto **Name**.

Figura 3-44 Conexión

📃 Connection	Settings	×
Connection	Authentication SSH TLS Advanced	
Туре:	Direct Connection	\sim
Name:	test	
Address:	: 8635	
	Specify host and port of MongoDB server. Host can be either IPv4, IPv6 or domain name.	r
From URI	Import connection details from MongoDB URI connection stri	ng
<u>i</u> <u>I</u> est	Save Can	cel

2. En la pestaña Authentication, establezca Database en admin, User Name en rwuser y Password en la contraseña de administrador establecida durante la creación de la instancia de clúster.

Figura 3-45 Autenticación

Connection S	ettings	×					
Connection	Authentication SSH TLS Advanced						
Perform authentication							
Database	Database admin						
	The admin database is unique in MongoDB. Users with						
User Name	rwuser						
Password	<u>۱</u>						
Auth Mechanism	SCRAM-SHA-1 ~						
Manually specify visible databases							
1 <u>T</u> est	Save Cancel						

- 3. Haga clic en Save.
- Paso 3 En la página MongoDB Connections, haga clic en Connect para conectarse a la instancia del conjunto de réplicas.

Figura 3-46 Información de conexión de conjunto de réplicas

ġ	MongoDB Connections X									
ġ	<u>reate</u> ,	<u>edit</u> ,	<u>remove</u> ,	<u>clone</u> or	reorder con	nections via d	brag' n'	drop.		
	Name				Address			Attributes	Auth. Database / User	
	📃 te	st				:8635		TLS	🔎 admin / rwuser	
									Connect	Cancel

Paso 4 Si la instancia del conjunto de réplicas se conecta correctamente, se muestra la página mostrada en Figura 3-47.

Figura 3-47 Conexión correcta

• Robo 3T - 1.4 File View Options Winde 	ow Help	
 test (3) System admin 	 ♦ Welcome × ♦ db.getCollection('system'' × itest = 10.154.221.78:8635 admin 	🗣 db. getCollection(" system. *** 🗙
 Collections (4) System 	<pre>db.getCollection('system.roles').fin</pre>	d(∯)
> system.x > system.r > system.u > system.v	Fetched 0 record(s) in 88ms	
> Functions > Users > 🗐 local		
> 🗐 config		

----Fin

3.2.5 Conexión a una instancia de conjunto de réplicas mediante código de programa

3.2.5.1 Java

Si se está conectando a una instancia mediante Java, un certificado SSL es opcional, pero descargar un certificado SSL y cifrar la conexión mejorará la seguridad de su instancia. SSL está deshabilitado de forma predeterminada para instancias recién creadas, pero puede habilitar SSL haciendo referencia a **Habilitación o deshabilitación de SSL**. SSL cifra las conexiones a las bases de datos, pero aumenta el tiempo de respuesta de la conexión y el uso de la CPU. Por este motivo, no se recomienda habilitar SSL.

Prerrequisitos

Familiarícese con:

- Conceptos básicos de computadora
- Código Java

Obtención y uso de Java

- Descargue el controlador Jar desde: https://repo1.maven.org/maven2/org/mongodb/ mongo-java-driver/3.0.4/
- Para ver la guía de uso, visite https://mongodb.github.io/mongo-java-driver/4.2/ driver/getting-started/installation/.

Uso de un certificado SSL

NOTA

- Descargue el certificado SSL y verifique el certificado antes de conectarse a las bases de datos.
- En el área **DB Information** de la página **Basic Information**, haga clic en de en el campo **SSL** para descargar el certificado raíz o el paquete de certificados.
- Para obtener más información sobre cómo configurar una conexión SSL, consulte el documento oficial del controlador Java de MongoDB en https://www.mongodb.com/docs/drivers/java/sync/ current/fundamentals/connection/tls/#std-label-tls-ssl.

Utilice Java para conectarse al conjunto de réplicas. El formato del código Java es el siguiente:

```
mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>?
authSource=admin&replica&et=replica&ssl=true
```

Parámetro	Descripción
<username></username>	Nombre de usuario actual.
<password></password>	Contraseña para el nombre de usuario actual
<instance_ip></instance_ip>	Si intenta obtener acceso a la instancia desde un ECS, establezca <i>instance_ip</i> en la dirección IP privada que se muestra en la página Basic Information de la instancia a la que desea conectarse.
	Si tiene la intención de acceder a la instancia a través de una EIP, establezca <i>instance_ip</i> en la EIP que se ha enlazado a la instancia.

Tabla 3-19 Descripción del parámetro

Parámetro	Descripción	
<instance_port></instance_port>	Puerto de la base de datos que se muestra en la página Basic Information . Valor predeterminado: 8635	
<database_name></database_name>	Nombre de la base de datos que se va a conectar.	
authSource	Base de datos de usuarios de autenticación. El valor es admin.	
ssl	Modo de conexión. true indica que se utiliza el modo de conexión SSL.	

Utilice la herramienta keytool para configurar el certificado de CA. Para obtener más información sobre los parámetros, consulte **Tabla 3-20**.

```
keytool -importcert -trustcacerts -file <path to certificate authority file> -
keystore <path to trust store> -storepass <password>
```

 Tabla 3-20 Descripción del parámetro

Parámetro	Descripción
<pre><path authority="" certificate="" file="" to=""></path></pre>	Ruta para almacenar el certificado SSL.
<pre><path store="" to="" trust=""></path></pre>	Ruta para almacenar el truststore. Establezca este parámetro según sea necesario, por ejemplo, ./trust/ certs.keystore.
<pre><password></password></pre>	Contraseña personalizada.

Configure las propiedades del sistema JVM en el programa para que apunten al truststore y keystore correctos:

- System.setProperty("javax.net.ssl.trustStore","<path to trust store>");
- System.setProperty("javax.net.ssl.trustStorePassword","<password>");

Para obtener más información sobre el código Java, consulte el siguiente ejemplo:

```
public class Connector {
    public static void main(String[] args) {
        try {
            System.setProperty("javax.net.ssl.trustStore", "./trust/
certs.keystore");
            System.setProperty("javax.net.ssl.trustStorePassword",
"123456");
            ConnectionString connString = new
ConnectionString("mongodb://
<username>:<password>@<instance ip>:<instance port>/<database name>?
authSource=admin&replicaSet=replica&ssl=true");
           MongoClientSettings settings = MongoClientSettings.builder()
                    .applyConnectionString(connString)
                    .applyToSslSettings(builder -> builder.enabled(true))
                    .applyToSslSettings(builder ->
builder.invalidHostNameAllowed(true))
                    .build();
```

```
MongoClient mongoClient = MongoClients.create(settings);
MongoDatabase database = mongoClient.getDatabase("admin");
//Ping the database. If the operation fails, an exception
occurs.
BsonDocument command = new BsonDocument("ping", new
BsonInt64(1));
Document commandResult = database.runCommand(command);
System.out.println("Connect to database successfully");
} catch (Exception e) {
e.printStackTrace();
System.out.println("Test failed");
}
}
```

Conexión sin el certificado SSL

NOTA

No es necesario descargar el certificado SSL porque no se requiere la verificación del certificado en el servidor.

Conéctese a una instancia de conjunto de réplicas mediante Java. El formato de enlace Java es el siguiente:

mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>?
authSource=admin&replicaSet=replica

Parámetro	Descripción	
<username></username>	Nombre de usuario actual.	
<password></password>	Contraseña para el nombre de usuario actual	
<instance_ip></instance_ip>	Si intenta obtener acceso a la instancia desde un ECS, establezca <i>instance_ip</i> en la dirección IP privada que se muestra en la página Basic Information de la instancia a la que desea conectarse.	
	Si tiene la intención de acceder a la instancia a través de una EIP, establezca <i>instance_ip</i> en la EIP que se ha enlazado a la instancia.	
<instance_port></instance_port>	Puerto de la base de datos que se muestra en la página Basic Information . Valor predeterminado: 8635	
<database_name></database_name>	Nombre de la base de datos que se va a conectar.	
authSource	Base de datos de usuarios de autenticación. El valor es admin.	

Tabla 3-21 Descripción del parámetro

Para obtener más información sobre el código Java, consulte el siguiente ejemplo:

```
public class Connector {
    public static void main(String[] args) {
        try {
            ConnectionString connString = new
        ConnectionString("mongodb://
        <username>:<password>@<instance_ip>:<instance_port>/<database_name>?
        authSource=admin&replicaSet=replica");
    }
}
```

```
MongoClientSettings settings = MongoClientSettings.builder()
                    .applyConnectionString(connString)
                    .retryWrites(true)
                    .build();
            MongoClient mongoClient = MongoClients.create(settings);
            MongoDatabase database = mongoClient.getDatabase("admin");
            //Ping the database. If the operation fails, an exception
occurs.
            BsonDocument command = new BsonDocument("ping", new
BsonInt64(1));
            Document commandResult = database.runCommand(command);
            System.out.println("Connect to database successfully");
        } catch (Exception e) {
            e.printStackTrace();
            System.out.println("Test failed");
        }
```

3.2.5.2 Python

Esta sección describe cómo conectarse a una instancia de conjunto de réplicas usando Python.

Prerrequisitos

1. Para conectar un ECS a una instancia, el ECS debe poder comunicarse con la instancia DDS. Puede ejecutar el siguiente comando para conectarse a la dirección IP y el puerto del servidor de instancia para probar la conectividad de red.

curl ip:port

Si se muestra el mensaje It looks like you are trying to access MongoDB over HTTP on the native driver port, la conectividad de red es normal.

- 2. Instale Python y el paquete de instalación de terceros **pymongo** en el ECS. Se recomienda Pymongo 2.8.
- 3. Si SSL está habilitado, debe descargar el certificado raíz y subirlo al ECS.

Código de conexión

```
• Habilitación de SSL
```

```
import ssl
from pymongo import MongoClient
conn_urls="mongodb://rwuser:rwuserpassword@ip:port/{mydb}?
authSource=admin&replicaSet=replica"
connection = MongoClient(conn_urls,connectTimeoutMS=5000,ssl=True,
ssl_cert_reqs=ssl.CERT_REQUIRED,ssl_match_hostname=False,ssl_ca_certs
=${path to certificate authority file})
dbs = connection.database_names()
print "connect database success! database names is %s" % dbs
```

• Desactivación de SSL

```
import ssl
from pymongo import MongoClient
conn_urls="mongodb://rwuser:rwuserpassword@ip:port/{mydb}?
authSource=admin&replicaSet=replica"
connection = MongoClient(conn_urls,connectTimeoutMS=5000)
dbs = connection.database_names()
print "connect database success! database names is %s" % dbs
```

NOTA

- La base de datos de autenticación en la URL debe ser admin. Eso significa configurar authSource a admin.
- En el modo SSL, es necesario generar manualmente el archivo trustStore.
- La base de datos de autenticación debe ser **admin** y, a continuación, cambiar a la base de datos de servicio.

4 Tareas iniciales con nodos únicos

4.1 Compra de una instancia de nodo único

4.1.1 Quick Config

NOTA

Huawei Cloud has discontinued the sale of DDS single node instances since July 15, 2023.

This section describes how to purchase a single node instance on the management console. DDS helps you quickly configure and create a single node within several minutes.

Precautions

Each account can create up to 20 single nodes in total.

Prerrequisitos

- Ha registrado un ID de Huawei y ha habilitado servicios de Huawei Cloud.
- El saldo de su cuenta es mayor o igual a \$0 USD.
- Para mostrar si el disco está cifrado en la lista de instancias de base de datos, envíe un ticket de servicio. En la esquina superior derecha de la consola de gestión, elija Service Tickets > Create Service Ticket.

Procedure

Paso 1 Log in to the management console.

Paso 2 Click in the upper left corner and select a region and a project.

If you want compute and network resources dedicated to your exclusive use, **enable a DeC** and **apply for DCC resources**. After enabling a DeC, you can select the DeC region and project.

Paso 3 Click — in the upper left corner of the page and choose **Databases** > **Document Database Service**.

- **Paso 4** On the **Instances** page, click **Comprar instancias de base de datos**. The **Quick Config** page is displayed by default.
- Paso 5 Select a billing mode. Specify instance details and click Siguiente.

Figura 4-1 Basic configurations

Basic Information				
Billing Mode	Yearly/Monthly Pay-per-t	se.		
Region	CN North-Beijing4	*		
	Regions are geographic areas isolated from	each other. Resources are region-specific and canno	t be used across regions through internal network connectio	ons. For low network latency and quick resource access, select the nea
AZ	cn-north-4a cn-north-4b	cn-north-4c AZ7		
DB Instance Type (?)	Cluster Replica set	Single node		
	The availability (SLA) cannot be guaranteed because the instance is deployed on a single server.			
	DDS single node instance applies to R&D,	esting, and other non-enterprise core data storage so	cenarios. DDS supports one-click deployment, visualized O&	M, and elastic capacity expansion at a low price.
	Single nodes you can still create: 20. Incre	ise Quota		
Compatible MongoDB Version	4.4 Beta 4.2	4.0 3.4	View Version Details	
Specifications	General-purpose Enhance	d II		
Recommended Specifications				
	Recommendations	Recommendations	Recommendations	Custom
	2 vCPUs 8GB	2 vCPUs 4GB	4 vCPUs 8GB	1 vCPU 4GB *
	100 GB Ultra-high I/C	50 GB Ultra-high I/O	200 GB Ultra-high I/O	10 GB Ultra-high I/O
	Maximum Connections: 1000	Maximum Connections: 1000	Maximum Connections: 8000	Maximum Connections: 500
	Currantly selected _ dds monordb s6 Jama	Leinnia I 2 of Blic I 8/58		

Tabla 4-1 Billing mode

Parameter	Description
Billing Mode	Select a billing mode, Yearly/Monthly or Pay-per-use.
	• Yearly/Monthly
	 Specify Required Duration, and the system deducts the fees incurred from your account based on the service price.
	 If you do not expect to continue using the instance much after it expires, you can change the billing mode from yearly/monthly to pay-per-use. For details, see Changing the Billing Mode from Yearly/Monthly to Pay-per-Use.
	NOTA Instances billed on a yearly/monthly basis cannot be deleted. They can only be unsubscribed from. For details, see Unsubscribing from a Yearly/Monthly Instance.
	• Pay-per-use
	 You are billed for usage based on how much time the service is in use.
	 If you expect to use the service extensively over a long period of time, you can change its billing mode from pay-per-use to yearly/monthly to reduce costs. For details, see Changing the Billing Mode from Pay-per-Use to Yearly/Monthly.
Region	The region where the resource is located.
	NOTA Instances deployed in different regions cannot communicate with each other through a private network, and you cannot change the region of an instance once it is purchased. Exercise caution when selecting a region.

Parameter	Description
AZ	An AZ is a part of a region with its own independent power supply and network. AZs are physically isolated but can communicate through internal network connections.
DB Instance	Select Single Node.
Туре	The single node architecture is another option for you, helping you reduce costs while ensuring data reliability.
Compatible	• 4.4
MongoDB Version	• 4.2
verbion	• 4.0
	• 3.4
СРИ Туре	DDS supports x86 and Kunpeng CPU architectures.
	 x86 x86 CPUs use the Complex Instruction Set Computing (CISC) instruction set. Each instruction can be used to execute low-level hardware operations. CISC instructions vary in length, and tend to be complicated and slow compared to Reduced Instruction Set Computing (RISC).
	• Kunpeng The Kunpeng CPU architecture uses RISC. The RISC instruction set is smaller and faster than CISC, thanks to the simplified architecture. Kunpeng CPUs also offer a better balance between power and performance than x86.
	Kunpeng CPUs offer a high density, low power option that is more cost effective for heavy workloads.
Specifications	With an x86 architecture, you have the following options:
	• General-purpose (s6): S6 instances are suitable for applications that require moderate performance generally but occasional bursts of high performance, such as light-workload web servers, enterprise R&D and testing environments, and low- and medium-performance databases.
	• Enhanced II (c6): C6 instances have multiple technologies optimized to provide stable powerful compute performance. 25 GE intelligent high-speed NICs are used to provide ultra-high bandwidth and throughput, making it an excellent choice for heavy- load scenarios. It is suitable for websites, web applications, general databases, and cache servers that have higher performance requirements for compute and network resources; and medium- and heavy-load enterprise applications.
Recommended Specifications	Currently, recommended and customized specifications are provided.

Figura 4-2 Network, Required Duration, and Quantity

Tabla 4-2 Network settings

Parameter	Description
VPC	The VPC where your DB instances are located. A VPC isolates networks for different services. It allows you to easily manage and configure private networks and change network configurations.
	You need to create or select the required VPC. For details, see Creating a VPC in the <i>Virtual Private Cloud User Guide</i> . For details about the constraints on the use of VPCs, see Métodos de conexión .
	If there are no VPCs available, DDS creates one for you by default.
	NOTA After the DDS instance is created, the VPC cannot be changed.
Enterprise Project	Only enterprise users can use this function. To use this function, contact customer service.
	An enterprise project is a cloud resource management mode, in which cloud resources and members are centrally managed by project.
	Select an enterprise project from the drop-down list. The default project is default .
	To customize an enterprise project, click Enterprise in the upper right corner of the console. The Enterprise Management page is displayed. For details, see Creating an Enterprise Project in <i>Enterprise</i> <i>Management User Guide</i> .

|--|

Parameter	Description
Required Duration	The system will automatically calculate the fee based on the validity period you have selected.
Auto-renew	 By default, this option is not selected. If you select this option, the auto-renew cycle is determined by the length of the subscription.

Parameter	Description
Quantity	The purchase quantity depends on the single node instance quota. If your current quota does not allow you to purchase the required number of instances, you can apply for an increased quota. Yearly/Monthly instances that were purchased in batches have the same specifications except for the instance name and ID.

Tabla 4-4 Default configuration items

Specifications	Value	Editable After Instance Creation
DB Instance Name	dds-d168	Yes
СРИ Туре	x86	No
Storage Engine	WiredTiger	No
Password Settings	Not configured	Yes
SSL	Disabled	Yes
Database Port	8635	Yes
Single Node Parameter Template	Default-DDS-4.0-Single	Yes
Tags	Not configured	Yes
Advanced Settings	Not configured	Yes

- Some settings are configured by default during purchase, but can still be modified after the instance is created. If you do not see a setting listed for your instance, click **Custom Config**.
- Instance performance depends on the specifications you select during creation. The hardware configuration items that can be selected include the node class and storage space.

Paso 6 On the displayed page, confirm the instance details.

- Yearly/Monthly
 - If you need to modify the specifications, click **Previous** to return to the previous page.
 - If you do not need to modify the specifications, read and agree to the service agreement and click **Pay Now** to go to the payment page and complete the payment.
- Pay-per-use
 - If you need to modify the specifications, click **Previous** to return to the previous page.
 - If you do not need to modify the specifications, read and agree to the service agreement and click Submit to start creating the instance.

Paso 7 After a DDS instance is created, you can view and manage it on the Instances page.

- When an instance is being created, the status displayed in the **Status** column is **Creating**. This process takes about 15 minutes. After the creation is complete, the status changes to **Available**.
- DDS enables the automated backup policy by default. After an instance is created, you can modify or disable the automated backup policy. An automated full backup is immediately triggered after the creation of an instance.
- Yearly/Monthly instances that were purchased in batches have the same specifications except for the instance name and ID.

----Fin

4.1.2 Custom Config

NOTA

Huawei Cloud has discontinued the sale of DDS single node instances since July 15, 2023.

This section describes how to purchase a single node instance in custom mode on the management console. You can customize the computing resources and storage space of a single node instance based on your service requirements. In addition, you can configure advanced settings, such as slow query log and automated backup.

Precautions

Each account can create up to 20 single node instances.

Prerequisites

• You have registered a Huawei ID and enabled Huawei Cloud services.

Procedure

Paso 1 Log in to the management console.

Paso 2 Click in the upper left corner and select a region and a project.

If you want compute and network resources dedicated to your exclusive use, **enable a DeC** and **apply for DCC resources**. After enabling a DeC, you can select the DeC region and project.

- **Paso 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- Paso 4 On the Instances page, click Comprar instancias de base de datos.
- Paso 5 Click the Custom Config tab.
- Paso 6 Select a billing mode. Specify instance details and click Siguiente.

