Document Database Service

Getting Started

 Issue
 01

 Date
 2025-01-17





HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

NUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:

https://www.huawei.com/en/psirt/vul-response-process

For vulnerability information, enterprise customers can visit the following web page: <u>https://securitybulletin.huawei.com/enterprise/en/security-advisory</u>

Contents

1 Getting Started with DDS	1
2 Buying and Connecting to a Cluster Instance	. 2
3 Buying and Connecting to a Replica Set Instance	10
4 Getting Started with Clusters	17
4.1 Buying a Cluster Instance	17
4.1.1 Quick Config	17
4.1.2 Custom Config	23
4.2 Connecting to a Cluster Instance	35
4.2.1 Connection Methods	35
4.2.2 (Recommended) Connecting to Cluster Instances Through DAS	36
4.2.2.1 Overview	36
4.2.2.2 Connecting to a Cluster Instance Through DAS	37
4.2.3 Connecting to a Cluster Instance over a Private Network	37
4.2.3.1 Configuring Security Group Rules	37
4.2.3.2 Connecting to a Cluster Instance Using Mongo Shell (Private Network)	41
4.2.3.3 Connecting to Read Replicas Using Mongo Shell	51
4.2.4 Connecting to a Cluster Instance over a Public Network	55
4.2.4.1 Binding and Unbinding an EIP	55
4.2.4.2 Configuring a Security Group	58
4.2.4.3 Connecting to a Cluster Instance Using Mongo Shell (Public Network)	.61
4.2.4.4 Connecting to a Cluster Instance Using Robo 3T	68
4.2.5 Connecting to a Cluster Instance Using Program Code	75
4.2.5.1 Java	75
4.2.5.2 Python	79
5 Getting Started with Replica Sets	80
5.1 Buying a Replica Set Instance	80
5.1.1 Quick Config	80
5.1.2 Custom Config	85
5.2 Connecting to a Replica Set Instance	97
5.2.1 Connection Methods	97
5.2.2 (Recommended) Connecting to Replica Set Instances Through DAS	98
5.2.2.1 Overview	98

5.2.2.2 Connecting to a Replica Set Instance Through DAS	
5.2.3 Connecting to a Replica Set Instance over a Private Network	
5.2.3.1 Configuring Security Group Rules	
5.2.3.2 Connecting to a Replica Set Instance Using Mongo Shell (Private Network)	103
5.2.3.3 Connecting to Read Replicas Using Mongo Shell	115
5.2.4 Connecting to a Replica Set Instance over a Public Network	119
5.2.4.1 Binding and Unbinding an EIP	119
5.2.4.2 Configuring Security Group Rules	122
5.2.4.3 Connecting to a Replica Set Instance Using Mongo Shell (Public Network)	125
5.2.4.4 Connecting to a Replica Set Instance Using Robo 3T	132
5.2.5 Connecting to a Replica Set Instance Using Program Code	138
5.2.5.1 Java	
5.2.5.2 Python	142
6 Getting Started with Single Nodes	143
6.1 Connecting to a Single Node Instance	143
6.1.1 Connection Methods	143
6.1.2 (Recommended) Connecting to a Single Node Instance Through DAS	144
6.1.2.1 Overview	144
6.1.2.2 Connecting to a Single Node Instance Through DAS	144
6.1.3 Connecting to a Single Node Instance over a Private Network	145
6.1.3.1 Configuring a Security Group	145
6.1.3.2 Connecting to a Single Node Instance Using Mongo Shell (Private Network)	
6.1.4 Connecting to a Single Node Instance over a Public Network	153
6.1.4.1 Binding and Unbinding an EIP	153
6.1.4.2 Configuring a Security Group	155
6.1.4.3 Connecting to a Single Node Instance Using Mongo Shell (Public Network)	158
6.1.4.4 Connecting to a Single Node Instance Using Robo 3T	163
6.1.5 Connecting to a Single Node Instance Using Program Code	169
6.1.5.1 Java	
6.1.5.2 Python	173
7 Logging In to and Logging Out of the DDS Console	174
8 Example: Buying and Connecting to a DDS Instance	
8.1 Connecting to a DB Instance Using Mongo Shell	
8.2 Connecting to a DDS Instance Through an EIP	193
9 Getting Started with Common Practices	212

Getting Started with DDS

This section describes DDS instance and product types, helping you quickly create and connect to a DDS instance.

Connection Methods

Data Admin Service (DAS) enables you to manage DB instances on a web-based console, simplifying database management and improving working efficiency. You can connect to and manage DB instances through DAS. By default, you have the remote login permission. Using DAS to connect to your DB instance is recommended, which is more secure and convenient.

Method	Scenario	Description
DAS	You can log in to an instance on the console without using an IP address.	 Easy to use, secure, advanced, and intelligent Recommended

Table 1	-1	Connection of	on DAS	
---------	----	---------------	--------	--

2 Buying and Connecting to a Cluster Instance

This section describes how to quickly purchase a cluster instance on the management console and how to connect to the cluster instance through DAS.

Operation Process

Process	Description
Preparations	Sign up for a HUAWEI ID, enable Huawei Cloud services, and make sure you have a valid payment method configured.
Step 1: Quickly Buy a Cluster Instance	Select required basic settings and additional options and buy a DDS DB instance.
Step 2: Connect to a Cluster Instance Through DAS	DAS provides a GUI and allows you to perform visualized operations on the console.

Preparations

- 1. Sign up for a HUAWEI ID and enable Huawei Cloud services.
- 2. For fine-grained permissions management on Huawei Cloud resources, use Identity and Access Management (IAM) to create a user or user group and grant it specific operation permissions. For details, see **Creating a User and Granting Permissions**.

Step 1: Quickly Buy a Cluster Instance

- Step 1 Go to the Quick Config page.
- **Step 2** On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.