Basic Information		
Billing Mode	Yearly/Monthly Pay-per-use	
Region	CN North-Beijing4 ·	
	Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network	connections. For low network latency and quick resource access, select the nearest region.
AZ	cn-north-4a cn-north-4b cn-north-4c AZ7	
DB Instance Name	dds-9092	
DB Instance Type (?)	Cluster Replica set Single node	
	The availability (SLA) cannot be guaranteed because the instance is deployed on a single server.	
	DDS single node instance applies to R&D, testing, and other non-enterprise core data storage scenarios. DDS supports one-click deployment, visua	slized O&M, and elastic capacity expansion at a low price.
	Single nodes you can still create: 20. Increase Quota	
Compatible MongoDB Version	4.4 4.2 4.0 3.4 View Version Details	
Storage Type	Ultra-high I/O	
Storage Engine	RocksDB	
Specifications	General-purpose Enhanced II	
Node Class	vCPU Memory	Maximum Connections
	1 vCPU 4 GB	500
	2 vCPUs 4 GB	1000
	2 vCPUs 8 GB	1000
	○ 4 vCPUs 8 GB	8000
	○ 4 vCPUs 16 G8	8000
	0 8 vCPUs 16 G8	10000
	O 8 vCPUs 32 G8	10000
	Currently selected dds.mongodb.s6.medium.4.single 1 vCPU 4 GB	
	10 GB	
Storage Space		
	10 500 1000 1500 2000 2500 3000 3500 4000 4500 5000	10 + GB 💮
	To ensure that the DB instance can still be used if the storage space is about to be used up, the database is set to read-only, and data cannot be n	modified. If this happens, you can add more storage to restore the database to read/write status
Disk Farmation	Disabled Faabled	

Figura 4-3 Basic configurations

Tabla 4-5 Billing mode

Parameter	Description	
Billing Mode	Select a billing mode, Yearly/Monthly or Pay-per-use.	
	• Yearly/Monthly	
	 Specify Required Duration, and the system deducts the fees incurred from your account based on the service price. 	
	 If you do not expect to continue using the instance much after it expires, you can change the billing mode from yearly/monthly to pay-per-use. For details, see Changing the Billing Mode from Yearly/Monthly to Pay-per-Use 	
	NOTA Instances billed on a yearly/monthly basis cannot be deleted. They can only be unsubscribed from. For details, see Unsubscribing from a Yearly/Monthly Instance .	
	• Pay-per-use	
	 You are billed for usage based on how much time the service is in use. 	
	 If you expect to use the service extensively over a long period of time, you can change its billing mode from pay-per-use to yearly/monthly to reduce costs. For details, see Changing the Billing Mode from Pay-per-Use to Yearly/Monthly 	

Parameter	Description
Region	The region where the resource is located. NOTA Instances deployed in different regions cannot communicate with each other through a private network, and you cannot change the region of an instance once it is purchased. Exercise caution when selecting a region.
AZ	An AZ is a part of a region with its own independent power supply and network. AZs are physically isolated but can communicate through internal network connections.
DB Instance Name	 The instance name can be the same as an existing instance name. The instance name that you specify after the purchase. The instance name must contain 4 to 64 characters and must start with a letter. It is case sensitive and can contain letters, digits, hyphens (-), and underscores (_). It cannot contain other special characters.
	• If you buy a batch of instances at once, a 4-digit numerical suffix will be added to the instance names, starting with -0001. If you later make another batch purchase, the new instance names will be numbered first using any suffixes missing from the sequence of your existing instances, and then continuing on from where your last batch purchase left off. For example, a batch of 3 instances get the suffixes -0001, -0002, and -0003. If you deleted instance 0002 and then bought 3 more instances, the new instances would get the suffixes -0002, -0004, and -0005.
	• After the DB instance is created, you can change its name. For details, see Changing an Instance Name.
DB Instance Type	Select Single Node . The single node architecture is another option for you, helping you reduce costs while ensuring data reliability.
Compatible MongoDB Version	 4.4 4.2 4.0 3.4

Parameter	Description
CPU Type	 DDS supports x86 and Kunpeng CPU architectures. x86 x86 CPUs use the Complex Instruction Set Computing (CISC) instruction set. Each instruction can be used to execute low-level hardware operations. CISC instructions vary in length, and tend to be complicated and slow compared to Reduced Instruction Set Computing (RISC). Kunpeng The Kunpeng CPU architecture uses RISC. The RISC instruction set is smaller and faster than CISC, thanks to the simplified architecture. Kunpeng CPUs also offer a better balance between power and performance than x86. Kunpeng CPUs offer a high density, low power option that is more
Storege Tripe	Cost effective for heavy workloads.
Storage Engine	 WiredTiger WiredTiger is the default storage engine of DDS 3.4 and 4.0. WiredTiger provides different granularity concurrency control and compression mechanism for data management. It can provide the best performance and storage efficiency for different kinds of applications. RocksDB RocksDB RocksDB is the default storage engine of DDS 4.2. RocksDB supports efficient point lookup, range scan, and high-speed write. RocksDB can be used as the underlying data storage engine of MongoDB and is suitable for scenarios with a large number of write operations.
Specifications	 With an x86 architecture, you have the following options: General-purpose (s6): S6 instances are suitable for applications that require moderate performance generally but occasional bursts of high performance, such as light-workload web servers, enterprise R&D and testing environments, and low- and medium-performance databases. Enhanced II (c6): C6 instances have multiple technologies optimized to provide stable powerful compute performance. 25 GE intelligent high-speed NICs are used to provide ultra-high bandwidth and throughput, making it an excellent choice for heavy-load scenarios. It is suitable for websites, web applications, general databases, and cache servers that have higher performance requirements for compute and network resources; and medium- and heavy-load enterprise applications.
Node Class	For details about the instance specifications, see Instance Specifications .

Parameter	Description
Storage Space	Value range: 10 GB to 1,000 GB (must be a multiple of 10)
	You can scale up an instance after it is created. For details, see Scaling Up a Single Node Instance.
	ΝΟΤΑ
	• If the storage space you purchased exceeds 600 GB and the remaining storage space is 18 GB, the instance becomes Read-only .
	• If the storage space you purchased is less than 600 GB and the storage space usage reaches 97%, the instance becomes Read-only .
	In these cases, delete unnecessary resources or expand the capacity.
Disk Encryption	• Disabled : Disable encryption.
	• Enabled: Enable encryption. This feature improves data security but slightly affects read/write performance. Key Name: Select or create a private key, which is the tenant key. NOTA
	• After an instance is created, the disk encryption status and the key cannot be changed. Disk encryption will not encrypt backup data stored in OBS. To enable backup data encryption, contact customer service.
	 If disk encryption or backup data encryption is enabled, keep the key properly. Once the key is disabled, deleted, or frozen, the database will be unavailable and data may not be restored. If disk encryption is enabled but backup data encryption is not enabled, you can restore data to a new instance from backups.
	If both disk encryption and backup data encryption are enabled, data cannot be restored.
	• For details about how to create a key, see "Creating a CMK" in <i>Data Encryption Workshop User Guide</i> .

Figura 4-4 Administrator settings

Administrator				
Password	Configure	Skip		
Administrator	rwuser			
Administrator Password			Q	Keep your password secure. The system cannot retrieve your password.
Confirm Password			40	

Parameter	Description	
Password	• Configure Enter and confirm the new administrator password. After an instance is created, you can connect to the instance using the password.	
	• Skip To log in, you will have to reset the password later on the Basic Information page. If you need to connect to an instance after it is created, locate the instance and click Reset Password in the Operation column to set a password for the instance first.	
Administrator	The default account is rwuser .	
Administrator Password	Set a password for the administrator. The password must be 8 to 32 characters in length and contain uppercase letters, lowercase letters, digits, and at least one of the following special characters: ~!@#%^*= +? Keep this password secure. If lost, the system cannot retrieve it for you.	
Confirm Password	Enter the administrator password again.	

 Tabla 4-6 Administrator settings

Figura 4-5 Network, Required Duration, and Quantity

Network	
VPC	default_vpc + C View VPC
	▲ After the DDS instance is created, the VPC cannot be changed.
Subnet	default_subnet(192.168.0.0/24)
	Available private IP addresses in the subnet: 227
Security Group	Sys-default(b6f16cee-e859-47e2-a418 • C View Security Group
	In a security group, rules that authorize connections to DB instances apply to all DB instances associated with the security group.
SSL	View Details (2)
	To encrypt transmission, enable SSL
Database Port	Default port: 8635
Enterprise Project	
Enterprise Project	Select C View Project Management (2)

Tabla 4-7 Network

Parameter	Description
VPC	The VPC where your DB instances are located. A VPC isolates networks for different services. It allows you to easily manage and configure private networks and change network configurations.
	You will need to create or select the required VPC. For details about how to create a VPC, see "Creating a VPC" in <i>Virtual Private Cloud User Guide</i> . For details about the constraints on the use of VPCs, see Métodos de conexión.
	If there are no VPCs available, DDS creates one for you by default. NOTA After the DDS instance is created, the VPC cannot be changed.
Subnet	A subnet provides dedicated network resources that are logically isolated from other networks for security reasons.
	After the instance is created, you can change the private IP address assigned by the subnet. For details, see Changing a Private IP Address . NOTA IPv6 subnets are not supported. You are advised to create and select IPv4 subnets.
Security	A security group controls access between DDS and other services.
Group	If there are no security groups available, DDS creates one for you by default.
	Ensure that there is a security group rule configured that allows clients to access instances. For example, select an inbound TCP rule with the default port 8635, and enter a subnet IP address or select a security group that the instance belongs to.
SSL	Secure Sockets Layer (SSL) encrypts connections between clients and servers, preventing data from being tampered with or stolen during transmission.
	You can enable SSL to improve data security. After an instance is created, you can connect to it using SSL.
Database Port	The default DDS port is 8635, but this port can be modified if necessary. If you change the port, add a corresponding security group rule to allow access to the instance.
Enterprise Project	Only enterprise users can use this function. To use this function, contact customer service.
	An enterprise project is a cloud resource management mode, in which cloud resources and members are centrally managed by project.
	Select an enterprise project from the drop-down list. The default project is default .

Figura 4-6 Advanced settings

Advanced Settings		
Single Node Parameter Template	Default-DDS-4.2-Single 🔻	C View Parameter Template
Automated Backup	0	
Retention Period	- 7 + Enter an integer from 1 to 732.	
Time Window	00:00 - 01:00 *	GMT+08:00
Maintenance Window	Skip Configure	
Tags	It is recommended that you use TMS's predefined tag function to	add the same tags to different cloud resources, $C\ \ View \ predefined \ tags$
	Tag key Tag value	
	You can add 20 more tags.	

Tabla 4-8 Advanced settings

Parameter	Description	
Single Node Parameter Template	The parameters that apply to single node instances. After an instance is created, you can change the parameter template you configured for the instance to bring out the best performance.	
	Tor details, see Editing a Faranteer Template.	
Automated Backup	DDS enables an automated backup policy by default, but you can disable it after an instance is created. An automated full backup is immediately triggered after the creation of an instance. For details, see Configuring an Automated Backup Policy .	
Retention Period (days)	Retention Period refers to the number of days that data is kept. You can increase the retention period to improve data reliability. The backup retention period is from 1 to 732 days.	
Time Window	The backup interval is 1 hour.	

Parameter	Description	
Maintenance Window	 A maintenance period refers to the period during which a user is allowed to start a task that affects the running of a database instance, for example, an OS upgrade or database software upgrade. Skip Skip The maintenance window is 02:00–06:00 by default and you can change it as required. For details, see Configuring the Maintenance Window. Configure You are advised to set the maintenance period to off-peak hours to prevent service interruption during maintenance. You can change the maintenance window after an instance is created. For details, see Configuring the Maintenance Window. Figura 4-7 Configuring the maintenance window 	
	Interval 1h 2h 3h 4h ▲ Changing the maintenance window will not affect the execution of scheduled tasks in the original maintenance window.	
	Maintenance Window 02:00 - 06:00 • 02:00 - 06:00 • • 06:00 - 10:00 • • 10:00 - 14:00 • • 14:00 - 18:00 • •	

Parameter	Description
Tags	(Optional) You can add tags to DDS instances so that you can quickly search for and filter specified instances by tag. Each DDS instance can have up to 20 tags.
	• Create a tag. You can create tags on the DDS console and configure the tag key and value .
	Key: This parameter is mandatory.
	 Each tag key must be unique for each instance.
	 A tag key consists of up to 36 characters.
	 The key can only consist of digits, letters, underscores (_), and hyphens (-).
	Value: This parameter is optional.
	 The value consists of up to 43 characters.
	 The value must consist of only digits, letters, underscores (_), periods (.), and hyphens (-).
	• Add a predefined tag. Predefined tags can be used to identify multiple cloud resources.
	To tag a cloud resource, you can select a created predefined tag from the drop-down list, without entering a key and value for the tag.
	For example, if a predefined tag has been created, its key is Usage and value is Project1. When you configure the key and value for a cloud resource, the created predefined tag will be displayed on the page.
	After an instance is created, you can click the instance name to view its tags. On the Tags page, you can also modify or delete the tags . In addition, you can quickly search for and filter specified instances by tag .
	You can add a tag to an instance after the instance is created. For details, see Adding a Tag.

If you have any question about the price, click Price Details.

NOTA

Instance performance depends on the specifications you select during creation. The hardware configuration items that can be selected include the node class and storage space.

Paso 7 On the displayed page, confirm the instance details.

- Yearly/Monthly
 - If you need to modify the specifications, click **Previous** to return to the previous page.
 - If you do not need to modify the specifications, read and agree to the service agreement and click **Pay Now** to go to the payment page and complete payment.
- Pay-per-use
- If you need to modify the specifications, click **Previous** to return to the previous page.
- If you do not need to modify the specifications, read and agree to the service agreement and click **Submit** to start creating the instance.

Paso 8 After a DDS instance is created, you can view and manage it on the Instances page.

- When an instance is being created, the status displayed in the **Status** column is **Creating**. This process takes about 15 minutes. After the creation is complete, the status changes to **Available**.
- Yearly/Monthly instances that were purchased in batches have the same specifications except for the instance name and ID.

----Fin

4.2 Conexión a una instancia de nodo único

4.2.1 Métodos de conexión

Puede acceder a DDS a través de redes privadas o públicas.

Tabla 4-9 Métodos de conexión

Métod o	Direcció n IP	Escenario	Descripción
DAS	No requerido	DAS proporciona una GUI y le permite realizar operaciones visualizadas en la consola. La ejecución SQL, la gestión avanzada de bases de datos y la operación inteligente están disponibles para hacer que la gestión de bases de datos sea simple, segura e inteligente.	 Fácil de usar, seguro, avanzado e inteligente Recomendada
Red privada	Dirección IP privada	DDS proporciona una dirección IP privada de forma predeterminada. Si sus aplicaciones se ejecutan en un ECS en la misma subred de región, zona de disponibilidad y VPC que su instancia DDS, se recomienda utilizar una dirección IP privada para conectar el ECS a sus instancias DDS.	Rendimiento seguro y excelente

Métod o	Direcció n IP	Escenario	Descripción
Red pública	EIP	 Si sus aplicaciones se ejecutan en un ECS que se encuentra en una región diferente de la donde se encuentra la instancia de base de datos, utilice una EIP para conectar el ECS a las instancias de base de datos de DDS. Si sus aplicaciones se despliegan en otra plataforma en la nube, se recomienda EIP. 	 Bajo nivel de seguridad Para una transmisión más rápida y una seguridad mejorada, se recomienda migrar sus aplicaciones a un ECS que esté en la misma subred que su instancia de DDS y utilizar una dirección IP privada para acceder a la instancia.

4.2.2 (Recomendado) Conexión a una instancia de nodo único mediante DAS

4.2.2.1 Descripción

DAS proporciona una GUI y le permite realizar operaciones visualizadas en la consola. La ejecución SQL, la gestión avanzada de bases de datos y la operación inteligente están disponibles para hacer que la gestión de bases de datos sea simple, segura e inteligente. Se recomienda utilizar DAS para conectarse a instancias de base de datos.

Esta sección describe cómo conectarse a una instancia de nodo único a través de DAS.

Proceso

Para conectarse a una instancia de nodo único, realice los siguientes pasos:

1. Conéctese a una instancia de nodo único a través de DAS.

4.2.2.2 Conexión a una instancia de nodo único mediante DAS

Data Admin Service (DAS) le permite gestionar instancias de bases de datos en una consola basada en web, simplificando la gestión de bases de datos y mejorando la eficiencia del trabajo. Puede conectar y gestionar instancias a través de DAS. De forma predeterminada, tiene el permiso necesario para el inicio de sesión remoto. Se recomienda utilizar el servicio DAS para conectarse a instancias. DAS es seguro y conveniente.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic ^(Q) en la esquina superior izquierda y seleccione una región y un proyecto.

Si desea recursos informáticos y de red dedicados a su uso exclusivo, **habilite un DeC** y **solicite recursos de DCC**. Después de habilitar un DeC, puede seleccionar la región y el proyecto de DeC.

- **Paso 3** Haga clic = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.
- Paso 4 En la página Instances, busque la instancia de base de datos de destino y haga clic en Log In en la columna Operation.

También puede hacer clic en la instancia de base de datos de destino en la página **Instances**. En la página **Basic Information** mostrada, haga clic en **Log In** en la esquina superior derecha de la página.

Figura 4-8 Gestión de instancias

Renew Change to Yearly/Monthly			All DB	intances 💌 Enter a D	B instance name, a DB instanc	e ID, or an address.	Q Search by Tag 😸 C
Name/ID J≡	DB Instance Type	DB Engine Version	Status ↓Ξ	Billing Mode	Address	Operation	
dds-ca62 e5b9940b12ad464a9dce63ed38a8c875in02	Single node	Community Edition 4.0	 Available 	Pay-per-use Created on Jan 20, 2020	mongodb://rwuser.****	Log In View Metric More	•

Paso 5 En la página de inicio de sesión mostrada, introduzca el nombre de usuario y la contraseña del administrador y haga clic en **Login**.

Para obtener más información acerca de cómo gestionar bases de datos a través de DAS, consulte **Gestión de instancias de DDS**.

----Fin

4.2.3 Conexión a una instancia de nodo único a través de una red privada

4.2.3.1 Configuración de un grupo de seguridad

Un grupo de seguridad es un grupo lógico. Proporciona políticas de control de acceso para los ECS y las instancias que tienen los mismos requisitos de protección de seguridad y son de confianza mutua en una VPC.

Para garantizar la seguridad y confiabilidad de la base de datos, debe configurar reglas de grupo de seguridad para permitir que las direcciones IP y los puertos específicos accedan a instancias de DDS.

Puede conectarse a una instancia mediante la configuración de las reglas de grupo de seguridad de las dos maneras siguientes:

 Si el ECS y la instancia están en el mismo grupo de seguridad, pueden comunicarse entre sí de forma predeterminada. No es necesario configurar ninguna regla de grupo de seguridad. Vaya a Conexión a una instancia de nodo único mediante Mongo Shell (red privada).

Figura 4-9 Mismo grupo de seguridad



• Si el ECS y la instancia están en diferentes grupos de seguridad, debe configurar las reglas de grupo de seguridad para ellos, por separado.





- Instancia: configura una inbound rule para el grupo de seguridad asociado a la instancia.
- ECS: La regla de grupo de seguridad predeterminada permite todos los paquetes de datos salientes. En este caso, no es necesario configurar una regla de grupo de seguridad para el ECS. Si no se permite que todo el tráfico llegue a la instancia, configure una regla de **outbound** para el ECS.

Esta sección describe cómo configurar una regla de entrada para una instancia.

Precauciones

- De forma predeterminada, una cuenta puede crear hasta 500 reglas de grupo de seguridad.
- Demasiadas reglas de grupo de seguridad aumentarán la latencia del primer paquete, por lo que se recomienda un máximo de 50 reglas para cada grupo de seguridad.
- Una instancia DDS solo puede asociarse a un grupo de seguridad.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

- **Paso 2** Haga clic en 🔍 en la esquina superior izquierda, y seleccione una región y un proyecto.
- Paso 3 Haga clic en = en la esquina superior izquierda de la página y elija Databases > Document Database Service.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia. Se muestra la página Basic Information.
- **Paso 5** En el área **Network Information** de la página **Basic Information**, haga clic en el grupo de seguridad.

Figura 4-11 Grupo de seguridad

Network Information			
VPC	dds-st-test-vpc	Subnet	dds-st-test-subnet-2 (1)
Security Group	Sys-default 🖉	Database Port	8635 🖉

También puede elegir **Connections** en el panel de navegación de la izquierda. En la pestaña **Private Connection**, en el área **Security Group**, haga clic en el nombre del grupo de seguridad.

Figura 4-12 Grupo de seguridad

Security Group		
Security Group Sys-default 🖉		
Add Rule Delete		С
Inbound Rules(1) Outbound Rules	(1)	
Protocol & Port ⑦	Source ⑦	Description
All	Sys-default	-

- Paso 6 En la página Security Group, busque el grupo de seguridad de destino y haga clic en Manage Rule en la columna Operation.
- Paso 7 En la pestaña Inbound Rules, haga clic en Add Rule. Aparece el cuadro de diálogo Add Inbound Rule.
- Paso 8 Agregue una regla de grupo de seguridad como se le solicite.