inglobal inglobal region region reginet region	Basic Information	
npin Second	Billing Mode	Yearly/Monthy Payper can
Paper Paper Ad Composition of compositio	Region 8	
npin Immonf m monf		Regions are geographic areas isolated from each other. For low network latency and quick resource access, solect the nearest region.
1 Image: All and all all all all all all all all all al	Project	
Deby well Binstein in sigle A2 to the A2. bit high analatile; Die Binstein Tiger ① Die binstein in sigle A2 to the A2. bit high analatile; Construction die structure binstein structure binder stating phase. The high analatile; stating the phase here are stating and phase here are binder stating phase. The high analatile; stating the phase here are stating and phase here are binder stating phase. The high analatile; stating the phase here are stating and phase here are binder stating phase. The high analatile; stating phase methods the stating phase methods. The stating phase methods the stating phase methods the stating phase methods. The stating phase methods the stating phase methods the stating phase methods. The stating phase metho	AZ	an-andh-4a an nardh-4b an-nardh-4c AZ7 an nardh-4a,an nardh-4a,AZ7
Di Hanton Tyne Carrer Reifa mil Oudrithine mpifa mil Di Hanton Tyne Carrer Reifa mil Oudrithine mpifa mil Di Hanton Tyne Di Carrer Low and permanes them insteade und spotes. The high availability and floadile stating the possible stating the p		Deploy your DB instance in a single AZ or three AZs for high availability.
Calculation provide the rest rest and the rest back reading spaces. The high analytic program for rest provide material is a line and the rest rest rest rest and the rest rest rest and the rest rest rest rest and the rest rest rest and the rest rest rest and the rest rest rest rest and the rest rest rest rest rest rest rest res	DB Instance Type (2)	Ouster Replica set Cloud native replica set
Compatibility op call lenges 12. Neurone Dates Compatibility op call lenges 12. Neurone Dates Recommended genolosis Recommended genolo		Clusters offer more robust performance than replica sets and more flexible scaling options. The high availability and flexible scaling they provide make them an excellent choice for large enterprises.
Competitive Mongold Weint 10 14 42 40 14 Recentended Specificators Competitive Mongold Main and Corrections 2,000 Main and Corrections 1,000 Main and Correctiore 1,000 Main and Corections 1,000		Clusters of community edition you can still create: 10. Increase Quota
Restination Exemption Exemption Restination Exemption Exemption Main 2 vPClk [M30 UberlighTi0] ExPCVlk [M30 UberlighTi0] ExeCVlk [M30 UberlighTi0] ExeCVlk [M30 UberlighTi0] Main 2 ++ The quarkly ranges from 2 to 32. Correct yearstat datampathatlange4 ranges [2 vCRk [M30 ExeCVlk [M30 UberlighTi0] ExeCVlk [M30 UberlighTi0] Main 2 ++ The quarkly ranges from 2 to 32. Exertive static ranges dutalinge 4 ranges [2 vCRk [M30 Main	Compatible MongoDB Version	50 Bets 44 42 40 3.4
Reconverted Specificators dds morges Noh Gam 2:470.18 (503 Ubra tigh 10 4:470.18 (1503 Ubra tigh 10 1:4270.14 0.8 ··· 1:4270.14 0.8 ··· Ubra tigh 10 Nodes - 2 + The quartity ranges from 2 to 30. Converty whethed discrime_Convections 1000 Maximum Convections 1000 Maximum Convections 1000 Nodes - 2 + The quartity ranges from 2 to 30. Converty whethed discrime_Convections 1000 1:4270.14 0.8 ··· Ubra tigh 10 Stade 4:4270.18 (1603 Ubra tigh 10 1:4270.14 0.8 ··· Ubra tigh 10 Stade - 2 + The quartity ranges from 2 to 30. Imaximum Convections 1,000 Imaximum Convections 1,000 Nodes - 2 + The quartity ranges from 2 to 64. Imaximum Convections 1,000 Imaximum Convections 1	Specifications	Generati-purpose Ethonood II
Nob Oss 2 xPCb1 [803 Ubrstight0] 4 xPCb1 [100 Ubrstight0] B xPCb1 [100 Ubrstight0] I vPCV1 4 4 8 w Ubrstight0 Maximum Connections 10.00 Nobs 2 ++ The quarkly ranges from 2 to 32. Carently selected distancequals Margue Annarges [2 xPCb1 100 Ubrstight0] I vPCV1 4 6 8 w Ubrstight0 Maximum Connections 10.00 I vPCV1 4 0 8 w Ubrstight0 Maximum Connections 10.00 Shard I vPCV1 100 Ubrstight0 100 0 8 Waterum Connections 10.00 I vPCV1 4 0 8 w Ubrstight0 100 0 8 Waterum Connections 10.00 I vPCV1 4 0 8 w Ubrstight0 100 0 8 Waterum Connections 10.00 Nade: 2 ++ The quarkly ranges form 2 to 64. I vPCV1 + 100 Horstight 10 100 0 8 Waterum Connections 10.00 Nade: 2 ++ The quarkly ranges form 2 to 64. I vPCV1 + 1008 Currently wateriet distancequarkLoader[4 x/QCV2 h] 1008 I vPCV1 + 1008 Config Storage 200	Recommended Specifications	dds mongos
Notified 2, 476 kg 1668 Wassingh 100 4 x676 kg 1668 Wassingh 100 1 x670 kg 1668 Notified 2 + The quartify arrays 10 x00 Massimum Connections 10,000 Massimum Connections 10,000 Notified 2 + The quartify arrays 10 x00 kg 100 Massimum Connections 10,000 Massimum Connections 10,000 Notified 4 x076 kg 1068 Massimum Connections 10,000 Massimum Connections 10,000 Notified 4 x076 kg 1068 Massimum Connections 10,000 Massimum Connections 10,000 Notified 4 x076 kg 1068 Massimum Connections 10,000 Massimum Connections 10,000 Notified 4 x076 kg 1068 Massimum Connections 10,000 Massimum Connections 10,000 Notified 2 + The quartify arrays from 2 to 64. Massimum Connections 10,000 Config Massimum Connections 10,000 Massimum Connections 10,000 Massimum Connections 10,000 Massimum Connections 10,000 Notified 4 x070 kg 106.01 Massimum Connections 10,000 Massimum Connections 10,000 Massimum Connections 10,000 Notified 4 x070 kg 106.01 Massimum Connections 10,000 Massimum Connections 10,000 Massimum Connections 10,000		
Ozna Maximum Corrections: 0.00 Maximum Corrections: 10.00 Nodes		Node 2 vCPUs 8GB Utra-high I/O 4 vCPUs 16GB Utra-high I/O 8 vCPUs 16GB Utra-high I/O 1 vCPU 4 GB V Utra-high I/O
Mainum Corrections 2.000 Mainum Corrections 10.00 Mainum Corrections 10.00 Mainum Corrections 2.000 Mainum Corrections 10.00 Mainum Corrections 10.00 Mainum Corrections 2.00 Mainum Corrections 10.00 Mainum Corrections 10.00 Mainum Corrections 2.00 Scored y stacked data respective data starsport of the starsport o		Class
Node: - 2 + The quantity ranges from 2 to 30. Currently selected: disturmangutustualizage.f.morages [2×CPLb] 608 Subsci 4×CPLb [1502 Ubes high 100 [1×CPL] 4/0.62 ∨ Ubes high 100 Open 4×CPLb [1502 Ubes high 100 [1×CPL] 4/0.62 ∨ Ubes high 100 Open 10000 [10×CPL] 4/0.62 ∨ Ubes high 100 [1×CPL] 4/0.62 ∨ Node: - 2 + The quantity ranges from 2 to 64. [10×CPL] 4/0.62 Currently selected: disturmarges.dutes[4×CPLb [1602 [10×CPL] 4/0.62 [10×CPL] 4/0.62 Config		Maximum Connections:2,000 Maximum Connections:4,000 Maximum Connections:16,000 Maximum Connections:10,000
Node: 2 + The quartity ranges for 2 to 50. Currently selected: disk mangada diagnet. Amongs [2 xCPLs 60:03 Stand 4xPC ks 10:03 0: xCPLs 10:03 Mode: 4xPC ks 10:03 0: xCPLs 10:03 Mode: 2 + Mode: 2 + Durently selected: disk mangada diagnet. 4 xCPLs 10:08 Currently selected: disk mangada diagnet. 4 xCPLs 10:08 Corrently selected: disk mangada diagnet. 4 xCPLs 10:08 Corrently selected: disk mangada diagnet. 4 xCPLs 10:08		
Note 2 + The questly images from 2 to 32. Carrently selected data margadual datages. From yes [2 x CPUs] (600 Shard 		
Converty instead disturbuildings. Amorge [2:CRLs] 608		Nodes - 2 + The quantity ranges from 2 to 32.
Currently weeked disk maragadhudkages. Amorgan (2 x CPUs) (608) Stand Image: Single (2 x CPUs) (608) (2 x Light (10) (2 x Light		
shard Nois Oam 4-024k1 1968 Uites tigh 10 0008 Maximum Corrections 1,000 1-0291 4 68 v Uites tigh 10 200 0 Noise Maximum Corrections 1,000 10008 Maximum Corrections 1,000 10008 Maximum Corrections 1,000 Noise 2 + The quereity ranges from 2 to 64. Correctly selected disconsequents thologies 4 short 4-024 to 1608 Control y selected disconsequents thologies 4 short 4-024 to 1608 Control y selected disconsequents thologies 4 short 4-024 to 1608		Currently selected dds.mongozb.s6.large.4.mongos 2 vCPUs 8GB
Node 4 xCPUs 1608 Uites high 10 8 xCPUs 1608 Uites high 10 Open Maximum Corrections 4,000 Maximum Corrections 10,000 Maximum Corrections 10,000 Nodes 2 + The quarkity ranges from 2 to 64. Connerly selected disk managed sublarged subla		shard
Name 4 x (CPLs) (803 Uter-high 10 8 x (CPLs) (803 Uter-high 10 10038 10038 10038 10038 10038 10038 Materium Corrections (500 Materium Corrections (100) 10038 10038 10038 Materium Corrections (100) Materium Corrections (100) 10038 10038 10038 Currently webcited data mengedusticities (14 x (CPLs) (1608) 10038 10038 10038 Config 10038 10038 10038 10038 10038 Materia 10038 10038 10038 10038 10038		Note
0008 0008 200 80 Meanum Corrections 4.000 Mainum Corrections 1.000 Mainum Corrections 1.000 Mainum Corrections 1.000 Nodes - 2 + + The quartity ranges from 2 to 64. Scored Scored Scored Currently selected disturmargues data/selects/distance Scored Scored Scored Nodes - 2 + + The quartity ranges from 2 to 64. Scored Scored Scored Currently selected disturmargues data/selects/distance Scored Sco		Claves 4 vGPUs 16GB Ultra-high I/O 8 vGPUs 16GB Ultra-high I/O 1 vGPU 4 GB V Ultra-high I/O
Nades 2 + The quartify ranges from 2 to 64. Currently selected dista mangadu skillarge4 dated [4 xCPkk] %068 Config Storage Storage Nobe 4 xCPkk 8 GB ∨ Storage Storage Storage		100GB 100GB 200 GB
Nodes 2 + The quarkly ranges from 2 to 64. Currently indexed data mangatula datard [4 + QPUs] 16 GB config		Maximum Connections:1,000 Maximum Connections:18,000 Maximum Connections:1,000
Nodes 2 + The quartity ranges from 2 to 64. Currently selected disk mangrads dial larges. 4 share} 4 x CPUs 16008 Config Storage 2008 Date 4 x CPUs 1608 v 2008		
Nodes - 2 + The quartify regress from 2 to 64. Currently selected dista mergodu du blarges. 4 sharel 4 x CPUs 16 CB Config		
Currently selected: data merupathadulatignet_scharted [4 + QPUs] 16081 config		Nodes _ 2 + The quantity ranges from 2 to 64.
Currently selected data mangadust datarge 4.4 mB 1 8.00B sonfig Note Gase 4.070 k 8.0B v Storage 2008 Space		
config Nobe Strape Game \$008		Currently selected dds.mongodb.sfb.slarge.4.shard 4 vCPUs 16GB
Note Storage 2008		config
Node Strage Class 4√CPUs 5 GB ∨ 220GB Space		
Class Space		Node 4 vCPUs 8 G8 √ 20G8
		Class Space

Figure 2-1 Basic configurations

Parameter	Example Value	Description
Billing Mode	Pay-per-use	Select a billing mode, Yearly/Monthly or Pay- per-use.
		For yearly/monthly instances
		 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 Yearly/Monthly to Pay-per-Use.
		NOTE 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.
		For pay-per-use instances
		 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 Pay-per-Use to Yearly/Monthly.
Region	CN-Hong	The region where the resource is located.
	Kong	NOTE 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.
Project	default	The project corresponds to the current region and can be changed.

 Table 2-1
 Basic configurations

Parameter	Example Value	Description
AZ	az1	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.
		Instances can be deployed in a single AZ or three AZs.
		NOTE The 3-AZ deployment is not available in all regions. If the 3-AZ option is not displayed on the page for you to buy an instance, try a different region.
		 If your service requires low network latency between instances, you deploy the components of the instance in the same AZ. If you select a single AZ to deploy your instance, anti-affinity deployment is used by default. With an anti-affinity deployment, your primary, secondary, and hidden nodes are deployed on different physical machines for high availability.
		• If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the dds mongos, shard, and config nodes are evenly distributed across the three AZs.
DB	Cluster	Select Cluster .
Instance Type		A cluster instance includes three types of nodes: dds mongos, shard, and config. Each shard and config is a three-node replica set to ensure high availability.
Compatibl e MongoDB Version	4.4	The database version.
CPU Type	X86	DDS supports x86 and Kunpeng CPU architectures.

Parameter	Example Value	Description
Specificati ons	Enhanced II	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 mediumand heavy-load enterprise applications. For details about the supported instance specifications, see Cluster Instance
dds mongos Node Class	2U8G	For details about the dds mongos CPU and memory, see Cluster Instance Specifications . You can change the class of an instance after it is created. For details, see Changing the Instance Class .
dds mongos Nodes	2	The value ranges from 2 to 32. You can add nodes to an instance after it is created if necessary. For details, see Adding Cluster Instance Nodes .
shard Node Class	4U16G	For details about the shard CPU and memory, see Cluster Instance Specifications . The shard node stores user data but cannot be accessed directly. You can change the class of an instance after it is created. For details, see Changing the Instance Class .

Parameter	Example Value	Description
shard Storage Space	100GB	 The value ranges from 10 GB to 5,000 GB and must be a multiple of 10. You can scale up an instance after it is created. For details, see Scaling Up a Cluster Instance. NOTE 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.
shard Nodes	2	The value ranges from 2 to 32. You can add nodes to an instance after it is created if necessary. For details, see Adding Cluster Instance Nodes.
config Node Class	2U4G	For details about the CPU and memory of the config node, see Cluster Instance Specifications . You can change the class of an instance after it is created. For details, see Changing the Instance Class .
config Storage Space	20GB	Based on the functions and minimum requirements of the config node, the storage space of the config node is set to 20 GB by default. You cannot scale up the storage of the node after it is created.

Figure 2-2 Network, Required Duration, and Quantity



Parameter	Example Value	Description
VPC	default	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> .
		If no VPC is available or has been created, DDS allocates a VPC to you by default.
		NOTE After the DDS instance is created, the VPC cannot be changed.
Enterprise Project	default	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 . For more information about enterprise project, see Project Management in <i>Enterprise Management User Guide</i> .
		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> .

Table 2-2 Network settings

Step 3 On the displayed page, confirm the instance details.

- For yearly/monthly instances
 - 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.
- For pay-per-use instances
 - 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.
- **Step 4** Click **Back to Instance List**. 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 an automated backup policy by default, but you can disable it after an instance is created. After an instance is created, DDS automatically creates a full backup.

----End

Step 2: Connect to a Cluster Instance Through DAS

Data Admin Service (DAS) enables you to manage DB instances on a web-based console, simplifying database management and improving working efficiency. You can connect and manage instances through DAS. By default, you have the permission required for remote login. It is recommended that you use the DAS service to connect to DB instances. DAS is secure and convenient.

Procedure

Step 1 Log in to the management console.

Step 2 Click ¹ 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.

- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, locate the target DB instance and click **Log In** in the **Operation** column.

Alternatively, click the target instance on the **Instances** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner of the page.

- **Step 5** In the **Instance Login** dialog box, enter the correct information and click **Log In** to access and manage your database.
- **Step 6** After the login is successful, you can perform operations such as creating a database, managing accounts, and managing databases.

For details, see **Database Management**.

----End

3 Buying and Connecting to a Replica Set Instance

This section describes how to quickly purchase a replica set instance on the management console and how to connect to the replica set instance through DAS.

Operation Process

Process	Description
Preparations	Sign up for a HUAWEI ID, enable Huawei Cloud services, and make sure you have a valid payment method configured.
Step 1: Quickly Buy a Replica Set Instance	Select required basic settings and additional options and buy a DDS DB instance.
Step 2: Connect to a Replica Set Instance Through DAS	DAS provides a GUI and allows you to perform visualized operations on the console.

Preparations

- 1. Sign up for a HUAWEI ID and enable Huawei Cloud services.
- 2. For fine-grained permissions management on Huawei Cloud resources, use Identity and Access Management (IAM) to create a user or user group and grant it specific operation permissions. For details, see **Creating a User and Granting Permissions**.

Step 1: Quickly Buy a Replica Set Instance

- Step 1 Go to the Quick Config page.
- **Step 2** On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.

Basic Information Yearly/Monthly Pay-per-use Billing Mode Region other. For low network latency and quick resource access, select the nearest region Project cn north-4a cn-north-4b cn-north-4c AZ7 cn-north-4a,cn-north-4b,AZ7 Deploy your DB instance in a single AZ or three AZs for high availability. AZ Cluster Replica set Cloud native replica set Replica sets deliver reliability and disaster recovery, they can provide excellent reliability and are suitable for small and medium sized enterprises. DB Instance Type ⑦ Replica sets you can still create: 49. Increase Quota 5.0 Beta 4.4 4.2 4.0 3.4 Compatible MongoDB Version General-purpose Enhanced II Specifications Recommended Specifications Custom Medium- and Lightweight Databases 2 vCPUs | 8GB 2 vCPUs | 8GB v 100 GB Ultra-high I/O 10 GB Ultra-high I/O Maximum Connections: 1,000 Maximum Connections: 1,000 Currently selected dds.mongodb.c6.large.4.repset | 2 vCPUs | 8GB Disable Enable 🙆 📀 Disk Encryption

Figure 3-1 Basic configurations

Table 3-1 Basic configurations

Parame ter	Exampl e Value	Description
Billing	Pay- per-use	Select a billing mode, Yearly/Monthly or Pay-per-use.
Mode		For yearly/monthly instances
		 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 Yearly/Monthly to Pay-per-Use.
		NOTE 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.
		For pay-per-use instances
		 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 Pay-per-Use to Yearly/Monthly.

Parame ter	Exampl e Value	Description	
Region	CN- Hong Kong	The region where the resource is located. NOTE 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.	
Project	default	The project corresponds to the current region and can be changed.	
AZ	az1	 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. Instances can be deployed in a single AZ or three AZs. If your service requires low network latency between instances, you deploy the components of the instance in the same AZ. If you select a single AZ to deploy your instance, anti-affinity deployment is used by default. With an anti-affinity deployment, your primary, secondary, and hidden nodes are deployed on different physical machines for high availability. If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the primary, secondary, and hidden nodes are evenly distributed across three AZs. NOTE The 3-AZ deployment is not available in all regions. If the 3-AZ option is not displayed on the page for you to buy an instance, try a different region.	
DB Instance Type	Replica set	Select Replica set . A replica set consists of the primary node, secondary node, and hidden node. If a primary node goes down or becomes faulty, a secondary node is automatically assigned to the primary role and continues normal operation. If a secondary node is unavailable, a hidden node will take the role of the secondary to ensure high availability.	
Compati ble MongoD B Version	4.4	 5.0 4.4 4.2 4.0 3.4 	

Parame ter	Exampl e	l Description			
	Value				
CPU Type	x86	 DDS supports x86 and Kunpeng CPU architectures. NOTE This parameter is available only for MongoDB 4.0 and 3.4. You do not need to set this parameter for other versions. The default value is x86. 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.			
Specifica tions	Enhanc ed II (c6)	 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. 			
Recomm ended Specifica tions	2U8G	Currently, medium- and lightweight database specifications and customized specifications are supported. NOTE • The storage space ranges from 10 GB to 5,000 GB.			

Network						
VPC	default_wpc v Q Subnet Subnet V Q Security Group default_subnet V Q					
	A After the DDS instance is created, the VPC cannot be changed.					
	Available private IP addresses in the subnet: 235					
	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- View Project Management (5)					
Required Duration and Qua	Required Duration and Quantity					
Required Duration	1 2 3 4 5 6 7 8 9 months 1 year 🛄 2 years 🛄 3 years 🛍					
Quantity	Auto-renew Fee deduction and Renewal duration					
quantity	- I + O Tou can create 49 more up instances. Increase Quota					

Figure 3-2 Network, Required Duration, and Quantity

Parameter	Example Value	Description
VPC	default_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> .
		If no VPC is available or has been created, DDS allocates a VPC to you by default.
		NOTE After the DDS instance is created, the VPC cannot be changed.
Enterprise Project	default	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 . For more information about enterprise project, see Project Management in <i>Enterprise Management User</i> <i>Guide</i> .
		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 Management User Guide</i> .

 Table 3-2
 Network settings

Parameter	Exa mp le Val ue	Description
Required Duration	1 yea r	The system will automatically calculate the fee based on the validity period you have selected.
Auto-renew	Che ck the box	 By default, this option is not selected. If you select this option, the auto-renew cycle is determined by the length of the subscription.
Quantity	1	The purchase quantity depends on the replica set instance quota. If your current quota does not allow you to purchase the required number of instances, you can apply for increasing the quota as prompted. Yearly/Monthly instances that were purchased in batches have the same specifications except for the instance name and ID.