Figura 4-13 Agregar regla de entrada

Add Inbound Rule Learn n	nore about security group of	configuration.			X
1 Inbound rules allow incoming tr	affic to instances associated wit	h the security group.			
Security Group Sys-default You can import multiple rules in a batch	L				
Protocol & Port ⑦	Туре	Source	Description	Operation	
TCP Example: 22 or 22-30	IPv4 v	IP address 0.0.0.0/0	• · · · · · · · · · · · · · · · · · · ·	Operation 🗸	
		🕀 Add Rule			
		OK Cancel			

Tabla 4-10 Configuración de reglas entrantes

Parámetro	Descripción	Ejemplo
Priority	Prioridad de regla de grupo de seguridad. El valor de prioridad varía de 1 a 100. La prioridad predeterminada es 1 y tiene la prioridad más alta. La regla de grupo de seguridad con un valor menor tiene mayor	1
Action	Las acciones de la regla del grupo de seguridad. Una regla con una acción de denegación invalida a otra con una acción de permiso si las dos reglas tienen la misma prioridad.	Allow
Protocol & Port	El protocolo de red requerido para el acceso. Opciones disponibles: TCP, UDP, ICMP, o GRE	ТСР
	Puerto: el puerto en el que desea permitir el acceso a DDS. El puerto predeterminado es 8635. El puerto oscila entre 2100 y 9500 o puede ser 27017, 27018, o 27019.	8635
Туре	Tipo de dirección IP. Solo IPv4 y IPv6 son compatibles.	IPv4

Parámetro	Descripción	Ejemplo
Source	Especifica la dirección IP, el grupo de seguridad y el grupo de direcciones IP compatibles, que permiten el acceso desde direcciones IP o instancias de otro grupo de seguridad. Ejemplo:	0.0.0/0
	• Dirección IP única: 192.168.10.10/32	
	 Segmento de dirección IP: 192.168.1.0/24 	
	• Todas las direcciones IP: 0.0.0.0/0	
	• Grupo de seguridad: sg-abc	
	• Grupo de direcciones IP: ipGroup-test	
	Si introduce un grupo de seguridad, todos los ECS asociados al grupo de seguridad cumplen con la regla creada.	
	Para obtener más información acerca de los grupos de direcciones IP, consulte Grupo de direcciones IP .	
Description	(Opcional) Proporciona información adicional acerca de la regla del grupo de seguridad. Este parámetro es opcional.	-
	La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	

Paso 9 Haga clic en OK.

----Fin

4.2.3.2 Conexión a una instancia de nodo único mediante Mongo Shell (red privada)

Mongo shell es el cliente por defecto para el servidor de base de datos MongoDB. Puede utilizar Mongo Shell para conectarse a instancias de base de datos y consultar, actualizar y gestionar datos en bases de datos. Para usar Mongo Shell, descargue e instale primero el cliente MongoDB y, a continuación, use el shell Mongo para conectarse a la instancia de base de datos.

De forma predeterminada, una instancia DDS proporciona una dirección IP privada. Si sus aplicaciones se despliegan en un ECS y están en la misma región y VPC que las instancias DDS, puede conectarse a las instancias DDS mediante una dirección IP privada para lograr una velocidad de transmisión rápida y una alta seguridad.

Esta sección describe cómo utilizar Mongo Shell instalado en un ECS de Linux para conectarse a una instancia de nodo único a través de una red privada.

Puede conectarse a una instancia mediante una conexión SSL o una conexión sin cifrar. La conexión SSL es encriptada y más segura. Para mejorar la seguridad de la transmisión de datos, conéctese a instancias mediante SSL.

Prerrequisitos

- 1. Para obtener más información acerca de cómo crear e iniciar sesión en un ECS, consulte Comprar un ECS e iniciar sesión en un ECS.
- 2. Instale el cliente MongoDB en el ECS.

Para obtener más información sobre cómo instalar un cliente MongoDB, consulte ¿Cómo puedo instalar un cliente MongoDB?

3. El ECS puede comunicarse con la instancia DDS. Para obtener más información, véase ECS.

SSL

AVISO

Si se conecta a una instancia a través de la conexión SSL, habilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo habilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

Paso 1 Inicie sesión en la consola de gestión.

- Paso 2 Haga clic en 💿 en la esquina superior izquierda, y seleccione una región y un proyecto.
- Paso 3 Haga clic en = en la esquina superior izquierda de la página y elija Databases > Document Database Service.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia.
- Paso 5 En el panel de navegación de la izquierda, elija Connections.
- Paso 6 En el área Basic Information, haga clic en 📥 junto al campo SSL.
- Paso 7 Importar el certificado raíz al Linux o Windows ECS. Para obtener más información, consulte ¿Cómo puedo importar el certificado raíz a un sistema operativo Windows o Linux?
- Paso 8 Conéctese a una instancia DDS.

Uso de una dirección IP privada

Ejemplo de comando:

```
./mongo --host <DB_HOST> --port <DB_PORT> -u <DB_USER> -p --
authenticationDatabase admin --ssl --sslCAFile<FILE_PATH> --
sslAllowInvalidHostnames
```

Descripción de parámetros:

• DB_HOST es la dirección IP privada de la instancia que se va a conectar.

En la página **Instances**, haga clic en el nombre de la instancia. Se muestra la página **Basic Information**. Elija **Connections**. En la pestaña **Private Connection**, obtenga la dirección IP del nodo correspondiente.

Node Information					
Name/ID	Status	AZ	Private IP Address	EIP	Operation
dds_single_40_single_node_1 35e189a27e874a93bb9718	ə Available	az4			View Metric Change Private IP Address Unbind EIP

• **DB_PORT** es el puerto de la base de datos. El número de puerto predeterminado es 8635.

Puede hacer clic en el nombre de la instancia para ir a la página **Basic Information**. En el panel de navegación de la izquierda, elija **Connections**. En la página mostrada, haga clic en la pestaña **Private Connection** y obtenga el puerto del **Database Port** en el área **Basic Information**.

Figura 4-14 Obtención del puerto

P	rivate Connection	Public Connection		
	Basic Information			
	Database Port	8635 🖉	VPC	dds-st-test-vpc
	SSL	Ţ	Subnet	dds-st-test-subnet ()

- **DB_USER** es el usuario de la base de datos. El valor predeterminado es **rwuser**.
- FILE_PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: Para asegurarse de que la comunicación interna de los nodos únicos no ocupe recursos como la dirección IP del usuario y el ancho de banda, el certificado de nodo único se genera utilizando la dirección IP de gestión interna. -- sslAllowInvalidHostnames es necesario para la conexión SSL a través de redes privadas.

Ejemplo de comandos:

./mongo --host 192.168.xx.xx --port 8635 -u rwuser -p --authenticationDatabase admin -ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames

Introduzca la contraseña de la base de datos cuando se le solicite:

Enter password:

Paso 9 Compruebe el resultado de la conexión. Si se muestra la siguiente información, la conexión se realiza correctamente.

replica:PRIMARY>

----Fin

Conexión sin encriptar

AVISO

Si se conecta a una instancia a través de una conexión no cifrada, deshabilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo deshabilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

- **Paso 1** Inicie sesión en el ECS.
- Paso 2 Conéctese a una instancia DDS.

Uso de una dirección IP privada

Ejemplo de comando:

./mongo --host<*DB_HOST*>--port<*DB_PORT*>-u<*DB_USER*>-p --authenticationDatabase admin

Descripción de parámetros:

• DB_HOST es la dirección IP privada de la instancia que se va a conectar.

En la página **Instances**, haga clic en el nombre de la instancia. Se muestra la página **Basic Information**. Elija **Connections**. En la pestaña **Private Connection**, obtenga la dirección IP del nodo correspondiente.

Node Information



• **DB_PORT** es el puerto de la base de datos. El número de puerto predeterminado es 8635.

Puede hacer clic en el nombre de la instancia para ir a la página **Basic Information**. En el panel de navegación de la izquierda, elija **Connections**. En la página mostrada, haga clic en la pestaña **Private Connection** y obtenga el puerto del **Database Port** en el área **Basic Information**.

Figura 4-15 Obtención del puerto

Private Connection	Public Connection		
Basic Informatic	on		
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	Ŧ	Subnet	dds-st-test-subnet (

• **DB_USER** es el usuario de la base de datos. El valor predeterminado es **rwuser**.

Ejemplo de comandos:

```
./mongo --host 192.168.xx.xx --port 8635 -u rwuser -p --authenticationDatabase admin
```

Introduzca la contraseña de la base de datos cuando se le solicite:

Enter password:

Paso 3 Compruebe el resultado de la conexión. Si se muestra la siguiente información, la conexión se realiza correctamente.

replica:PRIMARY>

----Fin

4.2.4 Conexión a una instancia de nodo único a través de una red pública

4.2.4.1 Vinculación y desvinculación de una EIP

Después de crear una instancia, puede enlazar una EIP a ella para permitir el acceso externo. Si más adelante desea prohibir el acceso externo, también puede desvincular la EIP de la instancia.

Precauciones

- La supresión de una EIP vinculada no significa que la EIP no esté vinculada.
- Antes de acceder a una base de datos, solicite una EIP en la consola de VPC. A continuación, agregue una regla de entrada para permitir las direcciones IP o los intervalos de direcciones IP de los ECS. Para obtener más información, véase Configuración de un grupo de seguridad.
- Para cambiar la EIP que se ha enlazado a un nodo, desvincúlela del nodo primero.

Vinculación de una EIP

Paso 1 Inicie sesión en la consola de gestión.

- Paso 2 Haga clic en 🔍 en la esquina superior izquierda, y seleccione una región y un proyecto.
- **Paso 3** Haga clic en = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.

Paso 4 En la página Instances, haga clic en el nombre de instancia de nodo único.

Paso 5 En el panel de navegación de la izquierda, elija Connections. Haga clic en la pestaña Public Connection. En el área Basic Information, localice el nodo al que desea enlazar una EIP y haga clic en Bind EIP en la columna Operation.

Figura 4-16 Vinculación de una EIP

te Connection Put	olic Connectio	n			
Basic Information					
atabase Port 8	635 🖉			SSL	▲
Address					
ublic Network Connection A	Address Unb	ound			
Name/ID	AZ	Private IP Address	Private Domain	EIP	Operation
dds-d629_single_node_1	az1	192.	d42ec4836de74	Onbound	Change Private IP Address More 🔺
					Change Private Domain Name
					Bind EIP

También puede localizar el nodo en el área **Node Information** de la página **Basic Information** y hacer clic en **Bind EIP** en la columna **Operation**.

Figura 4-17 Vinculación de una EIP

Node Information							
Name/ID	Status	AZ	Private IP Address	Private Domain Name	EIP	Operation	
dds-d629_single_node_1	 Available 	az1	192.	d42ec4836de74e37ae2e19da03	Unbound	View Metric Change Priva	ite IP Address More 🔺
							Change Private Domain Name
							Bind EIP

Paso 6 En el cuadro de diálogo que se muestra, se muestran todos las EIP independientes disponibles. Seleccione la EIP requerido y haga clic en OK. Si no se muestran las EIP disponibles, haga clic en View EIP y cree una EIP en la consola de VPC.

Figura 4-18 Selección de una EIP

For out	security purpo bound and inb	oses, after bindin ound rules in the	ig the EIP, use SSL to con e security group.	nect to t	the database and add	
lode	Information	Node Name		Status		
				A)	vailable	
elect	EIP					C
	EIP		Status		Bandwidth	
			⊗ Unbound		5 Mbit/s	
0			🕲 Unbound		5 Mbit/s	
			Onbound		88 Mbit/s	

Paso 7 En la columna EIP, puede ver la EIP que estaba enlazada.

Para desvincular una EIP de la instancia, consulte Desvinculación de una EIP.

----Fin

Desvinculación de una EIP

Paso 1 Inicie sesión en la consola de gestión.

- Paso 2 Haga clic en 💿 en la esquina superior izquierda, y seleccione una región y un proyecto.
- **Paso 3** Haga clic en = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.
- Paso 4 En la página Instances, haga clic en el nombre de instancia de nodo único.
- Paso 5 En el panel de navegación de la izquierda, elija Connections. Haga clic en la pestaña Public Connection. En el área Basic Information, localice el nodo y haga clic en Unbind EIP en la columna Operation.

Figura 4-19 Desvinculación de una EIP

Name/	AZ	Private IP Address	EIP	Operation	
b76d17	az	192.168.106.237		Change Private IP Address	Unbind EIP

También puede localizar el nodo en el **Node Information area** de la página **Basic Information** y hacer clic en **Unbind EIP** en la columna **Operation**.

Paso 6 En el cuadro de diálogo que se muestra, haga clic en Yes.

Para enlazar una EIP a la instancia de nuevo, consulte Vinculación de una EIP.

----Fin

4.2.4.2 Configuración de un grupo de seguridad

Un grupo de seguridad es un grupo lógico. Proporciona políticas de control de acceso para los ECS y las instancias que tienen los mismos requisitos de protección de seguridad y son de confianza mutua en una VPC.

Para garantizar la seguridad y confiabilidad de la base de datos, debe configurar reglas de grupo de seguridad para permitir que las direcciones IP y los puertos específicos accedan a instancias de DDS.

Si intenta conectarse a una instancia a través de una EIP, debe configurar una regla de entrada para el grupo de seguridad asociado a la instancia.

Precauciones

- De forma predeterminada, una cuenta puede crear hasta 500 reglas de grupo de seguridad.
- Demasiadas reglas de grupo de seguridad aumentarán la latencia del primer paquete, por lo que se recomienda un máximo de 50 reglas para cada grupo de seguridad.
- Una instancia DDS solo puede asociarse a un grupo de seguridad.

Procedimiento

Paso 1 Inicie sesión en la consola de gestión.

- **Paso 2** Haga clic en 🔍 en la esquina superior izquierda y seleccione una región y un proyecto.
- Paso 3 Haga clic en = en la esquina superior izquierda de la página y elija Databases > Document Database Service.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia. Se muestra la página Basic Information.
- **Paso 5** En el área **Network Information** de la página **Basic Information**, haga clic en el grupo de seguridad.

Figura 4-20 Grupo de seguridad

Network Information							
VPC	dds-st-test-vpc	Subnet	dds-st-test-subnet-2 (
Security Group	Sys-default 🖉	Database Port	8635 🖉				

También puede elegir **Connections** en el panel de navegación de la izquierda. En la pestaña **Public Connection**, en el área **Security Group**, haga clic en el nombre del grupo de seguridad.

Figura 4-21 Grupo de seguridad

Security Group Security Group Add Rule Delete Inbound Rules(1)	/s-default 🖉	С
Protocol & Port (?)	Source (?)	Description
All	Sys-default	-

- Paso 6 En la página Security Group, busque el grupo de seguridad de destino y haga clic en Manage Rule en la columna Operation.
- Paso 7 En la pestaña Inbound Rules, haga clic en Add Rule. Aparece el cuadro de diálogo Add Inbound Rule.
- Paso 8 Agregue una regla de grupo de seguridad como se le solicite.

Figura 4-22 Agregar regla de entrada

Add Inbound Rule Learn more about security group configuration.									
Inbound rules allow incoming traffic to instances associated with the security group.									
Security Group Sys-default You can import multiple rules in a batch.									
Protocol & Port ⑦	Туре	Source ⑦	Description	Operation					
TCP Example: 22 or 22-30	IPv4 v	IP address 0.0.0.0/0	•	Operation -					
Add Rule									
		OK Cancel							

Tabla 4-11 Configuración de reglas entrantes

Parámetro	Descripción	Valor de ejemplo
Priority	Prioridad de regla de grupo de seguridad.	1
	El valor de prioridad varía de 1 a 100. La prioridad predeterminada es 1 y tiene la prioridad más alta. La regla de grupo de seguridad con un valor menor tiene mayor prioridad.	
Action	Las acciones de la regla del grupo de seguridad.	Allow
	Una regla con una acción de denegación invalida a otra con una acción de permiso si las dos reglas tienen la misma prioridad.	
Protocol & Port	El protocolo de red requerido para el acceso. La opción puede ser All, TCP, UDP, ICMP, o GRE.	ТСР

Parámetro	Descripción	Valor de ejemplo
	Puerto: el puerto en el que desea permitir el acceso a DDS. El puerto predeterminado es 8635. El puerto oscila entre 2100 y 9500 o puede ser 27017, 27018, o 27019.	8635
Туре	Tipo de dirección IP. Solo IPv4 y IPv6 son compatibles.	IPv4
Source	Especifica la dirección IP, el grupo de seguridad y el grupo de direcciones IP compatibles, que permiten el acceso desde direcciones IP o instancias de otro grupo de seguridad. Ejemplo:	0.0.0/0
	• Dirección IP única: 192.168.10.10/32	
	 Segmento de dirección IP: 192.168.1.0/24 	
	• Todas las direcciones IP: 0.0.0.0/0	
	• Grupo de seguridad: sg-abc	
	• Grupo de direcciones IP: ipGroup-test	
	Si introduce un grupo de seguridad, todos los ECS asociados al grupo de seguridad cumplen con la regla creada.	
	Para obtener más información acerca de los grupos de direcciones IP, consulte Grupo de direcciones IP .	
Description	(Opcional) Proporciona información adicional acerca de la regla del grupo de seguridad. Este parámetro es opcional.	-
	La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	

Paso 9 Haga clic en OK.

----Fin

4.2.4.3 Conexión a una instancia de nodo único mediante Mongo Shell (red pública)

En los siguientes escenarios, puede acceder a una instancia DDS desde Internet vinculando una EIP a la instancia.

Escenario 1: Las aplicaciones se despliegan en un ECS y no están en la misma región que la instancia DDS.



Figura 4-23 Acceso a DDS desde ECS en todas las regiones

Escenario 2: Sus aplicaciones se despliegan en un servidor en la nube proporcionado por otros proveedores.



Figura 4-24 Acceso a DDS desde otros servidores en la nube

Esta sección describe cómo utilizar Mongo Shell para conectarse a una instancia de nodo único a través de una EIP.

Puede conectarse a una instancia mediante una conexión SSL o una conexión sin cifrar. La conexión SSL es encriptada y más segura. Para mejorar la seguridad de la transmisión de datos, conéctese a instancias mediante SSL.

Prerrequisitos

- 1. Para obtener más información acerca de cómo crear e iniciar sesión en un ECS, consulte Comprar un ECS e iniciar sesión en un ECS.
- 2. Vincule una EIP a la instancia de nodo único y configure las reglas de grupo de seguridad para garantizar que se pueda acceder al EIP desde el ECS.
- 3. Instale el cliente MongoDB en el ECS.

Para obtener más información sobre cómo instalar un cliente MongoDB, consulte ¿Cómo puedo instalar un cliente MongoDB?

SSL

AVISO

Si se conecta a una instancia a través de la conexión SSL, habilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo habilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

- Paso 1 Inicie sesión en la consola de gestión.
- **Paso 2** Haga clic en 🔍 en la esquina superior izquierda, y seleccione una región y un proyecto.
- Paso 3 Haga clic en = en la esquina superior izquierda de la página y elija Databases > Document Database Service.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia.
- Paso 5 En el panel de navegación de la izquierda, elija Connections.
- Paso 6 En el área Basic Information, haga clic en 📥 junto al campo SSL.
- Paso 7 Importar el certificado raíz al Linux o Windows ECS. Para obtener más información, consulte ¿Cómo puedo importar el certificado raíz a un sistema operativo Windows o Linux?
- Paso 8 Conéctese a la instancia en el directorio donde se encuentra el cliente MongoDB.

Utilizar una EIP

Ejemplo de comando:

```
./mongo --host <DB_HOST> --port <DB_PORT> -u <DB_USER> -p --
authenticationDatabaseadmin --ssl --sslCAFile<FILE_PATH> --
sslAllowInvalidHostnames
```

Descripción de parámetros:

• **DB_HOST** es la EIP enlazada a la instancia que se va a conectar.

En la página **Instances**, haga clic en el nombre de la instancia. Se muestra la página **Basic Information**. Elija **Connections**> **Public Connection** y obtenga la EIP del nodo correspondiente.

Figura 4-25 Obtención de una EIP

B	Basic Informati	ion							
D	atabase Port		8635 🖉			SS	L	▲	
A	ddress								
P	ublic Network C	onnectio	on Address	Unbound					
	Name/ID	AZ	Private	Private	EIP		Operation		
	elana. Maria	az2	192.16	a4f871	🕲 Unbou	und	Change Private IP A	ddress More 👻	

• **DB_PORT** es el puerto de la base de datos. El número de puerto predeterminado es 8635.

Puede hacer clic en el nombre de la instancia para ir a la página **Basic Information**. En el panel de navegación de la izquierda, elija **Connections**. En la página mostrada, haga clic en la pestaña **Public Connection** y obtenga el puerto del campo **Database Port** en el área **Basic Information**.

Figura 4-26 Obtención del puerto

Basic Information					
Database Port	863	5 🖉		SSL	
Address					
Public Network Conn	ection Add	lress	mongodb://r admin 🗇	wuser: <password>6</password>	8635/test?authSource=
Name/ID	AZ	Private I	EIP	Operation	
dds-ce25_mong 000e813fb5574c	az4	192.168		Change Private IP Addr	ress Unbind EIP
dds-ce25_mong bad06d1cf2594e	az4	192.168		Change Private IP Addr	ress Bind EIP

- **DB_USER** es el usuario de la base de datos. El valor predeterminado es **rwuser**.
- FILE_PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: Para asegurarse de que la comunicación interna de los nodos únicos no ocupe recursos como la dirección IP del usuario y el ancho de banda, el certificado de nodo único se genera utilizando la dirección IP de gestión interna. -- sslAllowInvalidHostnames es necesario para la conexión SSL a través de una red pública.

Ejemplo de comandos:

./mongo --host 192.168.xx.xx --port 8635 -u rwuser -p --authenticationDatabase admin -ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames

Introduzca la contraseña de la base de datos cuando se le solicite:

Enter password:

Paso 9 Compruebe el resultado de la conexión. Si se muestra la siguiente información, la conexión se realiza correctamente.