 Table 3-3 Required duration and quantity

Step 3 On the displayed page, confirm the instance details.

- For yearly/monthly instances
 - 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.
- For pay-per-use instances
 - 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.
- **Step 4** Click **Back to Instance List**. 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. After an instance is created, DDS automatically creates a full backup.

----End

Step 2: Connect to a Replica Set Instance Through DAS

Data Admin Service (DAS) enables you to manage DB instances on a web-based console, simplifying database management and improving working efficiency. You can connect and manage instances through DAS. By default, you have the permission required for remote login. It is recommended that you use the DAS service to connect to instances. DAS is secure and convenient.

Procedure

- Step 1 Log in to the management console.
- **Step 2** Click ^(Q) 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.

- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, locate the target DB instance and click **Log In** in the **Operation** column.

Alternatively, click the target DB instance on the **Instances** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner of the page.

Figure 3-3 Instance management

Renew Change to Yearly/Monthly Unsubs	icribe View	r Progress								
All projects v Q. Select one of	r more filters from 1	he pop-up lists. If yo	u enter a keyword	without a filter applied, the system will	I search for all insta	nce names matching this keyword.				000
NamedD 🕀	Description	DB Instanc	DB Engine	Status 🖯	Billing Mode	Connection Address Compatible with M	Enterprise	Tags	Operation	
	p	Replica set	5.0	 Available 	Pay-per-Use Created on	mongodb://iniuser. <password>@192.16)</password>	default	-	Log In View Metric More \sim	

Step 5 On the displayed login page, enter the administrator username and password and click **Log In**.

For details about how to manage databases through DAS, see **Database Management**.

----End

4 Getting Started with Clusters

4.1 Buying a Cluster Instance

4.1.1 Quick Config

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

Precautions

Each account can create up to 10 cluster instances.

Prerequisites

- You have registered a Huawei ID and enabled Huawei Cloud services.
- To display whether the disk is encrypted in the DB instance list, submit a service ticket. In the upper right corner of the management console, choose Service Tickets > Create Service Ticket.

Procedure

- **Step 1** Go to the **Quick Config** page.
- **Step 2** On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.

Basic Information	
Biling Mode	Yearly Menthy Psycon can
Region	
Project	regions are georgeface areas assessed from each driver. I or ow methods latercy and quick resource access, used the nearest region.
ΛZ	cm/sh/4a cm/rafh-4b cm/rafh-4b; AZ7 cm/rafh-4b;/AZ7 Desiry yang TB interven in a londer X7 at these X7 for birth a solubility.
DB Instance Type	Curcer Replica set Coud-nailwe replica set
	Cuarter one more rouais performance man replica sets and more revised is cuarting approach, i me regn-availability and revise scaling mey provide make mem an excelent, choice for large enterpreses. Cuarters of community edition you can still create: 10, horease Quota
Compatible MongoDB Version	50 2011 44 42 40 3.4
Specifications	General-Jurpose Enhanced II
Recommended Specifications	dd scoropos Nole 2 x/CNa 102B Utte high IO 4 x/CNa 102B Utte high IO Maximum Connections 10.00 Maximum Connections 2.000 Maximum Connections 4.000 Maximum Connections 10.00 Maximum Connections 10.00 Node 2 + The quarterly integes from 2 to 20. Currently integed with subgraph Amorgan 2 x/CNa 102B Utter high IO Node 4 x/CNa 102B Utter high IO Node 4 x/CNa 102B Utter high IO Node 1 x/CNa 102B Utter high IO
	Nodes - 2 + The quantify ranges from 2 to 64. Currently released data managaful di Jargan, 6.4 Juard 4 vCPUh 1008
	config
	Node Sunge Cases 4xCRUs 6 GB Space Space

Figure 4-1 Basic configurations

Table 4-1 Basic configurations

Parameter	Description		
Billing Mode	Select a billing mode, Yearly/Monthly or Pay-per-use.		
	For yearly/monthly instances		
	 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 Yearly/ Monthly to Pay-per-Use. 		
	NOTE 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.		
	For pay-per-use instances		
	 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 Pay-per-Use to Yearly/Monthly. 		

Parameter	Description
Region	The region where the resource is located. NOTE 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.
Project	The project corresponds to the current region and can be changed.
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. Instances can be deployed in a single AZ or three AZs. NOTE The 3-AZ deployment is not available in all regions. If the 3-AZ option is not displayed on the page for you to buy an instance, try a different region. If your service requires low network latency between instances, you deploy the components of the instance in the same AZ. If you select a single AZ to deploy your instance, anti-affinity deployment is used by default. With an anti-affinity deployment, your primary, secondary, and hidden nodes are deployed on different physical machines for high availability. If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the dds mongos, shard, and config nodes are evenly distributed across the three AZs.
DB Instance Type	Select Cluster . A cluster instance includes three types of nodes: dds mongos, shard, and config. Each shard and config is a three-node replica set to ensure high availability.
Compatible MongoDB Version	 5.0 4.4 4.2 4.0 3.4

Parameter	Description	
CPU Type	 DDS supports x86 and Kunpeng CPU architectures. NOTE This parameter is available only for MongoDB 4.0 and 3.4. You do not need to set this parameter for other versions. The default value is x86. 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 lightworkload 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 ultrahigh 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. For details about the supported instance specifications, see Cluster Instance Specifications. 	
dds mongos Node Class	For details about the dds mongos CPU and memory, see Cluster Instance Specifications. You can change the class of an instance after it is created. For details, see Changing the Instance Class.	
dds mongos Nodes	The value ranges from 2 to 32. You can add nodes to an instance after it is created if necessary. For details, see Adding Cluster Instance Nodes.	

Parameter	Description
shard Node Class	For details about the shard CPU and memory, see Cluster Instance Specifications . The shard node stores user data but cannot be accessed directly. You can change the class of an instance after it is created. For details, see Changing the Instance Class .
shard Storage Space	 The value ranges from 10 GB to 5,000 GB and must be a multiple of 10. You can scale up an instance after it is created. For details, see Scaling Up a Cluster Instance. NOTE 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.
shard Nodes	The value ranges from 2 to 32. You can add nodes to an instance after it is created if necessary. For details, see Adding Cluster Instance Nodes.
config Node Class	For details about the CPU and memory of the config node, see Cluster Instance Specifications. You can change the class of an instance after it is created. For details, see Changing the Instance Class.
config Storage Space	Based on the functions and minimum requirements of the config node, the storage space of the config node is set to 20 GB by default. You cannot scale up the storage of the node after it is created.

Figure 4-2 Network, Required Duration, and Quantity

Network	
VPC	default_ypc v Q Submet/ default_submitteeting v Q Security Group default_submitteeting Q
	After the DDS instance is created, the VPC cannot be changed.
	Available private IP addresses in the subnet: 148
	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- View Project Management
Required Duration and Quant	ity
Required Duration	1 2 3 4 5 6 7 8 9 months 1 year 🖬 2 years 🖬 3 years 🖬
	Auto-renew Fee deduction and Renewal duration
Quantity	- 1 +) You can create 10 more DB instances. Increase Quota

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</i> <i>Guide</i> . For details about the constraints on the use of VPCs, see Connection Methods .
	If there are no VPCs available, DDS creates one for you by default.
	NOTE 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 . For more information about enterprise project, see Project Management in <i>Enterprise Management User Guide</i> .
	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 Management User Guide</i> .

Table 4-2 Network settings

Table 4-3 Required	duration	and	quantity
--------------------	----------	-----	----------

Parameter	Description
Required Duration	The length of your subscription if you select Yearly/Monthly billing. Subscription lengths range from one month to three years.
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.
Quantity	The purchase quantity depends on the cluster 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.

Step 3 On the displayed page, confirm the instance details.

• For yearly/monthly instances

- 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.
- For pay-per-use instances
 - 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.
- **Step 4** Click **Back to Instance List**. 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.

----End

4.1.2 Custom Config

This section describes how to purchase a cluster instance in custom mode on the management console. You can customize the computing resources and storage space of a cluster 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 10 cluster instances.

Prerequisites

- You have registered a Huawei ID and enabled Huawei Cloud services.
- To display whether the disk is encrypted in the DB instance list, submit a service ticket. In the upper right corner of the management console, choose Service Tickets > Create Service Ticket.

Procedure

- **Step 1** Go to the **Custom Config** page.
- **Step 2** On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.