----Fin

Conexión sin encriptar

AVISO

Si se conecta a una instancia a través de una conexión no cifrada, deshabilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo deshabilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

- Paso 1 Inicie sesión en el ECS.
- Paso 2 Conéctese a una instancia DDS.

Utilizar una EIP

Ejemplo de comando:

./mongo --host <*DB_HOST*> --port <*DB_PORT*> -u <*DB_USER*> -p -authenticationDatabase admin

Descripción de parámetros:

• **DB_HOST** es la EIP enlazada a la instancia que se va a conectar.

En la página **Instances**, haga clic en el nombre de la instancia. Se muestra la página **Basic Information**. Elija **Connections**> **Public Connection** y obtenga la EIP del nodo correspondiente.

Figura 4-27 Obtención de una EIP

Basic Informat	ion							
Database Port		8635 🖉			SSI		▲	
Address								
Public Network C	Connectio	on Address	Unbound					
Name/ID	AZ	Private	Private	EIP		Operation		
	az2	192.16	a4f871	🕲 Unbour	d	Change Private IP Ac	ldress More 👻	

• **DB_PORT** es el puerto de la base de datos. El número de puerto predeterminado es 8635.

Puede hacer clic en el nombre de la instancia para ir a la página **Basic Information**. En el panel de navegación de la izquierda, elija **Connections**. En la página mostrada, haga clic en la pestaña **Public Connection** y obtenga el puerto del campo **Database Port** en el área **Basic Information**.

Figura 4-28 Obtención del puerto

Basic Information					
Database Port	863	5 🖉		SSL	
Address					
Public Network Conn	ection Add	lress n a	nongodb://rv	vuser: <password>6</password>	8635/test?authSource=
Name/ID	AZ	Private I	EIP	Operation	
dds-ce25_mong 000e813fb5574c	az4	192.168		Change Private IP Ade	dress Unbind EIP
dds-ce25_mong bad06d1cf2594e	az4	192.168		Change Private IP Ade	dress Bind EIP

• **DB_USER** es el usuario de la base de datos. El valor predeterminado es **rwuser**.

Ejemplo de comandos:

./mongo --host 192.168.xx.xx --port 8635 -u rwuser -p --authenticationDatabase admin

Introduzca la contraseña de la base de datos cuando se le solicite:

Enter password:

Paso 3 Compruebe el resultado de la conexión. Si se muestra la siguiente información, la conexión se realiza correctamente. replica:PRIMARY>

----Fin

4.2.4.4 Conexión a una instancia de nodo único mediante Robo 3T

Si desea conectarse a una instancia desde un dispositivo local, puede vincular una EIP a la instancia y usar Robo 3T para conectarse a la instancia a través de una red pública.

Esta sección describe cómo usar Robo 3T para conectarse a una instancia de clúster desde un dispositivo local. En esta sección, se utiliza como ejemplo el sistema operativo Windows utilizado por el cliente.

Robo 3T puede conectarse a una instancia con una conexión no cifrada o una conexión cifrada (SSL). Para mejorar la seguridad de la transmisión de datos, conéctese a instancias mediante SSL.

Diagrama de conexión



Figura 4-29 Diagrama de conexión

Prerrequisitos

- 1. **Vincular una EIP** a la instancia de nodo único y configure las reglas de grupo de seguridad para garantizar que se pueda acceder a la instancia mediante Robo 3T.
- 2. Instale Robo 3T.

Instalar Robo 3T. Para obtener más información, consulte ¿Cómo puedo instalar Robo 3T?

SSL

AVISO

Si se conecta a una instancia a través de la conexión SSL, habilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo habilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

Paso 1 Ejecute el Robo 3T instalado. En el cuadro de diálogo mostrado, haga clic en Create.

🛃 MongoDB Connections					×
<u>Create</u> , <u>edit</u> , <u>remove</u> , <u>clone</u> or :	reorder connections via drag´n´	drop.			
Name	Address	Attributes	Auth.	Database / User	
			[📃 C <u>o</u> nnect - Cancel	

- Paso 2 En el cuadro de diálogo Connection Settings, establezca los parámetros de la nueva conexión.
 - 1. En la pestaña **Connection**, escriba el nombre de la nueva conexión en el cuadro de texto **Name** e introduzca el puerto EIP y la base de datos enlazados a la instancia de base de datos DDS en el cuadro de texto **Name**.

Figura 4-31 Conexión

Connection	Settings	
Connection	Authentication SSH TLS Advanced	
Туре:	Direct Connection	
Name:	test	
Address:		: 8635
	IPv4, IPv6 or domain name.	si can be either
From URI	Import connection details from MongoDB URI	connection string

2. En la pestaña Authentication, establezca Database en admin, User Name en rwuser y Password en la contraseña de administrador establecida durante la creación de la instancia de clúster.

Figura 4-32 Autenticación

📃 Connection Se	ettings	×
Connection	Authentication SSH TLS Advanced	
🗹 Perform autl	nentication	
Database	admin	
	The admin database is unique in MongoDB. Users with	
Vser Name	rwuser	
Password	<u>ښ</u>	
Auth Mechanism	SCRAM-SHA-1	
Manually spa	ecify visible databases	-
<u>() T</u> est	Save Cancel	

3. En la pestaña TLS, seleccione Use TLS protocol y seleccione Self-signed Certificate para Authentication Method.

Figura 4-33 SSL

Connection	Settings							×
Connection	Authentic	ation	SSH	TLS	Advanc	ed		
🗹 Use TLS p	rotocol							
Authenticati	on Method:	Self-:	signed (Certific	ate			\sim
		In gen unless certif will b valida	eral, a the ne icate i e encry tion of	void us: twork i: s used, pted how server	ing self s trusted the comm wever the identity	-signed cert d. If self munications are will be 7.	tificates signed channel no	
🗌 Vse PEM C	ert./Key:	Enable requir	this o es CA-s	ption to igned cl	o connec: lient cer	t to a Mongo tificates/}	DB that ey file.	
Advanced (Options							
<u>i <u>T</u>est</u>						Save	Cano	el

- 4. Haga clic en Save.
- Paso 3 En la página MongoDB Connections, haga clic en Connect para conectarse a la instancia de un nodo único.

🖁 MongoDB Connectio	ns		>
<u>Create, edit, remove, d</u>	Lone or reorder connections via d	rag'n' drop.	
Name	Address	Attributes Auth. Database / Us	ser
📃 test	:8635	TLS 🛛 🖉 admin / rwuser	
		📃 C <u>o</u> nnect	Cancel

Figura 4-34 Información de conexión de nodo único

Paso 4 Si la instancia de un solo nodo se conecta correctamente, se muestra la página mostrada en Figura 4-35.

Figura 4-35 Nodo único conectado





Conexión sin encriptar

AVISO

Si se conecta a una instancia a través de una conexión no cifrada, deshabilite SSL primero. De lo contrario, se notifica un error. Para obtener más información sobre cómo deshabilitar SSL, consulte **Habilitación y deshabilitación de SSL**.

Paso 1 Ejecute el Robo 3T instalado. En el cuadro de diálogo mostrado, haga clic en Create.

Figura 4-36 Conexione	s	
-----------------------	---	--

🛃 MongoDB Connections					×
<u>Create</u> , <u>edit</u> , <u>remove</u> , <u>clone</u> or :	reorder connections via drag´n´	drop.			
Name	Address	Attributes	Auth.	Database / User	
			[📃 C <u>o</u> nnect - Cancel	

- Paso 2 En el cuadro de diálogo Connection Settings, establezca los parámetros de la nueva conexión.
 - 1. En la pestaña **Connection**, escriba el nombre de la nueva conexión en el cuadro de texto **Name** e introduzca el puerto EIP y la base de datos enlazados a la instancia de base de datos DDS en el cuadro de texto **Name**.

Figura 4-37 Conexión

Connection	Authentication SSH TLS Advanced
ype:	Direct Connection
lame:	test
Address:	: 8635 Specify host and port of MongoDB server. Host can be eith TPu4. TPu6 or domain name
.ddress:	: 8635 Specify host and port of MongoDB server. Host can be eith IPv4, IPv6 or domain name.

2. En la pestaña Authentication, establezca Database en admin, User Name en rwuser y Password en la contraseña de administrador establecida durante la creación de la instancia de clúster.

Figura 4-38 Autenticación

📃 Connection Se	ettings	×
Connection	Authentication SSH TLS Advanced	
🗹 Perform aut	nentication	
Database	admin	
	The admin database is unique in MongoDB. Users with	
User Name	rwuser	
Password	<u>کې</u>	
Auth Mechanism	SCRAM-SHA-1	
Manually sp	ecify visible databases	-
i <u>T</u> est	Save Cancel	

3. En la pestaña TLS, seleccione Use TLS protocol y seleccione Self-signed Certificate para Authentication Method.

Figura 4-39 SSL

Connection	Settings							×
Connection	Authentic	ation	SSH	TLS	Advanc	ed		
🗹 Use TLS p	rotocol							
Authenticati	on Method:	Self-	signed (Certific	ate			\sim
		In gen unless certif will b valida	eral, a the ne icate i e encry tion of	void us; twork is s used, pted how server	ing self s truste the com vever th identit	-signed cer d. If self- munications ere will bo y.	rtifica -signed s chann e no	ites i iel
🗌 Vse PEM C	ert./Key:	Enable requir	this o es CA-s	ption to igned cl	o connec Lient ce	t to a Moną rtificates,	goDB th /key fi	iat le.
Advanced	Options							
<u>i <u>T</u>est</u>						Save		Cancel

- 4. Haga clic en Save.
- Paso 3 En la página MongoDB Connections, haga clic en Connect para conectarse a la instancia de un nodo único.

🖁 MongoDB Connections)
<u>reate, edit, remove, clone</u> d	r reorder connections via dr	ag'n'drop.		
Name	Address	Attributes	Auth. Database / User	
📃 test	:8635	TLS	🔎 admin / rwuser	
			📃 C <u>o</u> nnect 🛛 Car	ncel

Figura 4-40 Información de conexión de nodo único

Paso 4 Si la instancia de nodo único se conecta correctamente, se muestra la página mostrada en Figura 4-41.

Figura 4-41 Nodo único conectado



----Fin

4.2.5 Conexión a una instancia de nodo único mediante código de programa

4.2.5.1 Java

Si se está conectando a una instancia mediante Java, un certificado SSL es opcional, pero descargar un certificado SSL y cifrar la conexión mejorará la seguridad de su instancia. SSL está deshabilitado de forma predeterminada para las instancias de base de datos recién creadas. Puede habilitar SSL haciendo referencia a Activación o desactivación de SSL. SSL

cifra las conexiones a las bases de datos, pero aumenta el tiempo de respuesta de la conexión y el uso de la CPU. Por lo tanto, se recomienda no habilitar SSL.

Prerrequisitos

Familiarícese con:

- Conceptos básicos de computadora
- Código Java

Obtención y uso de Java

- Descargue el controlador Jar desde: https://repo1.maven.org/maven2/org/mongodb/ mongo-java-driver/3.0.4/
- Para ver la guía de uso, visite https://mongodb.github.io/mongo-java-driver/4.2/ driver/getting-started/installation/.

Uso de un certificado SSL

D NOTA

- Descargue el certificado SSL y verifique el certificado antes de conectarse a las bases de datos.
- En la página Instances, haga clic en el nombre de la instancia de base de datos de destino. En el área **DB Information** de la página **Basic Information**, haga clic en de en el campo **SSL** para descargar el certificado raíz o el paquete de certificados.
- Para obtener más información sobre cómo configurar una conexión SSL, consulte el documento oficial del controlador Java de MongoDB en https://www.mongodb.com/docs/drivers/java/sync/ current/fundamentals/connection/tls/#std-label-tls-ssl.

Conéctese a una instancia de nodo único mediante Java. El formato del enlace Java es el siguiente:

mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>?
authSource=admin&ssl=true

Parámetro	Descripción
<username></username>	Nombre de usuario actual.
<password></password>	Contraseña para el nombre de usuario actual
<instance_ip></instance_ip>	Si intenta obtener acceso a la instancia desde un ECS, establezca <i>instance_ip</i> en la dirección IP privada que se muestra en la página Basic Information de la instancia a la que desea conectarse.
	Si tiene la intención de acceder a la instancia a través de una EIP, establezca <i>instance_ip</i> en la EIP que se ha enlazado a la instancia.
<instance_port></instance_port>	Puerto de la base de datos que se muestra en la página Basic Information . Valor predeterminado: 8635
<database_name></database_name>	Nombre de la base de datos que se va a conectar.
authSource	Base de datos de usuarios de autenticación. El valor es admin.

Tabla 4-12 Descripción del parámetro

Parámetro	Descripción
ssl	Modo de conexión. true indica que se utiliza el modo de conexión SSL.

Utilice la herramienta keytool para configurar el certificado de CA. Para obtener más información sobre los parámetros, consulte **Tabla 4-13**.

keytool -importcert -trustcacerts -file <path to certificate authority file> keystore <path to trust store> -storepass <password>

Tabla 4-13 Descripción del parámetro

Parámetro	Descripción
<pre><path authority="" certificate="" file="" to=""></path></pre>	Ruta para almacenar el certificado SSL.
<pre><path store="" to="" trust=""></path></pre>	Ruta para almacenar el truststore. Establezca este parámetro según sea necesario, por ejemplo, ./trust/ certs.keystore.
<pre><password></password></pre>	Contraseña personalizada.

Configure las propiedades del sistema JVM en el programa para que apunten al truststore y keystore correctos:

- System.setProperty("javax.net.ssl.trustStore","path to trust store>");
- System.setProperty("javax.net.ssl.trustStorePassword","<password>");

Para obtener más información sobre el código Java, consulte el siguiente ejemplo: public class Connector {

```
public static void main(String[] args) {
        try {
            System.setProperty("javax.net.ssl.trustStore", "./trust/
certs.keystore");
            System.setProperty("javax.net.ssl.trustStorePassword",
"123456");
            ConnectionString connString = new
ConnectionString("mongodb://
<username>:<password>@<instance ip>:<instance port>/<database name>?
authSource=admin&ssl=true");
            MongoClientSettings settings = MongoClientSettings.builder()
                    .applyConnectionString(connString)
                    .applyToSslSettings(builder -> builder.enabled(true))
                    .applyToSslSettings(builder ->
builder.invalidHostNameAllowed(true))
                    .build();
            MongoClient mongoClient = MongoClients.create(settings);
            MongoDatabase database = mongoClient.getDatabase("admin");
            //Ping the database. If the operation fails, an exception
occurs.
            BsonDocument command = new BsonDocument("ping", new
BsonInt64(1));
            Document commandResult = database.runCommand(command);
            System.out.println("Connect to database successfully");
```

```
} catch (Exception e) {
    e.printStackTrace();
    System.out.println("Test failed");
}
```

Conexión sin el certificado SSL

D NOTA

No es necesario descargar el certificado SSL porque no se requiere la verificación del certificado en el servidor.

Conecte un único nodo usando Java. El formato de enlace Java es el siguiente: mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>? authSource=admin

Parámetro	Descripción
<username></username>	Nombre de usuario actual.
<password></password>	Contraseña para el nombre de usuario actual
<instance_ip></instance_ip>	Si intenta obtener acceso a la instancia desde un ECS, establezca <i>instance_ip</i> en la dirección IP privada que se muestra en la página Basic Information de la instancia a la que desea conectarse.
	Si tiene la intención de acceder a la instancia a través de una EIP, establezca <i>instance_ip</i> en la EIP que se ha enlazado a la instancia.
<instance_port></instance_port>	Puerto de la base de datos que se muestra en la página Basic Information. Valor predeterminado: 8635
<database_name></database_name>	Nombre de la base de datos que se va a conectar.
authSource	Base de datos de usuarios de autenticación. El valor es admin.

Ejemplo de script en Java:

```
public class Connector {
    public static void main(String[] args) {
        try {
            ConnectionString connString = new
ConnectionString("mongodb://
<username>:<password>@<instance ip>:<instance port>/<database name>?
authSource=admin");
            MongoClientSettings settings = MongoClientSettings.builder()
                    .applyConnectionString(connString)
                    .retryWrites(true)
                    .build();
            MongoClient mongoClient = MongoClients.create(settings);
            MongoDatabase database = mongoClient.getDatabase("admin");
            //Ping the database. If the operation fails, an exception
occurs.
            BsonDocument command = new BsonDocument("ping", new
BsonInt64(1));
```

```
Document commandResult = database.runCommand(command);
System.out.println("Connect to database successfully");
} catch (Exception e) {
    e.printStackTrace();
    System.out.println("Test failed");
}
}
```

4.2.5.2 Python

Esta sección describe cómo conectarse a una instancia de nodo único usando Python.

Prerrequisitos

1. Para conectar un ECS a una instancia, el ECS debe poder comunicarse con la instancia DDS. Puede ejecutar el siguiente comando para conectarse a la dirección IP y el puerto del servidor de instancia para probar la conectividad de red.

curl ip:port

Si se muestra el mensaje It looks like you are trying to access MongoDB over HTTP on the native driver port, la conectividad de red es normal.

- 2. Instale Python y el paquete de instalación de terceros **pymongo** en el ECS. Se recomienda Pymongo 2.8.
- 3. Si SSL está habilitado, debe descargar el certificado raíz y subirlo al ECS.

Código de conexión

Habilitación de SSL

```
import ssl
from pymongo import MongoClient
conn_urls="mongodb://rwuser:rwuserpassword@ip:port/{mydb}?
authSource=admin"
connection = MongoClient(conn_urls,connectTimeoutMS=5000,ssl=True,
ssl_cert_reqs=ssl.CERT_REQUIRED,ssl_match_hostname=False,ssl_ca_certs
=${path to certificate authority file})
dbs = connection.database_names()
print "connect database success! database names is %s" % dbs
```

• Deshabilitación de SSL

```
import ssl
from pymongo import MongoClient
conn_urls="mongodb://rwuser:rwuserpassword@ip:port/{mydb}?
authSource=admin"
connection = MongoClient(conn_urls,connectTimeoutMS=5000)
dbs = connection.database_names()
print "connect database success! database names is %s" % dbs
```

D NOTA

- La base de datos de autenticación en la URL debe ser admin. Eso significa configurar authSource a admin.
- En el modo SSL, es necesario generar manualmente el archivo trustStore.
- La base de datos de autenticación debe ser **admin** y, a continuación, cambiar a la base de datos de servicio.

5 Iniciar y cerrar sesión en la consola DDS

Prerrequisitos

Necesita tener una cuenta en la plataforma en la nube antes de poder usar DDS

Por primera vez que utilice DDS, solicite una cuenta en el sitio web oficial. Después de que la aplicación tenga éxito, su cuenta tiene permisos para acceder al servicio DDS, así como a todos los demás servicios en la nube.

Iniciar sesión en la consola DDS

- Paso 1 Abra sitio web oficial de Huawei Cloud
- Paso 2 Haga clic en Console en la parte superior derecha de la página. Se muestra la página de inicio de sesión de la consola de gestión de Huawei Cloud.
- Paso 3 Ingrese la información de la cuenta como se le solicite y haga clic en Log In.

El inicio de sesión es exitoso.

Paso 4 Haga clic en 🔍 en la esquina superior izquierda y seleccione una región y un proyecto.

Si desea utilizar recursos informáticos y de red exclusivamente, debe **habilitar un DeC** y **solicitar recursos de DCC**. Después de habilitar un DeC, puede seleccionar la región y el proyecto de DeC.

Se le cobrará adicionalmente por usar DeC.

Paso 5 Haga clic en = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.

----Fin

Cerrar sesión en la consola DDS

- **Paso 1** En cualquier página de la consola DDS, haga clic en el nombre de usuario en la esquina superior derecha.
- Paso 2 En el cuadro de diálogo que se muestra, haga clic en Log Out.

----Fin

6 Ejemplo: Comprar y conectarse a una

instancia DDS

6.1 Conexión a una instancia de base de datos mediante Mongo Shell

Esta sección describe cómo crear una instancia de base de datos, usar Mongo Shell para conectarse a la instancia de base de datos a través de una red privada, y leer datos y escribir datos en la instancia de base de datos.

- Paso 1: Comprar una instancia de base de datos
- Paso 2: Comprar un ECS
- Paso 3: Configurar reglas de grupo de seguridad
- Paso 4: Conectarse a una instancia de clúster DDS mediante Mongo Shell
- Paso 5: Crear una base de datos y escribir datos en la base de datos

Paso 1: Comprar una instancia de base de datos

- 1. Vaya a la página Custom Config.
- 2. En la página mostrada, seleccione un modo de facturación y configure la información sobre su instancia de base de datos. A continuación, haga clic en **Next**.

Basic Information				
Billing Mode	Yearly/Monthly Pay-per-use			
Region	Device an accurately areas included from each other. For two natural latency and mining proving areas: safet the pagest point			
Project				
AZ	azi az2 az3 az1,az2,az3			
	Deploy your DB instance in a single AZ or three AZs for high availability.			
DB Instance Name	dds-c5d2			
DB Instance Type 🕜	Claster Replica set Claster offer more tobust beeformance than replica sets and more flexible scaling options. The high-availability and flexible scaling have made in the unwalked make them an evaluated whole for tame entermotive			
	Clusters of community edition you can still create: 9. Increase Quota			
Compatible MongoDB Version	4.4 4.2 4.0 3.4 View Version Details			
Storage Type	Uttra-high I/O			
Storage Engine	RocksDB			
Specifications	General-purpose Enhanced II			
mongos				
Node Class	vCPU Memory	Maximum Connections		
	2 vCPUs 8 GB	2,000		
	4 vCPUs 16 GB	4,000		
	8 vCPUs 32 GB	16,000		
	0 16 vCPUs 64 GB	16,000		
	32 vCPUs 128 GB	16,000		
	64 vCPUs 256 GB	16,000		
	Currently selected dds.mongodb.c6.large.4.mongos 2 vCPUs 8 GB			
Nodes	- 2 + The quantity ranges from 2 to 16.			
Parameter Template	Default-DDS-12-Mongos C Vew Parameter Template			
	Deradit-DDS-4.2-Wongos View Parameter Temptate			
	Detaul-DLG-4,2-Munglos Very Paratheet Template			
shard	Desue-DD-42-mongos			
shard Node Class	VCPU Memory	Maximum Connections		
shard Node Class	VCPU J Memory	Maximum Connections 2.000		
shard Node Class	vCPU Memory 0 vev rialities remplace 0 2xCPUs 8 08 0 0 2xCPUs 16 08 0	Maximum Connections 2.000 2.000		
Shard Node Class	vCPU Memory 2xCPUs 8 0B 2xCPUs 16 0B 4xCPUs 16 0B 4xCPUs 16 0B 	Maximum Connections 2.000 2.000 4.000		
shard Node Class	vCPU Memory 2 vCPUs 8 08 2 vCPUs 108 4 vCPUs 108 4 vCPUs 108 4 vCPUs 108 4 vCPUs 108 	Maximum Connections 2.000 2.000 4.000 4.000		
shard Node Class	vCPU Memory • 2 vCPUs 8 08 • 2 vCPUs 16 08 • 4 vCPUs 15 08 • 4 vCPUs 12 08	Maximum Connections 2.000 2.000 4.000 4.000 16.000		
shard Node Class	vCPU Memory 2 vCPUs 8 08 2 vCPUs 10 08 4 vCPUs 10 08 4 vCPUs 12 08 8 vCPUs 52 08 8 vCPUs 64 08 7 vCPUs 64 08 	Maximum Connections 2.000 2.000 4.000 4.000 16.000 16.000		
shard Nose Class	vCPU Memory 2 vCPUs 8 GB 2 vCPUs 16 GB 4 vCPUs 12 GB 8 vCPUs 32 GB 8 vCPUs 34 GB 16 vCPUs 34 GB 16 vCPUs 34 GB 16 vCPUs 34 GB 	Maximum Connections 2.000 2.000 4.000 4.000 16.000 16.000 16.000		
shard Node Class	VEPU / Memory 2 vCPUs 8 08 2 vCPUs 16 08 4 vCPUs 16 08 4 vCPUs 12 08 8 vCPUs 20 08 9 vCPUs 64 08 16 vCPUs 64 08 Currently selected: dbs.monpobl.cbi.large.4.shard 2 vCPUs 8 08	Maximum Connections 2.000 2.000 4.000 4.000 16.000 16.000 15.000		
shard Node Class	vCPU Memory 2 xCPUs 8 GB 2 xCPUs 16 GB 4 xCPUs 12 GB 8 xCPUs 32 GB 9 xCPUs 54 GB 19 xCPUs 54 GB 19 xCPUs 54 GB Currently selected 000000000000000000000000000000000000	Maximum Connections 2.000 2.000 4.000 4.000 16.000 16.000		
shard Node Class	VEV / Memory 2 x <pu1 08<="" 18="" td=""> 2 x<pu1 08<="" 18="" td=""> 2 x<pu1 08<="" 18="" td=""> 4 x<pu1 08<="" 12="" td=""> 8 x<pu1 08<="" 12="" td=""> 9 x<pu1 08<="" 18="" td=""> 14 x<pu1 08<="" 12="" td=""> 9 x<pu1 08<="" 18="" td=""> 14 x<pu1 08<="" 12="" td=""> 9 x<pu1 08<="" 18="" td=""> 14 x<pu1 08<="" 12="" td=""> 16 x<pu1 08<="" 18="" td=""> 17 x<pu1 08<="" 18="" td=""> 16 x<pu1 08<="" 18="" td=""> 17 x<pu1 08<="" 18="" td=""> 17 x<pu1 08<="" 18="" td=""> 18 x<pu1 08<="" 18="" td=""> 19 x<pu1 08<="" 18="" td=""></pu1></pu1></pu1></pu1></pu1></pu1></pu1></pu1></pu1></pu1></pu1></pu1></pu1></pu1></pu1></pu1></pu1></pu1>	Maximum Connections 2,000 2,000 4,000 16,000 16,000 16,000 10 10 + 08 ^(*)		
shard Node Class	vCPU Memory VCPU is 18 08 2 vCPUs 18 08 4 vCPUs 18 08 4 vCPUs 12 08 8 vCPUs 52 08 8 vCPUs 64 08 Currently leaded data and log vCPUs 6 08 70 08 750 100 125 150 1750 2000 To call 9 250 500 750 100 125 150 1750 2000 To call 9 250 500 750 100 125 150 1750 2000 To call the that the DB instance can still be used if the storage space is about to be used up, the database is set to read-only, and data cannot be modified 	Maximum Connections 2:000 0:000 0:000 1:0:000 1:0:000 1:0:000 1:0:000 1:0:000 1:0:000 1:0:000 1:0:000 1:0:000 1:0:000 1:0:000 1:0:000		
shard Node: Class Storage Space	VEV / Neuropa Vev / Rainteen interplace vCPU Memory	Maximum Connections 2.000 2.000 4.000 4.000 16.000 17.000 16.000 16.000 17.000 18.000 19.000 10.000 10.000 11.000 11.000 11.000 11.000 11.000		
shard Nose Class Storage Space Noses Parameter Temptato	VEV J Memory 2 vCPUs 8 GB 2 vCPUs 16 GB 4 vCPUs 16 GB 4 vCPUs 12 GB 8 vCPUs 32 GB 8 vCPUs 54 GB 19 vCPUs 54 GB 19 vCPUs 54 GB 10 GE 20 200 70 To ensure that the DB instance can still be used if the storage space is about to be used up, the database is set to read-only, and data cannot be modified 2 until y cannot be modified	Maximum Connections 2,000		
shard Node Class Storage Space	VEV Finalment Integration VEV Finalment Integration VEVU fina	Maximum Connections 2,000 2,000 4,000 4,000 16,000		
shard Node Class Storage Space Nodes Parameter Template config	VEX.PU Memory 2 xxCPUs 8 G8 2 xxCPUs 16 G8 4 xxCPUs 16 G8 5 xxxPUs 16 G8 5 xxxxPUs 16 G8 5 xxxxPUs 16 G8 5 xxxxPUs 16 G8 5 xxxxxPUs 16 G8 5 xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Maximum Connections 2,000 2,000 4,000 4,000 16,000 15,000 15,000 16 Of Content of Conten		
shard Node Class	vCPU Memory • VKP / Balancer / Antipue • VCPU Memory • 2 xCPUs 8 GB • 2 xCPUs 16 GB • 4 xCPUs 16 GB • 4 xCPUs 16 GB • 4 xCPUs 12 GB • 8 xCPUs 54 GB • 16 xCPUs 54 GB • 16 xCPUs 64 GB • 16 xCPUs 64 GB • 16 xCPUs 64 GB • 0 to xCPUs 750 • 0 to xCPUs 750 </th <th>Maximum Connections 2,000 2,000 4,000 16,000 16,000 10 + GE ③ 1.0 + GE ③</th>	Maximum Connections 2,000 2,000 4,000 16,000 16,000 10 + GE ③ 1.0 + GE ③		
shard Node Class Storage Space Nodes Parameter Template config Node Class	VEV Finalment Amplan VCPU J Memory VCPU J 18 08 VEVENUE VEVENUE </th <th>Maximum Connections 2,000 2,000 4,000 16,000 16,000 10 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 +</th>	Maximum Connections 2,000 2,000 4,000 16,000 16,000 10 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 +		
shard Node Class Storage Space Nodes Parameter Tampiate Config Node Class	vcPU Memory • VcPU Memory • 2 vcPUs 8 08 • 2 vcPUs 16 08 • 4 vcPUs 16 08 • 4 vcPUs 12 08 • 8 vcPUs 64 08 • 8 vcPUs 64 08 • 16 vcPUs 64 08 • 17 vcPUs 64 08 • 16 vcPUs 64 08 • 17 vcPUs 64 08 • 18 vcPUs 64 08 • 18 vcPUs 64 08 • 18 vcPUs 64 08 • 19 vcPUs 64 08 • 19 vcPUs 64 08 • 10 vcPUs 64 08 • 1	Maximum Connections 2.000		
shard Node Class Storage Space Nodes Parameter Template Config Node Class Storage Space Parameter Template	vCPU Memory • VKP / Iduation • 2 vCPUs 8 08 • 2 vCPUs 16 08 • 4 vCPUs 16 08 • 4 vCPUs 12 08 • 8 vCPUs 64 08 • 16 vCPUs 64 08 • 17 vC • 17 vE vanthy ranges from 2 to 16. • 16 vLPUs 64 08 • 2 • 17 vE vanthy ranges from 2 to 16. • 16 vLPUs 64 08 • 2 vCPUs 64 08 <	Maximum Connections 2.000		
shard Node: Class	Understood 1.4-moliped View Praimateer Template vCPU Memory • • 2 vCPUs 8 0.8 • 2 vCPUs 10 0.8 • 4 vCPUs 10 0.8 • 4 vCPUs 10 0.8 • 4 vCPUs 10 0.8 • 8 vCPUs 64 0.8 • 8 vCPUs 64 0.8 • 8 vCPUs 64 0.8 • 9 vCPUs 64 0.8 • 7 vCPUs 64 0.8 • 9 vcPUs 64 0.8 • 10 vcPUs 64 0.8 <th>Maximum Connections 2.000 </th>	Maximum Connections 2.000		

Figura 6-1 Configuraciones básicas

Figura 6-2 Configuración del administrador

Administrator					
Password	Configure	Skip			
Administrator	rwuser				
Administrator Password			Ø	Keep your password secure. The system cannot retrieve your password.	
Confirm Password			Ø		

Figura 6-3 Red y duración requerida

Network		
VPC	default_vpc 🔹	C View VPC
	After the DDS instance is created, the VPC car	mot be changed.
Subnet	default_subnet(192.168.0.0/24) •	C View Subnet
	Available private IP addresses in the subnet: 227	
Security Group	Sys-default(b6f16cee-e859-47e2-a418 •	C View Security Group
	In a security group, rules that authorize connection	ns to D8 instances apply to all D8 instances associated with the security group.
SSL	View Details	
	▲ To encrypt transmission, enable SSL.	
Database Port	Default port: 8635	
Enterprise Project		
sitespine i rojuti		
Enterprise Project	Select	▼ C View Project Management ⑦

Figura 6-4 Configuración avanzada

Advanced Settings	
Automated Backup	0
Retention Period	- 7 + Enter an integer from 1 to 732.
Time Window	00.00 - 01:00 * GMT+08:00
Maintenance Window	Skip Configure 🕥
Tags	It is recommended that you use TMS's predefined tag function to add the same tags to different cloud resources. C View predefined tags
	Tag key Tag value
	You can add 20 more tags.

- 3. En la página mostrada, confirme los detalles de la instancia.
 - Para instancias anuales/mensuales
 - Si necesita modificar la configuración, haga clic en **Previous**.
 - Si no necesita modificar la configuración, lee y acepta el contrato de servicio y haga clic en Pay Now para ir a la página de pago y completar el pago.
 - Para instancias de pago por uso
 - Si necesita modificar la configuración, haga clic en **Previous**.
 - Si no necesita modificar la configuración, lee y acepta el contrato de servicio y haga clic en Submit para comenzar a crear la instancia.
- 4. Haga clic en **Back to Instance List**. Haga clic en **Back to Instance List**. Puede ver y gestionar la instancia de base de datos en la página **Instances**.
 - Cuando se crea una instancia de base de datos, el estado que se muestra en la columna Status es Creating. Este proceso dura unos 15 minutos. Una vez completada la creación, el estado cambia a Available.
 - Las instancias anuales/mensuales que se compraron en lotes tienen las mismas especificaciones, excepto el nombre y el ID de la instancia.
Paso 2: Comprar un ECS

- 1. Vaya a la página **Buy ECS**.
- 2. Configure los ajustes básicos y haga clic en **Next: Configure Network**. Mantenga la región y AZ del ECS iguales a los de la instancia DDS que se va a conectar.

Figura 6-5 Configuraciones básicas

Configure Basic Sett	tings (2) Configure Network	3 Configure Advanced Settings	(4) Confirm			
Biling Mode	Yearly/Monthly Pay-per-use	Spot price (2)				
Region	fon Oct Hong Kong •					
	For low network latency and quick resource access, s	elect the region nearest to your target users. L	earn how to select a region.			
AZ	Random AZ1	AZ2 ⑦				
C211 4	and Harrison (1)					
CPO Achiectare	Kanpeng					
Specifications	Latest generation • VCPUs A	Memory	All • Flav	or Name Q		
	General computing-plus General computin	ig Memory-optimized High-perfor	mance computing Ultra-high I/O	GPU-accelerated		
	Elizard Manua	of Rite L Manager (CB)	CPU JE	Assured / Maximum Bandwidth 🕥 🚛	Packets Per Second (PPS) ⑦ JE IPv6	
	Handi Haring	ACK OR LIMEIRON ACTION				
	c6.large.2	2 vCPUs 4 GIB	Intel Cascade Lake 3.0GHz	1.2 / 4 Gbit/s	400,000 Yes	
	c6large.2 c6large.4	2 vCPUs 4 GIB 2 vCPUs 8 GIB	Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz	1.2 / 4 Gbit/s 1.2 / 4 Gbit/s	400,000 Yes	
	c6large.2 c6klarge.2 c6klarge.2	2 vCPUs 4 GIB 2 vCPUs 4 GIB 2 vCPUs 8 GIB 4 vCPUs 8 GIB	Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz	1.2 / 4 Gbit/s 1.2 / 4 Gbit/s 2.4 / 8 Gbit/s	400,000 VHs 400,000 VHs 800,000 VHs	
	c6.large.2 c6.starge.4 c6.xtarge.4 c6.xtarge.4 c6.xtarge.4	2 vCPUs 4 GB 2 vCPUs 4 GB 2 vCPUs 8 GB 4 vCPUs 8 GB 4 vCPUs 8 GB 4 vCPUs 16 GB	Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz	1.2 / 4 Gbit/s 1.2 / 4 Gbit/s 2.4 / 8 Gbit/s 2.4 / 8 Gbit/s	400,000 Wes 400,000 Wes 800,000 Wes	
	e Skinge 2 e Skinge 2 e Skinge 4 e Skinge 2 e Skinge 2 e Skinge 2	2 VCPUs 4 GB 2 VCPUs 4 GB 2 VCPUs 8 GB 4 VCPUs 8 GB 4 VCPUs 8 GB 4 VCPUs 16 GB 8 VCPUs 16 GB	Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz	1.2 / 4 Gbit/s 1.2 / 4 Gbit/s 2.4 / 8 Gbit/s 2.4 / 8 Gbit/s 4.5 / 15 Gbit/s	400,000 We 400,000 We 400,000 We 400,000 We 1,000,000 We	
	ekiage2	2 vCPUs 4 cBit 2 vCPUs 4 cBit 2 vCPUs 4 cBit 4 vCPUs 8 cBit 4 vCPUs 8 cBit 4 vCPUs 16 cBit 8 vCPUs 16 cBit 8 vCPUs 16 cBit	Intel Cascade Lake 3.00Hz Intel Cascade Lake 3.00Hz	1 2 / 4 GbUs 1 2 / 4 GbUs 2 4 / 8 GbUs 2 4 / 8 GbUs 4 5 / 15 GbUs 4 5 / 15 GbUs	400,000 We 200,000 We 800,000 We 1.000,000 We 1.000,000 We	
	clurge1 clurge2 clurge3 c	2 x/CU (4 GB 2 x/CU (4 GB 4 x/CU (4 GB 4 x/CU (1 G GB 8 x/CU (1 G GB 8 x/CU (1 G GB 8 x/CU (1 G GB 8 x/CU (1 2 G GB 1 2 x/CU (2 G GB	Intel Cascade Lake 30GHz Intel Cascade Lake 30GHz	12/4 GM/s 12/4 GM/s 24/8 GM/s 24/8 GM/s 45/15 GM/s 45/15 GM/s 7/17 GM/s	440,000 We 440,000 We 460,000 We 1,000,000 We 1,000,000 We 2,000,000 We	

Figura 6-6 Selección de una imagen

image	Phátic mage Physite image Stared image Markelpiace image	
Host Security	Enable 🕥	
System Disk	Hgs 10 + GE 10PS limit 2,120, 10PS limit 5,000	¢
	Add Data Disk. You can attach 23 more disks.	Ģ
	Data disis addet to a Linux ECIS can be initialized using a vicant script.	
Quantity – 1	+ pro pro	work

3. Configure la información de red de ECS y haga clic en **Next: Configure Advanced Settings**. Mantenga la VPC y el grupo de seguridad del ECS igual que los de la instancia de DDS que se va a conectar.

Figura 6-7 Ajustes de red

< Elastic Cloud Se	Elastic Cloud Server							
(1) Configure Basic Settings	Configure Network	- (3) Configure Advanced S	Settings	frm				
Network	vpc-test01(192.168.0.0/16) Create VPC	• C subnet-lest01(19	12.168.0.0124) •	C Automatically assign IP address	 Available private IP 	addresses: 250 🕥		
Extension NIC	Edention NC O Add NC NCs you can util add 1							
Security Group	default/16663/28-10a2-4bc2-bc14-a4d5a Similar to a frewall, a security group logical Ensure that the selected security group alor Security Group Rules ^ Inbound Rules Outbound Rules	(b32844b)	C Create Security Group	 Image: Some state of the second second	ire Security Group Rules			
	Security Group Name	Priority	Action	Protocol & Port (?)	Type	Source (2)	Description	
		1	Permit	TCP: 8000	IPv4	0.0.0.00	-	
		1	Permit	TCP: 8635	IPv4	0.0.0.00	-	
		1	Permit	TCP: 8080	IPv4	0.0.0.00		
		1	Permit	UDP: 111	IPv4	0.0.0.00	Create by sfs turbo	
		4	Permit	TCP: 111	IPv4	0.0.0.00	Create by sfs turbo	

Figura 6-8 Selección de una EIP

EIP	Auto ass	ign 🔿 Us	e existing	○ Not re	quired 🥐					
EIP Type	D	ynamic BGP		:	Static BGP					
	⊘ Greater the second secon	Greater than or equal to 99.95% service availability rate								
Billed By	Bar For Billed based	ndwidth 🝁 heavy/stable f	iraffic irrespective o	of usage du	Traffic For light	/sharply fluc	tuating t bandwi	raffic dth size.		Shared bandwidth For staggered peak hours
andwidth Size	5	10	20	50	100	Custom	-	1	+	The bandwidth can be from 1 to 300 Mbit/s.
	⊙ Free Anti-	DDoS protecti	on							
Release Option	Release	with ECS 🤅)							

4. Configure la contraseña de ECS y haga clic en Next: Confirm.

Figura 6-9 Configuración avanzada

Configure Basic Settings -	Configure Network Gonfigure Advanced Settings (4) Confirm
ECS Name	Ecs-aba9 Allow duplicate name If you are creating multiple EC0s at the same time, automatic naming and customicable naming are available for you to select. To be a select.
Login Mode	Password Key pair Set password later
Username	root
Password	Keep the password secure. If you forget the password, you can log in to the ECS console and change it.
Confirm Password	&
Cloud Backup and Recovery	To use CBR, you need to purchase a backup valut. A vauit is a container that stores backups for servers. Create new Use existing Not required O
Cloud Eye	Enable Detailed Monitoring FIES ⑦ Called 1-minute fined-grained monitoring of ECS metrics, such as CPU, memory, network, disk, and process.
ECS Group (Optional)	Antradinaty ⑦ Select ECS group- C C C Comm

5. Confirme las configuraciones y haga clic en **Submit**.

Figura 6-10 Confirmación de las configuraciones

Configure Basic Set	tings (2) (Configure Network ——— ③ Configure Advanced Settings —	🙆 Confirm					
Configuration	Basic 🖉							
	Billing Mode	Pay-per-use	Region	Hong Kong		AZ	AZ2	
	Specifications System Disk	General computing-plus c6.large.2 2 vCPUs 4 GIB High I/O, 40 GIB	Image	CentOS 7.6 64bit		Host Security	Disabled	
	Network 🖉							
	VPC	default_vpc (192.168.0.0/16)	Security Group	default		Primary NIC	default_subnet (192.168.0.0/24)	
	EIP	Dynamic BGP Billed By: Traffic Bandwidth: 1 Mbit/s						
	Advanced 🖉							
	ECS Name	ecs-e5d6-test	Login Mode	Password		ECS Group	-	
Launch Template	Save as Launch	Template						
Enterprise Project	default	C Create Enterprise Projec	t (1)					
Quantity	- 1 +	You can create a maximum of 20 ECSs. Learn how to increase qu	ota.					
Agreement	I have read and	agree to the Service Level Agreement and Image Disclaimer.						
3CS Price	Price / hour + EP halls Price / K8 Privilia Solorit							

6. Consulta del ECS comprado.

Paso 3: Configurar reglas de grupo de seguridad

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en 💿 en la esquina superior izquierda y seleccione una región y un proyecto.