Basic Information		
Billing Mode	Yearly/Monthly Pay-per-use	
Region	······································	
	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 AZ4 AZ1.AZ2.AZ3 Deploy your OB instance in a single AZ or three AZs for high availability.	
D8 Instance Name	dd#-8591	
DB Instance Type	Cluster Replica set Cloud native 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 oreate: 10. Increase Quota	e them an excellent choice for large enterprises.
Compatible MongoDB Version	50 244 42 40 3.4	
Storage Type	Ultra-High I/O	
Specifications	General-purpose Entranced E	
dds mongos		
Note Store	-ANT Houses	Malaum Consultant
Node Class	v.rpu wemory v.rpu 3 08	2.000
		4000
	0 8 x 29 lin 132 68	14.000
		14.000
	22/CPI/N 128/GB	14.000
		48.000
	Currently selected dds.mongodb.c8.large.4.mongos 2 vCPUs 8 GB	
Nodes	z + The quantity ranges from 2 to 32.	
Parameter Template	Default-DDS-4-4-Mongos v Q View Parameter Template	
shard		
Node Class	vCPU Memory	Maximum Connections
	2 vCPUs 8 GB	2.000
	2 vCPUs 18 GB	2.000
	4 vCPUs 18 GB	4.000
	4 vCPUs [32:08	4.000
	0 8 vCPUs 132 08	10,000
	0 8 vCPUs (84 GB	18,000
	0 16 VCPUs 64 GB	18,000
	Currently selected dds.mongodb.o0Jarge.4.shard 2 vCPUs 8 GB	
	10 08	
Storage Space		10 + GB (0)
	10 500 1000 1500 2000 2500 3000 4000 4800 5000 7 To ensure that the DR instance can still be used if the storace scare is about to be used up the database is set to reach only and data cannot be more 5 <th>Steel If this hanners, you can add more storage to restore the database to read/artie status</th>	Steel If this hanners, you can add more storage to restore the database to read/artie status
Nodes	2 + The quantity ranges from 2 to 32.	
Parameter Template	Dataut-DDS-4.4-Shard v Q View Parameter Template	
config		
Node Class	2 vOPUs 4 GB	
	Currently selected dds.mongodb.o0.large.2.config 2 vCPUs 4 GB	
ovorage space	20.08	
Parameter Template	Default-DDS-4.4Config View Parameter Template	
Disk Encryption	Duable Enable Ó 🕥	

Figure 4-3 Basic configurations

Parameter	Description
Billing Mode	Select a billing mode, Yearly/Monthly or Pay-per-use.
	For yearly/monthly instances
	 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 Yearly/ Monthly to Pay-per-Use.
	NOTE 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.
	For pay-per-use instances
	 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 Pay-per-Use to Yearly/Monthly.
Region	The region where the resource is located.
	NOTE 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.
Project	The project corresponds to the current region and can be changed.

Table 4-4 Basic configurations

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.
	Instances can be deployed in a single AZ or three AZs.
	• If your service requires low network latency between instances, you deploy the components of the instance in the same AZ. If you select a single AZ to deploy your instance, anti-affinity deployment is used by default. With an anti-affinity deployment, your primary, secondary, and hidden nodes are deployed on different physical machines for high availability.
	• If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the dds mongos, shard, and config nodes are evenly distributed across the three AZs.
	NOTE The 3-AZ deployment is not available in all regions. If the 3-AZ option is not displayed on the page for you to buy an instance, try a different region.
DB 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.
	• The instance name can be the same as an existing instance name.
	 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 gets 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	Select Cluster .
Туре	A cluster instance includes three types of nodes: dds mongos, shard, and config. Each shard and config is a three-node replica set to ensure high availability.

Parameter	Description
Compatible MongoDB Version	 5.0 4.4 4.2 4.0 3.4
CPU Type	 DDS supports x86 and Kunpeng CPU architectures. NOTE This parameter is available only for MongoDB 4.0 and 3.4. You do not need to set this parameter for other versions. The default value is x86. 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.
Storage Type	 The storage type can be Ultra-high I/O and Extreme SSD for non-DeC users. For DeC users, the supported storage types depend on the selected resource type. If you select EVS for Resource Type, Storage Type is set to Cloud SSD. If you select DSS for Resource Type, Storage Type can be set to Common I/O, High I/O, or Cloud SSD.
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 and 4.4. 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.

Parameter	Description
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 lightworkload 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 ultrahigh 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.
	Cluster Instance Specifications.
dds mongos Node Class	For details about the dds mongos CPU and memory, see Cluster Instance Specifications. You can change the class of an instance after it is created. For details, see Changing the Instance Class.
dds mongos Nodes	The value ranges from 2 to 32. You can add nodes to an instance after it is created if necessary. For details, see Adding Cluster Instance Nodes.
dds mongos Parameter Template	The parameters that apply to the dds mongos nodes. After an instance is created, you can change the parameter template of a node to bring out the best performance. For details, see Editing a Parameter Template .
shard Node Class	For details about the shard CPU and memory, see Cluster Instance Specifications . The shard node stores user data but cannot be accessed directly. You can change the class of an instance after it is created. For details, see Changing the Instance Class .
shard Storage Space	The value ranges from 10 GB to 5,000 GB and must be a multiple of 10. You can scale up an instance after it is created. For details, see Scaling Up a Cluster Instance . NOTE 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.

Parameter	Description
shard Nodes	The value ranges from 2 to 32. You can add nodes to an instance after it is created if necessary. For details, see Adding Cluster Instance Nodes.
shard Parameter Template	The parameters that apply to the shard nodes. After an instance is created, you can change the parameter template of a node to bring out the best performance. For details, see Editing a Parameter Template .
config Node Class	For details about the CPU and memory of the config node, see Cluster Instance Specifications. You can change the class of an instance after it is created. For details, see Changing the Instance Class.
config Storage Space	Based on the functions and minimum requirements of the config node, the storage space of the config node is set to 20 GB by default. You cannot scale up the storage of the node after it is created.
config Parameter Template	The parameters that apply to the config nodes. After an instance is created, you can change the parameter template of a node to bring out the best performance. For details, see Editing a Parameter Template .
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. NOTE 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. To check whether the disk is encrypted, you can view Disk Encrypted in the DB instance list. 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 Data Encryption Workshop User Guide.
	 Data Encryption vvorksnop User Guide. Disk encryption supports only the AES_256 key algorithm.

Figure 4-4 Administrator settings

Administrator			
Password	Configure	Skip	
Administrator	rwuser		
New Password			0
Confirm Password			8

Table 4-5 Administrator settings

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 choose More > 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.

Network	
VPC	default_vpc
	After the DDS instance is created, the VPC cannot be changed.
Subnet	default_subnet
	Available private IP addresses in the subnet: 148
Security Group	default
	In a security group, rules that authorize connections to DB instances apply to all DB instances associated with the security group.
SSL	To encrypt transmission, enable SSL
Database Port	Default port: 8635
Enterprise Project	
Enterprise Project	
Enterprise Project	Select- View Project Management (9)
Required Duration and Quant	ity
Required Duration	1 2 3 4 5 6 7 8 9 months 1 year 🛄 2 years 🛄 3 years 🛍
	Auto-renew Fee deduction and Renewal duration
Quantity	- 1 + O You can create 10 more DB instances. Increase Quota

Figure 4-5 Network and required duration

Table 4-6 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 about how to create a VPC, see "Creating a VPC" in <i>Virtual</i> <i>Private Cloud User Guide</i> . For details about the constraints on the use of VPCs, see Connection Methods .
	If there are no VPCs available, DDS creates one for you by default.
	VPC owners can share the subnets in a VPC with one or multiple accounts through Resource Access Manager (RAM). This allows for more efficient use of network resources and reduces O&M costs.
	For more information about VPC subnet sharing, see VPC Sharing in the Virtual Private Cloud User Guide.
	NOTE 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 .
	NOTE Both IPv4 and IPv6 subnets are supported.
Parameter	Description
-----------------------	--
Security Group	A security group controls access between DDS and other services. If there are no security groups available, DDS creates one for you by default. NOTE
	• 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.
	 When creating a DB instance, you can select multiple security groups. For better network performance, you are advised to select no more than five security groups. In such a case, the access rules of all the selected security groups apply on the instance.
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.
	 The database port is the port of the dds mongos node. The default port is 8635. To change the port, see Changing a Database Port.
	• The shard node port is 8637, and the config node port is 8636, which cannot be changed. For details about how to connect to the shard and config nodes, see Enabling IP Addresses of Shard and Config Nodes .
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 . For more information about enterprise project, see <i>Enterprise Management User Guide</i> .

Figure 4-6 Advanced settings

Advanced Settings	
Show Original Log	0
Automated Backup	0
Retention Period	- 7 + Enter an integer from 1 to 732.
Time Window	00:00 - 01:00 V GMT+08:00
Maintenance Window	Skip Configure ③
Tags	Predefined tags are recommended for adding the same tag to different cloud resources. Create Predefined Tag C View predefined tags
	Tag key Tag value
	You can add 20 more tags.

Table 4-7 Advanced settings

Parameter	Description
Show Original Log	If Show Original Log is enabled, the original slow query logs will be displayed, and the logs will be transferred to an OBS bucket. By default, the system automatically deletes logs from the OBS bucket after 30 days, and the retention period cannot be changed.
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.
	Principal Principal Actionated Dackup Folicy.
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	A one-hour period the backup will be scheduled within 24 hours, such as 01:00-02:00. The backup time is in UTC format.

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.
	If your organization has configured tag policies for DDS, add tags to DB instances based on the policies. If a tag does not comply with the policies, DB instance creation may fail. Contact your organization administrator to learn more about tag policies.
	• 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 must consist of only 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**.

NOTE

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.

Step 3 On the displayed page, confirm the instance details.

- For yearly/monthly instances
 - 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.
- For pay-per-use instances
 - 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.
- **Step 4** Click **Back to Instance List**. 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.
 - ----End

4.2 Connecting to a Cluster Instance

4.2.1 Connection Methods

You can access DDS over private or public networks.