- **Paso 3** Haga clic en = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia. Se muestra la página Basic Information.
- **Paso 5** En el área Network Information de la página Basic Information, haga clic en el grupo de seguridad.

Figura 6-11 Grupo de seguridad

Network Information			
VPC	dds-st-test-vpc	Subnet	dds-st-test-subnet-2 (1)
Security Group	Sys-default 🖉	Database Port	8635 🖉

También puede elegir **Connections** en el panel de navegación de la izquierda. En la pestaña **Private Connection**, en el área **Security Group**, haga clic en el nombre del grupo de seguridad.

Figura 6-12 Grupo de seguridad

Security Group Security Group Add Rule Delete Inbound Rules(1) Outbound Rules	(1)	С
Protocol & Port ⑦	Source ⑦	Description
All	Sys-default	

- Paso 6 En la página Security Group, busque el grupo de seguridad de destino y haga clic en Manage Rule en la columna Operation.
- Paso 7 En la pestaña Inbound Rules, haga clic en Add Rule. Aparece el cuadro de diálogo Add Inbound Rule.
- Paso 8 Agregue una regla de grupo de seguridad como se le solicite.

Figura 6-13 Agregar regla de entrada

Add Inbound Rule Learn more about security group configuration.						
Inbound rules allow incoming traffic to instances associated with the security group.						
Security Group Sys-default You can import multiple rules in a batch	h.					
Protocol & Port ⑦	Туре	Source 🕐	Description	Operation		
TCP	IPv4 -	IP address 0.0.0.0/0	•	Operation 🗸		
↔ Add Rule						
OK Cancel						

Parámetro	Descripción	Valor de ejemplo
Priority	Prioridad de regla de grupo de seguridad. El valor de prioridad varía de 1 a 100. La prioridad predeterminada es 1 y tiene la prioridad más alta. La regla de grupo de seguridad con un valor menor tiene mayor prioridad.	1
Action	Las acciones de la regla del grupo de seguridad. Las reglas de denegación tienen prioridad sobre las reglas de permiso de la misma prioridad.	Allow
Protocol & Port	El protocolo de red requerido para el acceso. Opciones disponibles: TCP, UDP, ICMP, o GRE	ТСР
	Puerto: el puerto en el que desea permitir el acceso a DDS. El puerto predeterminado es 8635. El puerto oscila entre 2100 y 9500 o puede ser 27017, 27018, o 27019.	8635
Туре	Tipo de dirección IP. Solo IPv4 y IPv6 son compatibles.	IPv4
Source	 Especifica la dirección IP, el grupo de seguridad y el grupo de direcciones IP compatibles, que permiten el acceso desde direcciones IP o instancias de otros grupos de seguridad. Ejemplo: Dirección IP única: 192.168.10.10/32 Segmento de dirección IP: 192.168.1.0/24 Todas las direcciones IP: 0.0.0.0/0 Grupo de seguridad: sg-abc Grupo de direcciones IP: ipGroup-test Si introduce un grupo de seguridad, todos los ECS asociados al grupo de seguridad cumplen con la regla creada. Para obtener más información acerca de los grupos de direcciones IP, consulte Descripción general del grupo de 	0.0.0/0

Tabla 6-1 Configuración de reglas entrantes

Parámetro	Descripción	Valor de ejemplo
Description	(Opcional) Proporciona información adicional acerca de la regla del grupo de seguridad.	-
	La descripción puede contener un máximo de 255 caracteres y no puede contener corchetes angulares (< o >).	

Paso 9 Haga clic en OK.

----Fin

Paso 4: Conectarse a una instancia de clúster DDS mediante Mongo Shell

- Conexión SSL
- Paso 1 Inicie sesión en la consola de gestión.
- **Paso 2** Haga clic en 🔍 en la esquina superior izquierda y seleccione una región y un proyecto.
- **Paso 3** Haga clic en = en la esquina superior izquierda de la página y elija **Databases** > **Document Database Service**.
- Paso 4 En la página Instances, haga clic en el nombre de la instancia.
- Paso 5 En el panel de navegación de la izquierda, elija Connections.
- Paso 6 En el área Basic Information, haga clic en 📥 junto al campo SSL.
- Paso 7 Cargue el certificado raíz al ECS para conectarse a la instancia.

A continuación se describe cómo cargar el certificado en un ECS de Linux y Windows:

• En Linux, ejecute el siguiente comando:

scp

```
<IDENTITY_FILE><REMOTE_USER>@<REMOTE_ADDRESS>:<REMOTE_DIR>
```

D NOTA

- IDENTITY_FILE es el directorio donde reside el certificado raíz. El permiso de acceso al archivo es 600.
- **REMOTE_USER** es el usuario del sistema operativo de ECS.
- **REMOTE_ADDRESS** es la dirección de ECS.
- **REMOTE_DIR** es el directorio del ECS al que se carga el certificado raíz.
- En Windows, cargue el certificado raíz mediante una herramienta de conexión remota.
- Paso 8 Conéctese a la instancia en el directorio donde se encuentra el cliente MongoDB.

Método 1: Uso de la dirección de conexión HA privada (recomendado)

DDS proporciona una dirección de conexión HA privada que consiste en direcciones IP y puertos de todos los nodos mongos en una instancia de clúster. Puede utilizar esta dirección para conectarse a la instancia de clúster para mejorar la disponibilidad de la instancia de clúster.

Comando:

```
./mongo <Private HA connection address> --ssl --sslCAFile <FILE_PATH> --
sslAllowInvalidHostnames
```

Descripción de parámetros:

• Private HA Connection Address: En la página Instances, haga clic en el nombre de la instancia. Se muestra la página Basic Information. Elija Connections. Haga clic en la pestaña Private Connection y obtenga la dirección de conexión de la instancia actual en el campo Private HA Connection Address.

Figura 6-14 Obtención de la dirección de conexión HA privada

vate Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	· ⊥	Subnet	dds-st-test-subnet-2 ()
Auto-switch Private IP Address			
Address			
Cross-CIDR Access	Disabled Enable		
Private HA Connection	Address mongodb://rwuser: <password>@"</password>		/test?authSource=admin&replicaSet=replica 🗖 Learn more

El formato de la dirección de conexión HA privada es el siguiente. El nombre de usuario de la base de datos **rwuser** y la base de datos de autenticación **admin** no se pueden cambiar.

mongodb://**rwuser:**<*password*>@192.168.xx.xx:8635,192.168.xx.xx:8635/**test? authSource=admin**

La siguiente tabla muestra los parámetros requeridos en la dirección de HA privada.

Parámetro	Descripción			
rwuser	Nombre de usuario de la base de datos			
<password></password>	Contraseña para el nombre de usuario de la base de datos. Reemplácelo con la contraseña real.			
	Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.			
	Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25*** %21%24.			
192.168.xx.xx:8635,192.1 68.xx.xx:8635	Dirección IP y puerto del nodo mongos de la instancia de clúster que se va a conectar			

Tabla 6-2 Información de parámetros

Parámetro	Descripción
test	El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.
authSource=admin	La base de datos de autenticación del usuario rwuser debe ser admin . authSource=admin está fijo en el comando.

- FILE_PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: Para asegurarse de que la comunicación interna del clúster no ocupe recursos como la dirección IP del usuario y el ancho de banda, el certificado del clúster se genera mediante la dirección IP de gestión interna. -sslAllowInvalidHostnames es necesario para la conexión SSL a través de una red privada.

Ejemplo de comandos:

./mongo mongodb://rwuser:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/test? authSource=admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames

Método 2: Uso de la dirección de conexión HA privada (base de datos y cuenta definidas por el usuario)

Comando:

./mongo <*Private HA connection address*> --ssl --sslCAFile <*FILE_PATH*> -sslAllowInvalidHostnames

Descripción de parámetros:

Private HA Connection Address: En la página Instances, haga clic en el nombre de la instancia. Se muestra la página Basic Information. Elija Connections. Haga clic en la pestaña Private Connection y obtenga la dirección de conexión de la instancia actual en el campo Private HA Connection Address.

Figura 6-15 Obtención de la dirección de conexión HA privada

rivate Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	Ť	Subnet	dds-st-test-subnet-2 ()
Auto-switch Private IF Address			
Address			
Cross-CIDR Access	Disabled Enable		
Private HA Connection	n Address mongodb://rwuser: <password>@1</password>		/test?authSource=admin&replicaSet=replica 🗇 Learn more

El formato de la dirección de conexión HA privada obtenida es el siguiente: mongodb://rwuser:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/test? authSource=admin La siguiente tabla muestra los parámetros requeridos en la dirección de HA privada.

Parámetro	Descripción
rwuser	Nombre de usuario de base de datos. El valor predeterminado es rwuser . Puede cambiar el valor por el nombre de usuario en función de sus requisitos de servicio.
<password></password>	Contraseña para el nombre de usuario de la base de datos. Reemplácelo con la contraseña real.
	Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.
	Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25*** %21%24.
192.168.xx.xx:8635,192.1 68.xx.xx:8635	Dirección IP y puerto del nodo mongos de la instancia de clúster que se va a conectar
test	El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.
authSource=admin	La base de datos de autenticación de usuario rwuser es admin .
	NOTA Si utiliza una base de datos definida por el usuario para la autenticación, cambie la base de datos de autenticación en la dirección de conexión HA por el nombre de la base de datos definida por el usuario. Además, reemplace rwuser con el nombre de usuario creado en la base de datos definida por el usuario.

Tabla 6-3	Inform	nación	de	parámetros
-----------	--------	--------	----	------------

- FILE PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: Para asegurarse de que la comunicación interna del clúster no ocupe recursos como la dirección IP del usuario y el ancho de banda, el certificado del clúster se genera mediante la dirección IP de gestión interna. -sslAllowInvalidHostnames es necesario para la conexión SSL a través de una red privada.

Por ejemplo, si crea una base de datos definida por el usuario **Database** y un usuario **test1** en la base de datos, el comando de conexión es el siguiente:

./mongo mongodb://test1:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/Database? authSource=Database --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames

Método 3: Usar una dirección IP privada

Comando:

./mongo --host <DB_HOST> --port <DB_PORT> -u <DB_USER> -p -authenticationDatabase admin --ssl --sslCAFile <FILE_PATH> -sslAllowInvalidHostnames

Descripción de parámetros:

• **DB_HOST** es la dirección IP del nodo mongos de la instancia de clúster que se va a conectar.

Haga clic en el nombre de la instancia. En la página **Basic Information**, elija **Connections** > **Private Connection**, obtenga la dirección IP privada del nodo mongos en la pestaña **mongos** en el área **Node Information**.

Figura 6-16 Obtención de la dirección IP privada

sic Informatio	n					
tabase Port	8635 🖉		١	/PC	dds-st-test-vpc	
L		Ŧ	2	Subnet	dds-st-test-subnet-2 ()	
ddress						
ivate HA Connec	tion Address	mongodb://rwuser: <password< td=""><td>d>@</td><td></td><td>test?authSource=admin 🗇 Learn more</td><td></td></password<>	d>@		test?authSource=admin 🗇 Learn more	
		Note The parameters in or	range are variables and nee	ed to be modified i	based on service requirements. For details, click Learn	more.
ode Information	on ihard con	Note The parameters in or	range are variables and nee	ed to be modified b	based on service requirements. For details, click Learn	more.
ode Information	on ihard con AZ	Note The parameters in or fig	range are variables and nee	ed to be modified b	oased on service requirements. For details, click Learn	more.
Name/ID dds-c582_xwx	on hard con AZ az2	Note The parameters in or fig Private IP Address 192.	Private Domain Name	EIP S Unbound	Operation Change Private IP Address More +	more.

• **DB_PORT** es el puerto de la instancia que se va a conectar. El puerto predeterminado es 8635.

Haga clic en el nombre de la instancia. En la página **Basic Information**, elija **Connections**. En la pestaña **Private Connection**, obtenga la información del puerto de la base de datos en el campo **Database Port** en el área **Basic Information**.

Figura 6-17 Obtención del puerto

Private Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	→	Subnet	dds-st-test-subnet ()

- **DB USER** es el usuario de la base de datos. El valor predeterminado es **rwuser**.
- FILE_PATH es la ruta para almacenar el certificado raíz.
- --sslAllowInvalidHostnames: Para asegurarse de que la comunicación interna del clúster no ocupe recursos como la dirección IP del usuario y el ancho de banda, el certificado del clúster se genera mediante la dirección IP de gestión interna. --

sslAllowInvalidHostnames es necesario para la conexión SSL a través de una red privada.

Introduzca la contraseña de la cuenta de la base de datos si se solicita la siguiente información:

Enter password:

Ejemplo de comandos:

./mongo --host 192.168.1.6 --port 8635 -u rwuser -p --authenticationDatabase admin --ssl --sslCAFile /tmp/ca.crt --sslAllowInvalidHostnames

Paso 9 Compruebe el resultado de la conexión. Si se muestra la siguiente información, la conexión se realiza correctamente.

mongos>

----Fin

- Conexión sin cifrar
- Paso 1 Conéctese al ECS.
- Paso 2 Conéctese a la instancia en el directorio donde se encuentra el cliente MongoDB.

Método 1: Uso de la dirección de conexión HA privada (recomendado)

Comando:

./mongo "<Private HA Connection Address>"

Private HA Connection Address: En la página **Instances**, haga clic en el nombre de la instancia. Se muestra la página **Basic Information**. Elija **Connections**. Haga clic en la pestaña **Private Connection** y obtenga la dirección de conexión de la instancia actual en el campo **Private HA Connection Address**.

Figura 6-18 Obtención de la dirección de conexión HA privada

ivate Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	▲	Subnet	dds-st-test-subnet-2 ()
Auto-switch Private IP Address			
Address			
Cross-CIDR Access	Disabled Enable		
Private HA Connection	Address mongodb://rwuser: <password>@</password>	/	test?authSource=admin&replicaSet=replica 🗖 Learn more

El formato de la dirección de conexión HA privada es el siguiente. El nombre de usuario de la base de datos **rwuser** y la base de datos de autenticación **admin** no se pueden cambiar.

mongodb://**rwuser:**<*password*>@192.168.xx.xx:8635,192.168.xx.xx:8635/**test? authSource=admin**

La siguiente tabla muestra los parámetros requeridos en la dirección de HA privada.

Parámetro	Descripción
rwuser	Nombre de usuario de base de datos.
<password></password>	Contraseña para el nombre de usuario de la base de datos. Reemplácelo con la contraseña real. Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente. Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25***%21%24.
192.168.xx.xx:8635,192.168 .xx.xx:8635	Direcciones IP y puertos de los nodos mongos de la instancia de clúster que se va a conectar.
test	El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.
authSource=admin	La base de datos de autenticación del usuario rwuser debe ser admin . authSource=admin está fijo en el comando.

Tabla 6-4	Información	de 1	parámetros
-----------	-------------	------	------------

Ejemplo de comandos:

./mongo mongodb://rwuser:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/test? authSource=admin

Método 2: Uso de la dirección de conexión HA privada (base de datos y cuenta definidas por el usuario)

Comando:

./mongo "<Private HA Connection Address>"

Private HA Connection Address: En la página **Instances**, haga clic en el nombre de la instancia. Se muestra la página **Basic Information**. Elija **Connections**. Haga clic en la pestaña **Private Connection** y obtenga la dirección de conexión de la instancia actual en el campo **Private HA Connection Address**.

Figura 6-19 Obtención de la dirección de conexión HA privada

ivate Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	Ū ∓	Subnet	dds-st-test-subnet-2 ()
Auto-switch Private IP Address			
Address			
Cross-CIDR Access	Disabled Enable		
Private HA Connection	Address mongodb://rwuser: <password>@</password>		/test?authSource=admin&replicaSet=replica 🗇 Learn more

El formato de la dirección de conexión HA privada obtenida es el siguiente:

mongodb://**rwuser:**<*password*>@192.168.xx.xx:8635,192.168.xx.xx:8635/**test? authSource=admin**

La siguiente tabla muestra los parámetros requeridos en la dirección de HA privada.

Descripción
Nombre de usuario de base de datos. El valor predeterminado es rwuser . Puede cambiar el valor por el nombre de usuario en función de sus requisitos de servicio.
Contraseña para el nombre de usuario de la base de datos. Reemplácelo con la contraseña real.
Si la contraseña contiene signos (@), signos de exclamación (!), signos de dólar o signos de porcentaje (%), reemplácelos con códigos URL hexadecimales (ASCII) %40, %21, %24 y %25 respectivamente.
Por ejemplo, si la contraseña es ****@%***!\$, el código URL correspondiente es ****%40%25***%21%24 .
Direcciones IP y puertos de los nodos mongos de la instancia de clúster que se va a conectar.
El nombre de la base de datos de prueba. Puede establecer este parámetro en función de sus requisitos de servicio.
La base de datos de autenticación de usuario rwuser es admin . NOTA Si utiliza una base de datos definida por el usuario para la autenticación, cambie la base de datos de autenticación en la dirección de conexión HA por el nombre de la base de datos definida por el usuario. Además, reemplace rwuser con el nombre

Por ejemplo, si crea una base de datos definida por el usuario **Database** y un usuario **test1** en la base de datos, el comando de conexión es el siguiente:

./mongo mongodb://test1:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/Database? authSource=Database

Método 3: Usar una dirección IP privada

Comando:

./mongo --host <*DB_HOST*> --port <*DB_PORT*> -u <*DB_USER*> -p -authenticationDatabase admin

Descripción de parámetros:

• **DB_HOST** es la dirección IP del nodo mongos de la instancia de clúster que se va a conectar.

Haga clic en el nombre de la instancia. En la página **Basic Information**, elija **Connections** > **Private Connection**, obtenga la dirección IP privada del nodo mongos en la pestaña **mongos** en el área **Node Information**.

Basic Information	n											
Database Port	8635 🖉	•	N	/PC	dds-st-test-vpc							
SSL		Ŧ	5	Subnet	dds-st-test-subnet-2 ()							
Address												
Private HA Connect	tion Address	nongodb://rwuser: <passwo< td=""><td>rd>@</td><td></td><td>test?authSource=admin 🗖 Learn more</td><td colspan="7">Drivite H& Connection Address</td></passwo<>	rd>@		test?authSource=admin 🗖 Learn more	Drivite H& Connection Address						
		Note The parameters in the par	orange are variables and nee	ed to be modified	based on service requirements. For details, click Learn	more.						
Node Informatio	n hard con	Note The parameters in o	orange are variables and nee	ed to be modified	based on service requirements. For details, click Learn	more.						
Node Informatio	n hard con AZ	Note The parameters in o	Private Domain Name	ed to be modified	based on service requirements. For details, click Learn Operation	more.						
Node Informatio mongos sl Name/ID dds-c582_xwx	n hard con AZ az2	Note The parameters in o	Private Domain Name b382774b302b46608	EIP	Describer of the service requirements. For details, click Learn Operation Change Private IP Address More +	more.						

Figura 6-20 Obtención de la dirección IP privada

• **DB_PORT** es el puerto de la instancia que se va a conectar. El puerto predeterminado es 8635.

Haga clic en el nombre de la instancia. En la página **Basic Information**, elija **Connections**. En la pestaña **Private Connection**, obtenga la información del puerto de la base de datos en el campo **Database Port** en el área **Basic Information**.

Figura 6-21 Obtención del puerto

Private Connection	Public Connection				
Basic Information					
Database Port	8635 🖉	VPC		dds-st-test-vpc	
SSL	Ť	Subne	t	dds-st-test-subnet ()	

• **DB_USER** es el usuario de la base de datos. El valor predeterminado es **rwuser**.

Introduzca la contraseña de la cuenta de la base de datos si se solicita la siguiente información: Enter password:

Lincer pubbword.

Ejemplo de comandos:

./mongo --host 192.168.1.6 --port 8635 -u rwuser -p --authenticationDatabase admin

Paso 3 Compruebe el resultado de la conexión. Si se muestra la siguiente información, la conexión se realiza correctamente.

mongos>

----Fin

Paso 5: Crear una base de datos y escribir datos en la base de datos

Paso 1 Crear una base de datos.

use dbname

dbname: indica el nombre de la base de datos que se va a crear.

Figura 6-22 Creación de una base de datos

replica:P	PRIM	1ARY	` >	use	test001	
switched	to	db	te	st00	1	

Paso 2 Después de crear una base de datos, inserte datos en la base de datos para que pueda ver la base de datos en la lista de bases de datos.

Figura 6-23 Inserción de datos



NOTA

Hay tres bases de datos del sistema creadas por defecto: **admin**, **local** y **test**. Si inserta datos directamente sin crear una base de datos, los datos se insertan en la base de datos **test** de forma predeterminada.

Figura 6-24 Consulta de la base de datos

replica	a:PRIMARY>	show	dbs	
admin	0.000GB			
local	0.004GB			
test	0.000GB			

Paso 3 Ver datos en la base de datos.

Figura 6-25 Consulta de datos

```
replica:PRIMARY> show collections
user
replica:PRIMARY> db.user.find()
{ "_id" : ObjectId("5da1880d2b4ccf2e1163ad1d"), "key1" : "value1" }
```

----Fin

6.2 Conexión a una instancia DDS a través de una EIP

Esta sección utiliza una instancia de conjunto de réplicas DDS y un sistema operativo Windows como ejemplo para describir cómo comprar una instancia DDS, vincular una EIP, establecer un grupo de seguridad y conectarse a la instancia DDS mediante la herramienta Robo 3T en su entorno local. Los procedimientos son los siguientes:

- Paso 1: Comprar una instancia de base de datos
- Paso 2: Enlazar una EIP
- Paso 3: Configurar un grupo de seguridad
- Paso 4: Conectarse a una instancia DDS

Step 1: Buy a DB Instance

- 1. Vaya a la página Custom Config.
- 2. En la página mostrada, seleccione un modo de facturación y configure la información sobre su instancia de base de datos. A continuación, haga clic en **Next**.



Figura 6-26 Configuraciones básicas

Figura 6-27 Configuración del administrador

Administrator			
Password	Configure	Skip	
Administrator	rwuser		
Administrator Password		<i>i</i> e	keep your password secure. The system cannot retrieve your password.
Confirm Password		Q	

Figura 6-28 Red, duración requerida y cantidad

Network	
VPC	default_vpc C View VPC
	After the DDS Instance is created, the VPC cannot be changed.
Subnet	default_subnet C View Subnet
	Available private IP addresses In the subnet: 245
Security Group	default(69c7b525-4e6c-428a-b565-c6d 🔻 C View Security Group
	In a security group, rules that authorize connections to DB instances apply to all DB instances associated with the security group.
SSL	View Details ⑦
	▲ To encrypt transmission, enable SSL.
Database Port	Default port: 8635
Cross-CIDR Access	Configure Skip
	Only configure cross-CIDR access if the CIDR blocks of the client and the replica set instance are different. For example, if the client CIDR block is 192.168.0.0/
	the replica set instance.
Enterprise Project	
Enterprise Project	Select View Project Management ⑦
Required Duration and Quantit	ty
Required Duration	1 2 3 4 5 6 7 8 9 months 1 year
	Auto-renew Deduction rule and Renewal duration
Quantity	- 1 + 🕅 You can create 50 more DB instances. Increase Quota

Figura 6-29 Configuración avanzada

Advanced Settings		
Replica Set Parameter Template	Default-DDS-4.0-Replica 💌	C View Parameter Template
Show Original Log	0	
Automated Backup	0	
Retention Period	- 7 + Enter an integer from 1 to 732	2.
Time Window	00:00 - 01:00 -	GMT+08:00
Maintenance Window	Skip Configure	0
Tags	It is recommended that you use TMS's predefined tag function t	to add the same tags to different cloud resources. C $\;$ View predefined tags
	Tag key Tag value	
	You can add 20 more tags	

- 3. En la página mostrada, confirme los detalles de la instancia.
 - Para instancias anuales/mensuales
 - Si necesita modificar las especificaciones, haga clic en **Previous** para volver a la página anterior.

- Si no necesita modificar las especificaciones, lea y acepte el contrato de servicio y haga clic en Pay Now para ir a la página de pago y completar el pago.
- Para instancias de pago por uso
 - Si necesita modificar las especificaciones, haga clic en **Previous** para volver a la página anterior.
 - Si no necesita modificar las especificaciones, lea y acepte el contrato de servicio y haga clic en Submit para comenzar a crear la instancia.
- 4. Haga clic en **Back to Instance List**. Después de crear una instancia DDS, puede ver y gestionarla en la página **Instances**.
 - Cuando se crea una instancia, el estado que se muestra en la columna Status es Creating. Este proceso dura unos 15 minutos. Una vez completada la creación, el estado cambia a Available.
 - Las instancias anuales/mensuales que se compraron en lotes tienen las mismas especificaciones, excepto el nombre y el ID de la instancia.

Paso 2: Enlazar una EIP

- 1. Inicie sesión en la consola de gestión.
- 2. Haga clic en 🔍 en la esquina superior izquierda y seleccione una región y un proyecto.
- 3. Haga clic en = en la esquina superior izquierda de la página y elija Databases > Document Database Service.
- 4. En la página **Instances**, haga clic en la instancia. Se muestra la página **Basic Information**.
- 5. En el área **Node Information**, busque la fila que contiene el nodo principal y haga clic en **Bind EIP**.
- 6. En el cuadro de diálogo que aparece, seleccione la EIP adquirido y haga clic en **OK**. Si no hay EIP disponible, **asigne una EIP**.
- 7. Después de que la vinculación se haya realizado correctamente, vea la EIP en el área **Node Information**.

Paso 3: Configurar un grupo de seguridad

- 1. En el área **Network Information** de la página **Basic Information**, compruebe el puerto de base de datos de la instancia de base de datos.
- 2. En el área Network Information, haga clic en el nombre del grupo de seguridad.
- 3. En la página Security Groups, haga clic en el nombre del grupo de seguridad.
- 4. Haga clic en la pestaña **Inbound Rules** y haga clic en **Add Rule**. En el cuadro de diálogo que se muestra, agregue una regla de entrada para el puerto de la base de datos.

Paso 4: Conectarse a una instancia DDS

1. Acceda a la dirección de descarga de Robo 3T https://robomongo.org/download y haga clic en Download Studio 3T Free Today.

Figura 6-30 Página de descarga



2. En el cuadro de diálogo que aparece, introduzca la información requerida y haga clic en **Download Studio 3T for Windows** para descargar **studio-3t-x64.zip**.

Figura 6-31 Descarga de Robo 3T

77 3T	TOOLS - SOLUTIONS RESOURCES - CONTACT US - STORE - MY LICENSE DOWNLOAD Q
	Download Studio 3T Free Serving the global developer community since 2014. Download Studio 3T for Windows Other platforms

- 3. Descomprima el paquete descargado y haga doble clic en el archivo **studio-3t-x64.exe** en el directorio descomprimido para iniciar la instalación.
- Una vez completada la instalación, inicie la herramienta, como se muestra en Figura 6-32.

Figura 6-32 Ventana principal

Studio 3T for MongoDB - Full product trial File Edit Database Collection Index Document GridFS V	iew Help	- 0 ×
Connect Collection IntelliShell SQL Aggregate	🂱 🗍 🚱 🕌 🔚 🔚 🖓 🚱 🍾 🤱 🍡 Agp-Reduce Compare Schema Reschema Tasks Export Import Data Masking SQL Migration Users Roles	Feedback
Search Open Connections (Ctrl+F) aA < Quic	otart	
	Connection Manager X	^
	New Connection New Group Edit Delete Clone Import Export To URI marter. Get a Click here to filter connections 0 matches 0 matches 0 <	
	Name DB Server Security Last Accessed Shortcut	
	i automate common tas	iks.
	Show on startup	
	eip and Learning	
	Quick Options	
	Theme (requires restart): Same as system Show What's New tab after updating Studio 3T	
Operation:	Automatically open Connection Manager at startup Automatically open Connection Manager at startup Studio 3T features Studio 3T tips and tricks	~
operations	Li Enable Session Restore	

5. En la página Connection Manager, haga clic en New Connection.

<	Quickstart										
	[~]	
	-	Connection iv	lanager						^		
		New Connection	New Group	Edit Delete	Clone		Export				
	L	Click here to filte	r connections		- 1			_	0 matches	marter. Get a	
	Í	Name	🔁 New Connection					-	o x		
			If you have a connect can paste it here and Paste your connect	ction string (<u>SRV (</u> d Studio 3T will a ction string (SRV	<u>or standard</u>), uto-configure or standard)	e.g. for <u>you</u> your conne here:	<u>ir Mongol</u> ection sett	<u>DB Atlas</u> dep ings for you	oloyment, you	automate common tasks.	
			O Manually configur	re my connection	settings						
		Show on star									
								Next	Cancel		
		Quick C	ptions					Getting sta Knowledge	arted e base	-	
		Theme (requ	uires restart): Same as	system 🗸				Free Mong	oDB courses		
		Show V	Vhat's New tab after up	dating Studio 3T				Join the 3T	community		
		🗹 Automa	atically open Connection	n Manager at star	tup		P	Studio 3T 1	features		
^		Enable	Session Restore				P	Studio 3T 1	tips and tricks		

Figura 6-33 Administrador de conexiones

- 6. Conéctese a una instancia de base de datos de forma automática o manual.
 - Método 1: Conectarse a una instancia de base de datos automáticamente.
 - i. En el cuadro de diálogo que se muestra, escriba el URI, reemplace <password> y haga clic en Next.

NOTA

Cómo obtener el URI:

En la página **Instances**, haga clic en el nombre de la instancia de base de datos de destino. En la página **Basic Information**, haga clic en **Connections**. En el área **Public Connection**, obtenga la dirección de conexión pública de **Address**.

Figura 6-34 Ingresar el URI

File Edit Database Collection Index Document Grid	S View Help	
Connect Collection IntelliShell SQL Aggregat	e Map-Reduce Compare Schema Reschema Tasks Exp	The second secon
Search Open Connections (Ctrl+F)	Quickstart Wolconnection to Ctudio T Kyou have a connection string (SNV or standard), e.g. for your M Kyou have a connection string (SNV or standard) here: URI: mongodb//rwusen-password-@10.154.218.108655/ref Manually configure my connection settings Create a free Mongo0B cluster in the cloud	27 Full product trial accord Adds deployment, you in settings for you. struct that helps you automate common tasks. Task Manager Task Manager Task Manager Task Manager Task Manager Task Manager Task Manager Task Manager
Outpins 3 a	Quick Options Theme (requires restart): <u>Same as system v</u> S show What's New tab after updating Studie 3T Automatically open Connection Manager at startup Enable Session Restore	Getting started Consequences Free MangoDB courses Consequences Studio 31 features Studio

ii. En la pestaña Server, haga clic en OK en el cuadro de diálogo mostrado.

Figura 6-35 Servidor

onnect Collection IntelliShell	© • SQL Aggregate	Connection name: Connection group: contextent level>	Migration Users Roles Feedback
arch Oper Generations (CM+F) [[] propins are replica) [direct] 2] are constant 2] bbb 2] bbb 2] bbb 2] constant 2] bbb 2] constant 2] bbc 2] constant 2] beat 3] beat 3] beat 5]	aA < Qui	Server Authentication 551 SSH Provy IntelliShel MongoDB Tools Advanced Connection Type: Standatione Server: [10154.218.10 Port: 8835 Advanced V Vour connection has been successfully auto-configured. OK	JCT Trial re that helps you automate common tasks. R Manager new task Learning
		Read-Only Lock From URL. Use this option to import connection details from a connection string / URI To URL. Use this option to export complete connection details to a connection string / URI	rted base DB courses community eatures

iii. Haga clic en la pestaña Authentication.

Figura 6-36 Autenticación

Studio 3T for MongoDB - Full product trial	ment GridES	a New Connection	×	- 0	×			
Connect Collection IntelliShell SQL	Aggregate	Connection name: Connection group: <root level=""></root>		🖅 - 🏖 💽 🖃 Migration Users Roles Feedback				
Search Open Connections (Ctrl+F)	aA < Qui	Server Authentication SSL SSH Proxy IntelliShell MongoDB Too	xls Advanced					
▼ Fig. (replica set: replica) (direct) > □ aaa > □ bbb > □ bbb > □ ccc > □ local > □ local		Authentication Mode: Lagacy (SCRAM-SH4-1) Yoo have chosen an authentication method which might make your Monpool Poese refer to the <u>Monocold Social</u> : Checkling to hild server your debatevel User name: Password:	instance vulnerable to attacks.	ıct trial	^			
)		Authentication DB: admin The database where the user is defined		e that helps you automate common tasks. k Manager new task				
		Always show the authentication database of the user account Mays about all databases and collections defined in roles of the use Manually its additional wibide databases by their names. Databases: admin.text Databases visible for non-admin users (comma-separated)	ar account	Learning had base b08 courses community sturge				
Operations	" ^	Test Connection	Save Cancel	ower User manual: hidden gems that will	~			
安全组	dds-st-test-secur	ty-group Z		ART2C CONVIGUO BY	205			

iv. Haga clic en **Test Connection** para comprobar si la conexión se realiza correctamente.

Figura 6-37 Conexión de prueba

onnect Collection IntelliShell SQL Aggregate	Connection Connection	n name: n group: <root level=""></root>		~	Migration -	Lusers 1	Roles Feedb) Dack
earch Open Connections (Ctrl+F) AA < C [5] [replica set: replica] [direct] > () asa > () abb > () bbb	ui Server A Authentie You have Please ret	unthentication SSL SSH Proxy IntelliShell MongoDB To Connecting Testing connection	ols Advanced	ecks.	Jct tri	al		
2 ⊜ordig 2 ⊜ord 2 ∃ret 2 ∃ret 2 ⇒ text001	User nar Passwori Authentic	Operation Initializing connection Connecting to server Authenticating as runser Reading server status from connection Detecting accessible databases Detecting MongoDB server version Detecting MongoDB server feature compatibility version Connected	Status OK OK		re that helps ye k Manager new task	ou automate c	ommon tasks.	
	☑ Alway ☑ Alway ☑ Manui Database	Hide details OK ey an advancer trans- businesser by their tables ex (admin.text Databases visible for non-admin users (comma-separated	Cancel		Learning rted base oDB courses community eatures ips and tricks			

v. Haga clic en la pestaña SSL y seleccione Use SSL protocol to connect.

NOTA

Si la encriptación de datos SSL está deshabilitado, omita este paso y vaya a 6.viii.

Figura 6-38 SSL

New Connection		×								
Connection name:] 📕								
Connection group: <root level=""></root>	~]								
Server Authentication SSL SSH Proxy IntelliShell MongoDB Tools Adv	vanced									
<u> </u>										
○ Use own <u>R</u> oot CA file (sslCAFile)										
	[Q	1								
Accept server SSL certificates trusted by the <u>operating system</u>										
Client Certificate (ssiPEWiKeyFile)		8								
Passphrase:		8								
☑ My client certificate is not protected by a passphrase										
Select SSL/TLS: TLS	~ 🔒									
Allow invalid hostnames (sslAllowInvalidHostnames)										
Use Server Name Indication (Advanced)										
SNI Host Name:										
Iest Connection	ave Cance	I								

vi. Seleccione Use own Root CA file (--sslCAFile), importe el certificado y seleccione Allow invalid hostnames.

NOTA

Descargue el certificado SSL y verifique el certificado antes de conectarse a las bases de datos.

En la página Instances, haga clic en el nombre de la instancia de base de datos de

destino. En el área **DB Information** de la página **Basic Information**, haga clic en en el campo **SSL** para descargar el certificado raíz o el paquete de certificados.

Figura 6-39	Introducir	informació	n SSL
-------------	------------	------------	-------

on SSL SSH Proxy IntelliShell MongoDB Tools Advanced I to connect A file (sslCAFile) Image: Connect of the second	Server Authentication SSL SSH Proxy IntelliShell MongoDB Tools Advanced Use SSL protocol to connect Image: SSL SSL SSL SSL SSL SSL SSL SSL SSL SS	cation SSL SSH Proxy IntelliShell MongoDB Tools Advanced bool to connect t Cate is not protected by a passphrase Image: Cate is not protected by a passphrase Image: Cate is not protected by a passphrase Image: Cate is not protected by a passphrase
I to connect A file (ssICAFile) Control (Use SSL protocol to connect Image: SSL protocol to connect Ima	bccl to connect t CA file (sslCAFile) C file (sslCAFile) SSL certificates trusted by the operating system rver SSL certificates tificate (sslPEMKeyFile) ficate is not protected by a passphrase TLS
A file (sslCAFile) L certificates trusted by the operating system r SSL certificates cate (sslPEMKeyFile) ste is not protected by a passphrase	Use own Root CA file (sslCAFile) C:\Users\Downloads\ca.crt Accept server SSL certificates trusted by the operating system Accept any server SSL certificates Use Client Certificate (sslPEMKeyFile) Client Certificate: Passphrase: My client certificate is not protected by a passphrase Select SSL/TLS: TLS	t CA file (ssICAFile) SSL certificates trusted by the operating system rver SSL certificates tificate (ssIPEMKeyFile) ficate is not protected by a passphrase TLS
L certificates trusted by the operating system r SSL certificates cate (sslPEMKeyFile) te is not protected by a passphrase	C:\Users\Downloads\ca.crt Accept server SSL certificates trusted by the operating system Accept any server SSL certificates Use Client Certificate (sslPEMKeyFile) Client Certificate: Passphrase: My client certificate is not protected by a passphrase Select SSL/TLS: TLS	Downloads\ca.crt Image: Comparison of the operating system SSL certificates rver SSL certificates tificate (sslPEMKeyFile) Image: Comparison of the operating of the operating system inficate is not protected by a passphrase Image: Comparison of the operating system TLS Image: Comparison of the operating system
L certificates trusted by the operating system r SSL certificates cate (ssIPEMKeyFile) ate is not protected by a passphrase	O Accept server SSL certificates trusted by the operating system O Accept any server SSL certificates Use Client Certificate (sslPEMKeyFile) Client Certificate: Passphrase: My client certificate is not protected by a passphrase Select SSL/TLS:	SSL certificates trusted by the operating system rver SSL certificates tificate (sslPEMKeyFile) ficate is not protected by a passphrase TLS
er SSL certificates cate (ssIPEMKeyFile) ste is not protected by a passphrase	 ❑ Accept any server SSL certificates ❑ Use Client Certificate (sslPEMKeyFile) Client Certificate: Passphrase: ☑ My client certificate is not protected by a passphrase Select SSL/TLS: TLS 	rver SSL certificates tificate (sslPEMKeyFile) ficate is not protected by a passphrase TLS
cate (ssIPEMKeyFile) Image: Constraint of the state of t	□ Use Client Certificate (sslPEMKeyFile) Client Certificate: Passphrase: My client certificate is not protected by a passphrase Select SSL/TLS: TLS	tificate (ssIPEMKeyFile)
ate is not protected by a passphrase	Client Certificate:	ficate is not protected by a passphrase
ete is not protected by a passphrase	Passphrase: My client certificate is not protected by a passphrase Select SSL/TLS: TLS	ficate is not protected by a passphrase
ate is not protected by a passphrase		ficate is not protected by a passphrase TLS
	Select SSL/TLS: TLS (TLS 🗸 🖉
LS 🗸 🗸 🚺		and the second sec
	⊴ Allow invalid hostnames (sslAllowInvalidHostnames) 🕚	iostnames (sslAllowInvalidHostnames) 🚯
tnames (sslAllowInvalidHostnames) 🧕		div.
tnames (sslAllowInvalidHostnames)	Use Server Name Indication (Advanced)	
tnames (sslAllowInvalidHostnames) 👔 e Indication (Advanced) 🕦		ame Indication (Advanced) 1
15 ~	Allow invalid hostnames (sslAllowInvalidHostnames)	rostnames (sslAllowInvalidHostnames)
	刁 Allow invalid hostnames (sslAllowInvalidHostnames) ①	nostnames (sslAllowInvalidHostnames)
tnames (sslAllowInvalidHostnames) 🚯		
tnames (sslAllowInvalidHostnames) 🚺	Use Server Name Indication (Advanced) 🛛 🕕	
tnames (sslAllowInvalidHostnames) 1		ame Indication (Advanced) 🕕

vii. Haga clic en **Test Connection** para comprobar si la conexión se realiza correctamente.

	3				1		
erver A	uthentication S	SL SSH	Proxy	IntelliShell	MongoDB Tools	Advanced	
Use S	Connecting						×
O Use o	Testing connec	tion					
C:\Us							
Acces	Operation				-	Ctatur	5177
Accep	Initializing cor	nection	5			OK	
Accep	Configuring S	SL connec	tion			OK	
Use C	Connecting to	server				OK	
	Authenticating	as rwuse	r			ок	000
lient Ce	Reading serve	er status fi	rom con	nection		OK	LQ C
assphra	Detecting acc	essible da		ок	۲ ا		
My di	Detecting Mo	ngoDB se	rver ver	sion		OK	
	Detecting Mo	ngoDB se	rver feat	ture compati	bility version	ок	
elect SS	Connected					ок	•
Use S							
NI Host	Hide details]			ОК	Cancel	
L		10			1	- Medi	

Figura 6-40 Comprobación de la conexión SSL

viii. Una vez que la comprobación se haya realizado correctamente, haga clic en Save.

Figura 6-41 Información de conexión

Quickstart										
🛃 Connection Ma	inager							×		
New Connection	New Group	Edit Delete	Clone	Import	Export	To UR			t trial	
Click here to filter	connections							1 match		
Name	DB Server	Security			Last Acce	ssed	Shortcu	t		
Es	"e Bergiely	🚛 🔑 rwuser	@ admin						at helps you automate common tasks.	
									inager	
									:ask	
Show on startu	p				Co	nnect	c	lose	rning	
C	uick Options						Getti	ing started vledge ba	d se	
T	neme (requires restart):	Same as system	\sim				Free	MongoDi	3 courses	
5	Show What's New ta	b after updating	Studio 3T				Join	the 3T cor	mmunity	
5	Automatically open of	Connection Man	ager at start	up			& Stud	io 3T feat	ures	
E	Enable Session Resto	re					Stud	io 31 tips io 3T Pow	and tricks er User manual: hidden gems that will	

ix. En la página de información de conexión, haga clic en **Connect** para conectarse a la instancia del conjunto de réplicas. Una vez que la instancia del conjunto de réplicas se ha conectado correctamente, se muestra **Figura 6-42**.