Table 4-8 Connection methods

Method	IP Address	Scenario	Description
DAS	Not required	DAS provides a GUI and allows you to perform visualized operations on the console. SQL execution, advanced database management, and intelligent O&M are all available to make database management simple, secure, and intelligent. By default, the permission to connect to DAS is enabled.	 Easy to use, secure, advanced, and intelligent Recommended

Method	IP Address	Scenario	Description
Private network	Private IP address	DDS provides a private IP address by default. If your applications are running on an ECS in the same region and VPC as your DDS instance, you are advised to use a private IP address to connect the ECS to your DDS instances.	 Secure and excellent performance For faster transmission and improved security, you are advised to migrate your applications to an ECS that is in the same subnet as your DDS instance and use a private IP address to access the instance.
Public network	EIP	 If your applications are running on an ECS that is in a different region from the one where the DDS instance is located, use an EIP to connect the ECS to your DDS instances. If you use a third-party device or your local device to connect to a DDS instance, you can use an EIP to connect to the DB instance. 	• Low security

4.2.2 (Recommended) Connecting to Cluster Instances Through DAS

4.2.2.1 Overview

DAS provides a GUI and allows you to perform visualized operations on the console. SQL execution, advanced database management, and intelligent O&M are all available to make database management simple, secure, and intelligent. You are advised to use DAS to connect to instances.

This section describes how to buy a cluster instance on the management console and how to connect to the cluster instance through DAS.

Process

To purchase and connect to a cluster instance, perform the following steps:

- 1. Buy a cluster instance.
- 2. Connect to the cluster instance through DAS.

4.2.2.2 Connecting to a Cluster Instance Through DAS

Data Admin Service (DAS) enables you to manage DB instances on a web-based console, simplifying database management and improving working efficiency. You can connect and manage instances through DAS. By default, you have the permission required for remote login. It is recommended that you use the DAS service to connect to DB instances. DAS is secure and convenient.

Procedure

Step 1 Log in to the management console.

Step 2 Click ¹ 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.

- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, locate the target DB instance and click **Log In** in the **Operation** column.

Alternatively, click the target instance on the **Instances** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner of the page.

- **Step 5** In the **Instance Login** dialog box, enter the correct information and click **Log In** to access and manage your database.
- **Step 6** After the login is successful, you can perform operations such as creating a database, managing accounts, and managing databases.

For details, see Data Management.

----End

4.2.3 Connecting to a Cluster Instance over a Private Network

4.2.3.1 Configuring Security Group Rules

A security group is a collection of access control rules for ECSs and DDS instances that have the same security protection requirements and are mutually trusted in a VPC.

To ensure database security and reliability, you need to configure security group rules to allow specific IP addresses and ports to access DDS instances.

You can connect to an instance by configuring security group rules in following two ways:

• If the ECS and instance are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to Connecting to a Cluster Instance Using Mongo Shell (Private Network).



Figure 4-7 Same security group

• If the ECS and instance are in different security groups, you need to configure security group rules for them, separately.

Figure 4-8 Different security groups



- Instance: Configure an **inbound rule** for the security group associated with the instance.
- ECS: The default security group rule allows all outbound data packets. In this case, you do not need to configure a security group rule for the ECS. If not all traffic is allowed to reach the instance, configure an **outbound** rule for the ECS.

This section describes how to configure an **inbound** rule for an instance.

Precautions

• By default, an account can create up to 500 security group rules.

- Too many security group rules will increase the first packet latency, so a maximum of 50 rules for each security group is recommended.
- By default, one DDS instance is associated with only one security group.
- DDS allows you to associate multiple security groups to a DB instance. You can apply for the service based on your service requirements. For better network performance, you are advised to select no more than five security groups.

Procedure

- Step 1 Log in to the management console.
- **Step 2** Click ^(Q) in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the instance name. The **Basic Information** page is displayed.
- **Step 5** In the **Network Information** area on the **Basic Information** page, click the security group.

Figure 4-9 Security Group

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

You can also choose **Connections** in the navigation pane on the left. On the **Private Connection** tab, in the **Security Group** area, click the security group name.

Figure 4-10 Security Group

Security Group		
Security Group	default 🖉	
Inbound Rules(6)	Outbound Rules(3)	
Security Group	Protocol & Port (?)	Туре
default	TCP:22	IPv4

- **Step 6** On the **Security Group** page, locate the target security group and click **Manage Rule** in the **Operation** column.
- **Step 7** On the **Inbound Rules** tab, click **Add Rule**. The **Add Inbound Rule** dialog box is displayed.
- **Step 8** Add a security group rule as prompted.

Figure 4-11 Add Inbound Rule

Add Inbound Rule Learn more about security group configuration.	×
Some security group rules will not take effect for ECSs with certain specifications. Learn more If you select IP address for Source, you can enter multiple IP addresses, separated with commas (.). Each IP address represents a different security group rule.	
Security Group default You can import multiple rules in a batch. Priority (2) Action (2) Type Protocol & Port (2) Source (2) Description Operation	
1-100 Allow ~ IPv4 ~ IP address ~ Replicate Delete Example: 22 or 22,24 or 22-3 0.0.0.00 × Replicate Delete	
Add Rule Cancel OK	

Table 4-9 Inbound rule settings

Paramete r	Description	Example
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	The security group rule actions. A rule with a deny action overrides another with an allow action if the two rules have the same priority.	Allow
Protocol & Port	The network protocol required for access. Available options: TCP , UDP , ICMP , or GRE	ТСР
	Port: the port on which you wish to allow access to DDS. The default port is 8635. The port ranges from 2100 to 9500 or can be 27017, 27018, or 27019.	8635
Туре	IP address type. Only IPv4 and IPv6 are supported.	IPv4

Paramete r	Description	Example
Source	Specifies the supported IP address, security group, and IP address group, which allow access from IP addresses or instances in other security group. Example:	0.0.0/0
	• Single IP address: 192.168.10.10/32	
	• IP address segment: 192.168.1.0/24	
	All IP addresses: 0.0.0.0/0	
	 Security group: sg-abc 	
	 IP address group: ipGroup-test 	
	If you enter a security group, all ECSs associated with the security group comply with the created rule.	
	For more information about IP address groups, see IP Address Group.	
Descriptio n	(Optional) Provides supplementary information about the security group rule. This parameter is optional.	-
	The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	

Step 9 Click OK.

----End

4.2.3.2 Connecting to a Cluster Instance Using Mongo Shell (Private Network)

Mongo shell is the default client for the MongoDB database server. You can use Mongo Shell to connect to DB instances, and query, update, and manage data in databases. DDS is compatible with MongoDB. Mongo Shell is a part of the MongoDB client. To use Mongo Shell, download and install the MongoDB client first, and then use the Mongo shell to connect to the DB instance.

By default, a DDS instance provides a private IP address. If your applications are deployed on an ECS and are in the same region and VPC as DDS instances, you can connect to DDS instances using a private IP address to achieve a fast transmission rate and high security.

This section describes how to use Mongo Shell to connect to a cluster instance over a private network.

You can connect to an instance using an SSL connection or an unencrypted connection. The SSL connection is encrypted and more secure. To improve data transmission security, connect to instances using SSL.

Prerequisites

- 1. For details about how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
- Install the MongoDB client on the ECS. To ensure successful authentication, install the MongoDB client of the same version as the target instance.
 For details about how to install a MongoDB client, see How Can I Install a MongoDB Client?
- 3. The ECS can communicate with the DDS instance. For details, see **Configuring Security Group Rules**.

SSL Connection

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

- Step 1 Log in to the management console.
- **Step 2** Click ^(Q) in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the instance name.
- **Step 5** In the navigation pane on the left, choose **Connections**.
- **Step 6** In the **Basic Information** area, click \perp next to the **SSL** field.
- **Step 7** Upload the root certificate to the ECS to be connected to the instance.

The following describes how to upload the certificate to a Linux and Windows ECS:

• In Linux, run the following command:

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

D NOTE

- **IDENTITY_FILE** is the directory where the root certificate resides. The file access permission is 600.
- **REMOTE_USER** is the ECS OS user.
- **REMOTE_ADDRESS** is the ECS address.
- **REMOTE_DIR** is the directory of the ECS to which the root certificate is uploaded.
- In Windows, upload the root certificate using a remote connection tool.
- **Step 8** Connect to the instance in the directory where the MongoDB client is located.

Method 1: Using the private HA connection address (recommended)

DDS provides a private HA connection address that consists of IP addresses and ports of all dds mongos nodes in a cluster instance. You can use this address to connect to the cluster instance to improve availability of the cluster instance.

Example command:

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

Parameter description:

Drivate Connection Dublic Connection

• **Private HA Connection Address**: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 4-12 Obtaining the private HA connection address

	rubic 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

The format of the private HA connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

Pay attention to the following parameters in the private HA address:

Table 4-10 Parameter information

Parameter	Description
rwuser	Database username
<password></password>	Password for the database username. Replace it with the actual password.
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively.
	For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25*** %21%24 .

Parameter	Description
192.168.***.***:8635,192. 168.***.***:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user rwuser must be admin . authSource=admin is fixed in the command.

- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and bandwidth, the cluster certificate is generated using the internal management IP address. --sslAllowInvalidHostnames is needed for the SSL connection through a private network.

Command example:

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

Method 2: Using the private HA connection address (user-defined database and account)

Example command:

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

Parameter description:

• **Private HA Connection Address**: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 4-13 Obtaining the private HA connection address

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 I Address	۹			
Address				
Cross-CIDR Access	Disabled Enable			
Private HA Connectio	n Address mongodb://rwuser: <password>@*</password>		/test?authSource=admin&replicaSet=replica 🗇 L	earn more

The format of the obtained private HA connection address is as follows:

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

The following table lists the required parameters in the private HA address.

Parameter	Description
rwuser	Database username. The default value is rwuser . You can change the value to the username based on your service requirements.
<password></password>	Password for the database username. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25***
192.168.***.***:8635,192. 168.***.***:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user rwuser is admin . NOTE If you use a user-defined database for authentication, change the authentication database in the HA connection address to the name of the user-defined database. In addition, replace rwuser with the username created in the user-defined database.

 Table 4-11
 Parameter information

- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and bandwidth, the cluster certificate is generated using the internal management IP address. --sslAllowInvalidHostnames is needed for the SSL connection through a private network.

For example, if you create a user-defined database **Database** and user **test1** in the database, the connection command is as follows:

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

Method 3: Using a private IP address

Example command:

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

Parameter description:

 DB_HOST is the IP address of the dds mongos node of the cluster instance to be connected.

Click the instance name. On the **Basic Information** page, choose **Connections** > **Private Connection**, obtain the private IP address of the dds mongos node on the **dds mongos** tab in the **Node Information** area.

Figure 4-14 Obtaining the private IP address

Basic Informa	tion				
Database Port	8635	0.		VPC	dds-st-test-vpc
SSL	0	÷		Subnet	dds-st-lest-subnet
Address					
Private HA Conne	ection Address Co	ompatible with MongoDB	mongodb://rwuser: <pass< td=""><td>word>@102010000000</td><td>Control Control Contro</td></pass<>	word>@102010000000	Control Contro
			Note The parameters	in orange are variables and ne	ed to be modified based on service requirements. For details, click Lea
Node Informat	tion				
dds mongos	shard	config			
Name/ID	AZ	Private IP Address	EIP	Operation	
dds-5c63 72656654	az2	195	Outpound	Change Private IP Address	Sind EIP
dds-5c63 6f493319e	az2	193338888888	S Unbound	Change Private IP Address	Bind EIP

• **DB_PORT** is the port of the instance to be connected. The default port is 8635.

Click the instance name. On the **Basic Information** page, choose **Connections**. On the **Private Connection** tab, obtain the database port information in the **Database Port** field in the **Basic Information** area.

Figure 4-15 Obtaining the port

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

- **DB_USER** is the database user. The default value is **rwuser**.
- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and bandwidth, the cluster certificate is generated using the internal management IP address. --sslAllowInvalidHostnames is needed for the SSL connection through a private network.

Enter the database account password when prompted:

Enter password:

Command example:

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

Step 9 Check the connection result. If the following information is displayed, the connection is successful. mongos>

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

- **Step 1** Connect to the ECS.
- **Step 2** Connect to the instance in the directory where the MongoDB client is located.

Method 1: Private HA connection address (recommended)

Example command:

./mongo "<Private HA Connection Address>"

Private HA Connection Address: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 4-16 Obtaining the private HA connection address

Private Co	nnection	Public Connection				
Basic I	nformation					
Databa	se Port	8635 🖉		VPC	dds-st-test-vpc	
SSL		<u> </u>		Subnet	dds-st-test-subnet-2 ()
Auto-sv Address	witch Private IP					
Addre	55					
Cross-C	IDR Access	Disabled Enable				
Private	HA Connection A	ddress mongodb://rwuser:	<password>@1</password>		/test?authSource=admin&replicaSet=re	plica 🗇 Learn more

The format of the private HA connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

The following table lists the required parameters in the private HA address.

Parameter	Description
rwuser	Database username
<password></password>	Password for the database username. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25***%21%24.
192.168.***.***:8635,192.1 68.***.***:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user rwuser must be admin . authSource=admin is fixed in the command.

Table 4-12 Parameter information

Command example:

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

Method 2: Private HA connection (user-defined database and account)

Example command:

./mongo "<Private HA Connection Address>"

Private HA Connection Address: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 4-17 Obtaining the private HA connection address

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

The format of the obtained private HA connection address is as follows:

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

The following table lists the required parameters in the private HA address.

Parameter	Description
rwuser	Database username. The default value is rwuser . You can change the value to the username based on your service requirements.
<password></password>	Password for the database username. Replace it with the actual password.
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25***%21%24 .
192.168.***.***:8635,192.1 68.***.***:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user rwuser is admin . NOTE If you use a user-defined database for authentication, change the authentication database in the HA connection address to the name of the user-defined database. In addition, replace rwuser with the username created in the user-defined database.

 Table 4-13 Parameter information

For example, if you create a user-defined database **Database** and user **test1** in the database, the connection command is as follows:

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

Method 3: Using a private IP address

Example command:

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

Parameter description:

 DB_HOST is the IP address of the dds mongos node of the cluster instance to be connected.

Click the instance name. On the **Basic Information** page, choose **Connections** > **Private Connection**, obtain the private IP address of the dds mongos node on the **dds mongos** tab in the **Node Information** area.

Figure 4-18 Obtaining the private IP address

Basic Informa	tion				
Database Port	8635 0	2		VPC	dds-st-test-vpc
SSL		÷		Subnet	dds-st-test-subnet
Address					
Private HA Conne	ction Address Co	mpatible with MongoDB	mongodb://rwuser: <pass< td=""><td>word>@1027199799792090099</td><td>Service Contract Contra</td></pass<>	word>@1027199799792090099	Service Contract Contra
			Note The parameters	s in orange are variables and ne	ed to be modified based on service requirements. For details, click Lea
Node Informat	tion				
dds mongos	shard	config			
Name/ID	AZ	Private IP Address	EIP	Operation	
dds-5c63 72656654	az2	19:2000000000000000000000000000000000000	S Unbound	Change Private IP Address	Bind EIP
dds-5c63 6f493319e	az2	19200000000	Our Control of Cont	Change Private IP Address	Bind EIP

• **DB_PORT** is the port of the instance to be connected. The default port is 8635.

Click the instance name. On the **Basic Information** page, choose **Connections**. On the **Private Connection** tab, obtain the database port information in the **Database Port** field in the **Basic Information** area.

Figure 4-19 Obtaining the port

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

• **DB_USER** is the database user. The default value is **rwuser**.

Enter the database password when prompted: Enter password:

Command example:

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

Step 3 Check the connection result. If the following information is displayed, the connection is successful.

mongos>

4.2.3.3 Connecting to Read Replicas Using Mongo Shell

Mongo shell is the default client for the MongoDB database server. You can use Mongo Shell to connect to DB instances, and query, update, and manage data in databases. DDS is compatible with MongoDB. Mongo Shell is a part of the MongoDB client. To use Mongo Shell, download and install the MongoDB client first, and then use the Mongo shell to connect to the DB instance.

By default, a DDS instance provides a private IP address. If your applications are deployed on an ECS and are in the same region and VPC as DDS instances, you can connect to DDS instances using a private IP address to achieve a fast transmission rate and high security.

This section describes how to use Mongo Shell to connect to a read replica over a private network.

You can connect to a read replica using an SSL connection or an unencrypted connection. The SSL connection is encrypted and more secure. To improve data transmission security, connect to instances using SSL.

Prerequisites

- 1. For details about how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
- Install the MongoDB client on the ECS. To ensure successful authentication, install the MongoDB client of the same version as the target instance.
 For details about how to install a MongoDB client, see How Can I Install a MongoDB Client?
- 3. The ECS can communicate with the DDS instance. For details, see **Configuring Security Group Rules**.

SSL Connection

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

- **Step 1** On the **Instances** page, click the instance name.
- **Step 2** In the navigation pane on the left, choose **Connections**.
- **Step 3** In the **Basic Information** area, click $\stackrel{1}{
 m the}$ next to the **SSL** field.
- **Step 4** Upload the root certificate to the ECS to be connected to the instance.

The following describes how to upload the certificate to a Linux and Window ECS:

 In Linux, run the following command: scp<IDENTITY_FILE><REMOTE_USER>@<REMOTE_ADDRESS>:<REMOTE_DIR>

D NOTE

- **IDENTITY_FILE** is the directory where the root certificate resides. The file access permission is 600.
- **REMOTE_USER** is the ECS OS user.
- **REMOTE_ADDRESS** is the ECS address.
- **REMOTE_DIR** is the directory of the ECS to which the root certificate is uploaded.
- In Windows, upload the root certificate using a remote connection tool.
- **Step 5** Connect to a DDS instance. The DDS console provides the read replica connection address. You can use this address to connect to the read replica.

Example command:

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

Parameter description:

 Read Replica Connection Address: On the Instances page, click the instance to go to the Basic Information page. Choose Connections. Click the Private Connection tab. In the Address area, obtain the connection address of the read replica instance.

Figure 4-20 Obtaining the read replica connection address

vate Connection Public Conn	nection		
Basic Information			
Database Port 8635 🖉		VPC	dds-st-test-vpc
SSL		Subnet	dds-st-test-subnet (192.168.0.0/16)
Address			
Private HA Connection Address	mongodb://rwuser: *password>@192.168.187.18 6	6:8635,192.168.138.117:8635	/test?authSource=admin 📑 Learn more
Read Replica Connection Address 1	mongodb://rwuser: <password>@192.168.187.188 eadPreferenceTags=role:readonly</password>	5:8635,192.168.138.117:8635	inest?authSource=admin&readPreference=secondaryPreferred
Read Replica Connection Address 2	mongodb://rwuser: <password>@192.168.187.186 eadPreferenceTags=role:readonly&readPreference</password>	5:8635,192.168.138.117:8635 eTags= 디	Grest?authSource=admin&readPreference=secondaryPreferred&
	Note The parameters in orange are variables a plica connection address 2 cannot be used to con ce logged in using read replica connection addres nce logged in using read replica connection addres	and need to be modified base nect to a DB instance through s 1 is as follows: read replica ss 2 is as follows: read replic	d on service requirements. For details, click Learn more. Read n Mongo Shell. The read priority (from high to low) for a DB inst , primary node. The read priority (from high to low) for a DB inst a, secondary node, primary node.