Figura 6-42 Conexión correcta

studio 31 for MongoUB - Full	product trial												ш
File Edit Database Collection	Index Document GridFS	View Help											
Connect Collection Inte	elliShell SQL Aggregate	Map-Reduce	Compare Schem	a Reschema	Tasks	Export	Import C	Data Masking	SQL Migration	Lusers	Roles) Feedback	
Search Open Connections (Ctrl+F) aA < (uickstart											
🗸 📳 [replica set: replica] [direct]	1												
> □ admin > □ bbb > □ ccc > □ ccc > □ local > □ local > □ test		Get Reco	ent Connectio	e to St ne tool using ons	udic g our def	3T ailed K	- Fu	JII pro ge Base. Tasks is	s a feature that helps y	al ou automati	e common 1	tasks.	
		68	Open Connection M	lanager					ipen Task Manager				
		+	Create a new conne	ction				18 c	reate a new task				
		•	Create a free Monge	DB cluster in the	cloud			Help	and Learning				
		Quie	ck Options e (requires restart): [Same as system '				Field Set	tting started owledge base e MongoDB courses n the 3T community				
Operations	古 ^	₩ S ₩ A	now what's New tab wtomatically open C nable Session Restor	o arter updating S onnection Manag re	ger at startu			 	idio 3T features idio 3T tips and tricks idio 3T Power User ma	nual: hidder	n gerns that	t will	

- Método 2: Conectarse manualmente a una instancia de base de datos.
 - i. En el cuadro de diálogo que aparece, seleccione Manually configure my connection settings y haga clic en Next.

Figura 6-43 Modo de conexión manual

🔁 Studio 3T fo	r MongoDB - Full product	trial															-	\times
File Edit Data	abase Collection Index	Document	t GridFS	View Help														
Connect	Collection IntelliShell	SQL A	ggregate	Map-Reduce	Compare	Contraction Schema	Reschema	Tasks	Export	Import	Data Maskin	ng SQI	(B→ Migration	-	2 Users	Roles	Eedback	
Search Open Co	onnections (Ctrl+F)	al	4 < Q1	ickstart														
				Conn	ection Mana	ager								×				^
						+		È				5 14		Э	al 👘			
				New Co	onnection	New Group	<u>E</u> dit	Delete	<u>C</u> lone	Impor	t E _S port	To <u>U</u> RI	0	n	narter.	Get a		
				Alama	e to inter co	New Conce	rtion					_	TT I	×				
						i you have a an paste it h) Paste your URI:) Manually c	connection st ere and Studi connection st onfigure my c	ring (<u>SRV o</u> o 3T will au ring (SRV o onnection s	r standard) to-configur r standard ettings	l, e.g. for <u>y</u> re your cor) here:	our MongoDf Inection settin	<u>B Atlas</u> de Igs for yo	ployment, u.	you	automate	e common	ı tasks.	
				Show	on start						N	lext	Cance	ł				1
				Qu	uick Opt	ions					1	Getting st Knowledg	arted je base					
				The	me (require	s restart): Sa	me as system	~				Free Mon	goDB cour	ses				- 11
					Show What	t's New tab a	fter updating	Studio 3T			بر م	Join the 3 Studio 2T	T commun	ity				
Onerting					Automatica	ally open Cor	nection Mana	iger at start	up		P	Studio 3T	tins and tr	icks				~
operations		ć			Enable Ses	sion Restore							- and a					

ii. En la pestaña Server, establezca Server y Port.

NOTA

Server: EIP. Port: puerto de base de datos.

Figura 6-44 Servidor

new Connection	×
Connection name:	
Connection group: <pre><root level=""></root></pre>	
Server Authentication SSL SSH Proxy IntelliShell MongoDB Tools Advanced	
Connection Type: Standalone	
Server: D Port: Port:	
Read-Only Lock 1	
	-
From UKI Use this option to import connection details from a connection string / UKI	
Use this option to export complete connection details to a connection string / UKI	
Test Connection Save Cancel	

iii. Haga clic en la pestaña Authentication y seleccione Legacy(SCRAM-SHA-1).

Figura 6-45 Autenticación

Connection name:	
Connection group: <root level=""></root>	-
Server Authentication SSI SSH Provy IntelliShell MongoDB Tools Advanced	
Authentication Mode: Legacy (SCRAM-SHA-1)	\sim
You have chosen an aut None	
Please refer to the <u>Mond</u> Basic (SCRAM-SHA-256)	
X.509	
Kerberos (GSSAPI) - Studio 3T Ultimate	
Password: LDAP (PLAIN) - Studio 31 Ultimate AWS Identity and Access Management (IAM) - Studio 3T Ultimate	
Authentication DB:	
The database where the user is defined	
Always show the authentication database of the user assount	
\square Always show all databases and collections defined in roles of the user account	
Manually list additional visible databases by their names	
Test Connection Save Cano	el

iv. Establezca User name, Password y Authentication DB.

Figura 6-46 Autenticación

onnection	group: <ro< th=""><th>ot level</th><th>></th><th></th><th></th><th></th><th></th><th>~</th></ro<>	ot level	>					~	
Server A	uthentication	SSL	SSH	Proxy	IntelliShell	MongoDB Tools	Advanced		
Authentic	ation Mode:	Legac	y (SCR4	M-SHA	1))	
You have o Please refe	chosen an aut er to the <u>Mone</u>	thenticat	tion met curity C	thod whi hecklist	ich might mak to help secure	re your MongoDB ins your database(s).	tance vulnerable	e to attacks.	
User nam	ie:	rwuse	r						
Password	Ŀ	••••	•••••	•••••				•	
Authentic	ation DB:	admin							
		The database where the user is defined							
			D	2					
			C	3					
			5	3					
			5	\$					
Always	show the au	thentic	tion d	2 atabase	of the user	account			
☑ Always ☑ Always	show the au	uthentic. tabases	ation d	3 atabase	of the user	account roles of the user a	ccount		
☑ Always ☑ Always ☑ Manua	show the au show all dat	ithentici tabases onal vis	ation d and co ible da	atabase ollection tabases	of the user ns defined in s by their nar	account roles of the user a mes ①	ccount		
☑ Always ☑ Always ☑ Manua Database	show the au show all da ily list additi s: admin,te:	uthentica tabases onal vis st	ation d and co ible da	atabase ollection tabases	of the user ns defined in s by their nar	account roles of the user a mes 1	ccount		

v. Haga clic en **Test Connection** para comprobar si la conexión se realiza correctamente.

onnection	group: <root< th=""><th>t level></th><th></th><th></th><th></th><th></th><th></th></root<>	t level>					
Server Au	thentication	SSL SSH	Proxy	IntelliShell	MongoDB Tools	Advanced	
Authentic	🔁 Connectin	9					×
You have	Testing conne	ection					acks
Please rei							
User nar	Operation					Status	
Password	Initializing c	onnection				ок	
Fasswon	Connecting	to server				ок	
	Authenticati	ng as rwuse	er			ок	
Authentic	Reading ser	ver status f	rom con	nection		ок	
	Detecting a	ccessible da	tabases			ок	
	Detecting N	longoDB se	rver ver	sion		ок	
	Detecting N	longoDB se	rver fea	ture compati	bility version	ок	
	Connected					ок	
-							
Alway	Utile desci				OK	Canad	
✓ Alway	Hide detail	5			UK	Cancel	
Manuo Manuo	1 3 13 2001001			b by their nor	nes 🕒		
	. Industry and						

Figura 6-47 Conexión de prueba

vi. Haga clic en la pestaña SSL y seleccione Use SSL protocol to connect.

D NOTA

Si la encriptación de datos SSL está deshabilitado, omita este paso y vaya a 6.ix.

Figura 6-48 SSL

onnection group:	<root leve<="" th=""><th> ></th><th></th><th></th><th></th><th></th><th></th><th>~</th></root>	>						~
Server Authentic	ation SSL	SSH	Proxy	IntelliShell	MongoDB Tools	Advanced		
<u> U</u> se SSL proto	col to conn	ect					1	
⊖Use own <u>R</u> oot	CA file (s	slCAFile)					
								ĺ
O Accept server	SSL certifica	ites trus	ted by	the <u>o</u> peratin	g system			
Accept any ser	ver SSL cer	tificates						
Use Client Cert	ificate (s	slPEMKe	eyFile)					
Client Certificate:								6
Passphrase:							۲	6
✓ My client certif	icate is not	protect	ed by a	passphrase	•			
Select SSL/TLS:	TLS						~ 1	
Allow invalid h	ostnames (-	-sslAllo	wInvalio	dHostnames) 1			
Use Server Na	me Indicati	on (Adva	anced)	6				
				-				
SNI Host Name:								
SNI Host Name:								
SNI Host Name:								

vii. Seleccione Use own Root CA file (--sslCAFile), importe el certificado y seleccione Allow invalid hostnames.

NOTA

Descargue el certificado SSL y verifique el certificado antes de conectarse a las bases de datos.

En la página Instances, haga clic en el nombre de la instancia de base de datos de

destino. En el área **DB Information** de la página **Basic Information**, haga clic en en el campo **SSL** para descargar el certificado raíz o el paquete de certificados.

onnection g	group: <root le<="" th=""><th>vel></th><th></th><th></th><th></th><th>~</th></root>	vel>				~
Server Au	thentication SS	SL SSH Proxy	IntelliShell Mong	oDB Tools	Advanced	
Use SSL	. protocol to cor	nnect				7
Use own	n Root CA file (sslCAFile)				
C:\User	rs\	Downloads ca.cr	to ve			<u>a</u> 🤇
Accept	server SSL certif	icates trusted by	the operating syster	m		
O Accept	any server SSL c	ertificates				
Use Clie	ent Certificate (-	-sslPEMKeyFile)				
Client Cert	ificate:					20
Passphras	e:					• 6
My clier	nt certificate is n	ot protected by	a passphrase			
Select SSL	TLS: TLS					0
		o. 1997 (2011 W				
Allow in	valid hostnames	s (sslAllowInvali	dHostnames) 🚺			
	ver Name India	ation (Advanced)				
Use Ser	ver marrie mulca		-			
Use Ser						
	ver Name Indic	ation (Advanced)	0			

viii. Haga clic en **Test Connection** para comprobar si la conexión se realiza correctamente.

ication SSL SS	H Provy IntelliShell		1.	
	in troxy intensiten	MongoDB Tools	Advanced	
onnecting)	×
ng connection				
eration	6	S	tatus	
alizing connection	1 ⁻⁰	C	ж	
figuring SSL conr	lection	0	ж	
necting to server		0	JK .	
ding server statu	from connection	0	NK .	20
ecting accessible	databases)K	
ecting MongoDB	server version)K	
ecting MongoDB	server feature compatib	ility version C	ж	
nected		C	ж	0
de details		ОК	Cancel	
		10	The second s	20
	onnecting ng connection eration ializing connection figuring SSL conn necting to server henticating as rwu ading server statu- ecting accessible secting MongoDB secting MongoDB mected	ennecting ng connection eration ializing connection figuring SSL connection necting to server henticating as rwuser ading server status from connection tecting MongoDB server version tecting MongoDB server feature compatib nected de details	eration eration eration ializing connection figuring SSL connection figuring SSL connection figuring as rwuser coding server status from connection frecting accessible databases feeting MongoDB server feature compatibility version funceted	ang connecting Status ang connection eration ializing connection oK oK oK oK oK oK connecting to server oK benticating as rwuser oK benticating as rwuser oK benticating accessible databases oK becting MongoDB server feature compatibility version oK beneted oK beneted oK cancel be

Figura 6-50 Comprobación de la conexión SSL

ix. Una vez que la comprobación se haya realizado correctamente, haga clic en Save.

Figura 6-51 Información de conexión

Quickstart											
n Connection Ma	inager								×		
New Connection	New Group	Edit	Delete	Clone	Import	Export	To UR	I.		t trial	
Click here to filter	connections								1 match		
Name	DB Server		Security			Last Acce	ssed	Shortcut		1	
Ee	"a dangin"		rwuse	r @ admin							
										at helps you automate common tasks.	
										inager	
										task	
Show on startu	p					Co	onnect	Clo	se	rning	
C	uick Options							Getting	g started edge bas	se	
T	neme (requires restart):	Sam	e as system	n 🗸				Free N	longoDB	courses	
5	Show What's New t	ab afte	r updating	Studio 3T				Join th	e 3T con	nmunity	
5	Automatically open	Conne	ection Mar	ager at sta	artup			& Studio	3T featu	ires	
0	Enable Session Rest	ore						8 Studio	3T tips a	and tricks	
								V Studio	3T Powe	er User manual: hidden gems that will	

x. En la página de información de conexión, haga clic en Connect para conectarse a la instancia del conjunto de réplicas. Una vez que la instancia del conjunto de réplicas se ha conectado correctamente, se muestra Figura 6-52.

Figura 6-52 Conexión correcta

File Edit Database Collecti	on Index Do	cument GridFS	View Help												
onnect Collection	IntelliShell S	QL Aggregate	Map-Reduce	 Compare	C) Schema	Reschema	[] Tasks	Export	Import	Data Masking	SQL Migration	Lusers	Roles) Feedback	
earch Open Connections (Ctr	I+F)	aA < q	uickstart												
Coll (Fight a Set (Fight a) (and) ≦ asa) ≦ admin) ≦ bob) ⊕ toos) ⊕ toos) ⊕ toos) ⊕ toos) ⊕ toost) ⊕ toost) ⊕ toost	auj		Contraction Contra	Velcc et started ecent Cor last eccesec d Open Conr + Create a ne	ome with the inection 0.154.218.1 I moments and section Main we connect	to St e tool using ns coasos) nager ion	udia 9 our de	D 3T	- F	Ull pro dge Base. Task: Tasks is otasks iii c c iiii c c iiiii c	5 s a feature that helps ye set. open Task Manager reate a new task	al	e common	tasks.	
			Q Thu I I I I I I I I I I I I I I I I I I I	Create a fre uick Optio	re MongoE DITS restart): Sa New tab a y open Cor	B cluster in the me as system ` ifter updating S intection Manag	cloud	ip		Help Ge Kni Fre Joi Joi	and Learning tting started owledge base e MongoDB courses n the 3T community idio 3T features				
Operations		古 ^		Enable Sessi	on Restore					Stu Stu	idio 3T tips and tricks idio 3T Power User ma	nual: hidder	n gems tha	t will	

A Historial de cambios

Lanzado en	Descripción
2021-12-30	Esta versión es el trigésimo lanzamiento oficial, que incorpora los siguientes cambios:
	 Conexión a una instancia de clúster mediante código de programa agregado.
	 Conexión a una instancia de conjunto de réplicas mediante código de programa agregado.
	 Conexión a una instancia de nodo único mediante código de programa agregado.
2021-10-30	Esta versión es el vigésimo noveno lanzamiento oficial, que incorpora el siguiente cambio:
	Descripción agregado.
2021-05-30	Esta versión es el vigésimo octavo lanzamiento oficial, que incorpora el siguiente cambio:
	Compra rápida y compra personalizada admitidas.
2021-04-30	Esta versión es el vigésimo séptimo lanzamiento oficial, que incorpora el siguiente cambio:
	Grupo de parámetros cambiado a la plantilla de parámetros.
2020-10-30	Esta versión es el vigésimo sexto lanzamiento oficial, que incorpora el siguiente cambio:
	Hasta 20 etiquetas admitidas por instancia.
2020-09-30	Esta edición es el vigésimo quinto lanzamiento oficial, que incorpora los siguientes cambios:
	Compatible con instancias basadas en Kunpeng de Community Edition 4.0.

Lanzado en	Descripción
2020-08-30	Esta edición es el vigésimo cuarto lanzamiento oficial, que incorpora los siguientes cambios:
	• Admitidos hasta 32 nodos mongos y 32 nodos shard en cada instancia de clúster de Community Edition.
	• Admitidos hasta 3,000 GB de espacio de almacenamiento del conjunto de réplicas.
2020-07-30	Esta versión es el vigésimo tercer lanzamiento oficial, que incorpora los siguientes cambios:
	Admitido el acceso multi-CIDR a instancias de conjuntos de réplicas.
2020-07-15	Esta versión es el vigésimo segundo lanzamiento oficial, que incorpora el siguiente cambio: DCC admitido.
2020-05-30	Esta versión es el vigésimo primer lanzamiento oficial, que incorpora el siguiente cambio:
	Proyectos de empresa admitidos para la instancia de clúster mejorado.
2020-04-30	Esta versión es la vigésima versión oficial, que incorpora los siguientes cambios:
	• Actualizada la plantilla de permisos de IAM.
	• Admitida la compra de instancias de base de datos de multi-AZ Community Edition.
2020-04-15	Esta edición es el decimonoveno lanzamiento oficial, que incorpora el siguiente cambio:
	Admitido el acceso entre subred compatible para instancias de conjuntos de réplicas en la misma VPC.
2020-03-31	Esta versión es el decimoctavo lanzamiento oficial, que incorpora los siguientes cambios:
	• Admitido el cambio del modo de facturación de anual/mensual a pago por uso.
	• Permitido a los usuarios establecer una contraseña después de crear la instancia de base de datos.
	• Admitida la habilitación de direcciones IP de nodos de shard y config de instancias de clúster de Community Edition.
2020-02-14	Esta versión es el decimoséptimo lanzamiento oficial, que incorpora el siguiente cambio:
	Optimizados los procedimientos para crear una instancia de base de datos.
2020-01-07	Esta versión es la decimosexta versión oficial, que incorpora los siguientes cambios:
	• Ajustada la estructura de la sección Pasos iniciales.

Lanzado en	Descripción
2019-11-11	Esta versión es el decimoquinto lanzamiento oficial, que incorpora el siguiente cambio:
	Admitida la instancia de clúster de Community Edition con hasta 2,000 GB de almacenamiento.
2019-10-18	Esta versión es la decimocuarta versión oficial, que incorpora los siguientes cambios:
	• Admitida la selección de las especificaciones s6.
	• Agregados los procedimientos para usar Robo 3T para conectarse a la instancia DDS.
2019-09-11	Esta versión es la decimotercera versión oficial, que incorpora los siguientes cambios:
	Admitido un máximo de 16 nodos mongos y 16 shards para una instancia de clúster de Community Edition.
2019-08-13	Esta versión es la duodécima versión oficial, que incorpora el siguiente cambio:
	Admitida la selección de un tipo de CPU para la instancia de base de datos de pago por uso de Community Edition 3.4.
2019-07-07	Esta edición es la undécima versión oficial, que incorpora los siguientes cambios:
	Admitida la selección de un grupo de parámetros durante la creación de instancias de base de datos.
2019-06-13	Esta edición es el décimo lanzamiento oficial, que incorpora el siguiente cambio: Admitido DeC.
2019-04-19	Esta edición es la novena versión oficial, que incorpora los siguientes cambios:
	• Optimizados los procedimientos para crear y conectarse a una instancia de base de datos.
2019-02-15	Esta versión es el octavo lanzamiento oficial, que incorpora los siguientes cambios:
	Admitida la modificación de la dirección IP privada del nodo.
2019-01-07	Esta versión es el séptimo lanzamiento oficial, que incorpora los siguientes cambios:
	• Agregado el elemento de configuración de Tags en la página para comprar una instancia de base de datos de Community Edition.

Lanzado en	Descripción
2018-11-02	Esta versión es el sexto lanzamiento oficial, que incorpora los siguientes cambios:
	• Admitida la compra anual/mensual de instancias de base de datos en lotes.
	• Agregado el comando para conectarse a instancias de base de datos a través de direcciones de conexión.
2018-09-06	Esta versión es el quinto lanzamiento oficial, que incorpora el siguiente cambio:
	Optimizada la sección para guiar la compra de instancias de base de datos.
2018-08-03	Esta versión es el cuarto lanzamiento oficial, que incorpora los siguientes cambios:
	• Optimizada la página para comprar una instancia de base de datos.
	• Admitida la creación de instancias de clúster anuales/mensuales.
	• Admitida la renovación automática de instancias de conjuntos de réplicas anuales/mensuales.
2018-07-02	Esta edición es la tercera versión oficial, que incorpora el siguiente cambio:
	• Admitida la creación de una instancia de conjunto de réplicas en múltiples AZ.
	• Ajustada la posición de HA Type que se muestra en la página de la consola.
	 Cambiada la capacidad máxima de almacenamiento de los conjuntos de réplicas a 2,000 GB.
2018-06-01	Esta versión es el segundo lanzamiento oficial, que incorpora el siguiente cambio:
	• Admitidas las instancias de base de datos que son compatibles con MongoDB 3.4 Community Edition.
	• Admitida la asignación de recursos de VPC predeterminados durante la creación de la instancia de base de datos.
2018-05-04	Esta edición es el primer lanzamiento oficial.