The format of the read replica connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

mongodb://rwuser:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/test? authSource=admin&readPreference=secondaryPreferred&readPreferenceT ags=role:readonly

Pay attention to the following parameters in the read replica connection address:

Parameter	Description
rwuser	Account name, that is, the database username.
<password></password>	Password for the database account. Replace it with the actual password.
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively.
	For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25*** %21%24 .
192.168.xx.xx:8635,192.1 68.xx.xx:8635	IP address and port of the mongos node of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user rwuser must be admin . authSource=admin is fixed in the command.

Table 4-14 Parameter description

- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and bandwidth, the cluster certificate is generated using the internal management IP address. --sslAllowInvalidHostnames is needed for the SSL connection through a private network.

Command example:

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

NOTE

When connecting to an instance using the read replica connection address, add double quotation marks (") before and after the connection information.

If the following information is displayed, the instance is successfully connected: mongos>

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

- **Step 1** Log in to the ECS.
- **Step 2** Connect to a DDS instance. The DDS console provides the read replica connection address. You can use this address to connect to the read replica.

Example command:

./mongo "<Read replica connection address>"

Read Replica Connection Address: On the **Instances** page, click the instance to go to the **Basic Information** page. Choose **Connections**. Click the **Private Connection** tab. In the **Address** area, obtain the connection address of the read replica instance.

Figure 4-21 Obtaining the read replica connection address

Basic Information				
Database Port	8635 🖉		VPC	dds-st-test-vpc
SSL		<u>د</u>	Subnet	dds-st-test-subnet (192.168.0.0/16)
Address				
Private HA Connection Addr	ress	mongodb://rwuser: <password>@192.168.187.1</password>	86:8635,192.168.138.117:86	335/test?authSource=admin 🗇 Learn more
Read Replica Connection A	ddress 1	mongodb://rwuser: <password>@192.168.187.1 eadPreferenceTags=role:readonly</password>	86:8635,192.168.138.117:86	335/test?authSource=admin&readPreference=secondaryPreferrer
Read Replica Connection A	ddress 2	mongodb://rwuser: <password>@192.168.187.1 eadPreferenceTags=role:readonly&readPrefere</password>	86:8635,192.168.138.117:86 nceTags= 🗇	335/1est?authSource=admin&readPreference=secondaryPreferrec
		Note The parameters in orange are variable plica connection address 2 cannot be used to c ce logged in using read replica connection addr nce logged in using read replica connection addr	s and need to be modified by onnect to a DB instance thro ess 1 is as follows: read repl lress 2 is as follows: read rep	ased on service requirements. For details, click Learn more. Reac ugh Mongo Shell. The read priority (from high to low) for a DB ins ica, primary node. The read priority (from high to low) for a DB ins lica, secondary node, primary node.

The format of the read replica connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

mongodb://rwuser:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/test? authSource=admin&readPreference=secondaryPreferred&readPreferenceTags= role:readonly

Pay attention to the following parameters in the private HA address:

Parameter	Description
rwuser	Account name, that is, the database username.
<password></password>	Password for the database account. Replace it with the actual password.
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively.
	For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25*** %21%24 .
192.168.xx.xx:8635,192.168 .xx.xx:8635	IP address and port of the mongos node of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user rwuser must be admin . authSource=admin is fixed in the command.

Table 4-15	Parameter	description
-------------------	-----------	-------------

Command example:

```
./mongo "mongodb://
```

rwuser:<password>@192.168.xx.xx:8635,192.168.xx.xx:8635/test? authSource=admin&readPreference=secondaryPreferred&readPreferenceTags= role:readonly"

If the following information is displayed, the instance is successfully connected: $_{\mbox{mongos}>}$

----End

4.2.4 Connecting to a Cluster Instance over a Public Network

4.2.4.1 Binding and Unbinding an EIP

After you create a Cluster instance, you can bind an EIP to it to allow external access. If later you want to prohibit external access, you can also unbind the EIP from the instance.

Precautions

- Deleting a bound EIP does not mean that the EIP is unbound.
- Before accessing a database, apply for an EIP on the VPC console. Then, add an inbound rule to allow the IP addresses or IP address ranges of ECSs. For details, see **Configuring a Security Group**.

• In the cluster instance, only dds mongos can have an EIP bound. To change the EIP that has been bound to a node, you need to unbind it from the node first.

Binding an EIP

Step 1 Log in to the management console.

- **Step 2** Click ^(Q) in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the cluster instance name.
- Step 5 In the navigation pane on the left, choose Connections. Click the Public
 Connection tab. In the Basic Information area, locate the dds mongos node and click Bind EIP in the Operation column.

Figure 4-22 Binding an EIP

Private Connection	Public Connection			
Basic Information				
Database Port	8635 <i>C</i>		SSL	<u>ب</u>
Address				
Public Network Conne	ction Address Unbound			
Name/ID	AZ	Private IP Address	EIP	Operation
dds-5c63	az2		Our Contract Unbound	Change Private IP Address Bind EIP
dds-5c63	az2	*******	S Unbound	Change Private IP Address Bind EIP

Alternatively, in the **Node Information** area on the **Basic Information** page, locate the dds mongos node and choose **More** > **Bind EIP** in the **Operation** column.

Figure 4-23 Binding an EIP

Node Information							
dds mongos shard config							
Add dds mongos Change Classes in Batches							
Name/ID	Status	Node Class	AZ	Private IP Address	EIP	Operation	
dds-5c63-	Available	Enhanced II 2 vCPUs 8	az2		Unbound	Change Cl	ass Restart <u>More</u> ~
dds-5c63	Available	Enhanced II 2 vCPUs 8	az2		Unbound	Change	View Metric Change Private IP Address
						_	Bind EIP

Step 6 In the displayed dialog box, all available unbound EIPs are listed. Select the required EIP and click **OK**. If no available EIPs are displayed, click **View EIP** and create an EIP on the VPC console.

Figure 4-24 Selecting an EIP

For security p outbound and	urposes, after I inbound rules	binding the EIP, use SSL to c in the security group.	onnect to the database and	add
ode Informatio	n Node Na	ne	Status	
		_mongos_node_1	🔿 Available	
elect EIP				
EIP		Status	Bandwidth	
•		⊗ Unbound	5 Mbit/s	
0		🕲 Unbound	5 Mbit/s	
0		⊗ Unbound	88 Mbit/s	

Step 7 In the EIP column on the dds mongos tab, you can view the EIP that was bound.
To unbind an EIP from the instance, see Unbinding an EIP.
----End

Unbinding an EIP

- Step 1 Log in to the management console.
- **Step 2** Click ^(Q) in the upper left corner and select a region and a project.
- Step 3 Click = in the upper left corner of the page and choose Databases > Document Database Service.
- **Step 4** On the **Instances** page, click the cluster instance name.
- Step 5 In the navigation pane on the left, choose Connections. Click the Public
 Connection tab. In the Basic Information area, locate the dds mongos node and click Unbind EIP in the Operation column.

Figure 4-25 Unbinding an EIP

Name/	AZ	Private IP Addre	EIP	Operation
b76d17	az1po	192.168.106.237		Change Private IP Address Unbind EIP
65fd4c	azlpo	192.168.111.99	Our Contract Out of the second sec	Change Private IP Address Bind EIP

Alternatively, in the **Node Information** area on the **Basic Information** page, locate the dds mongos node and choose **More** > **Unbind EIP** in the **Operation** column.

Figure 4-26 Unbinding an EIP

Node Information						
mongos shard config						
Add mongos						
Q Select one or more filters from the pop-up lists. I	f you enter a keyword wit	hout a filter applied, the system	will search for all names mate	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	Our Unbound	Change Change Private IP Address
						Unbind EIP

Step 6 In the displayed dialog box, click **Yes**.

To bind an EIP to the instance again, see **Binding an EIP**.

----End

4.2.4.2 Configuring a Security Group

A security group is a collection of access control rules for ECSs and DDS instances that have the same security protection requirements and are mutually trusted in a VPC.

To ensure database security and reliability, you need to configure security group rules to allow specific IP addresses and ports to access DDS instances.

To access an instance from the Internet, add an inbound rule for the security group associated with the instance.

Precautions

- By default, an account can create up to 500 security group rules.
- Too many security group rules will increase the first packet latency, so a maximum of 50 rules for each security group is recommended.
- By default, one DDS instance is associated with only one security group.
- DDS allows you to associate multiple security groups to a DB instance. You can apply for the service based on your service requirements. For better network performance, you are advised to select no more than five security groups.

Procedure

- Step 1 Log in to the management console.
- **Step 2** Click ^(Q) in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the instance name. The **Basic Information** page is displayed.
- **Step 5** In the **Network Information** area on the **Basic Information** page, click the security group.

Figure 4-27 Security Group

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

You can also choose **Connections** in the navigation pane on the left. On the **Public Connection** tab, in the **Security Group** area, click the security group name.

Figure 4-28 Security Group

Security Group				
Security Group	default 🖉			
Inbound Rules(6)	Outbound Rules(3)			
Security Group	Protocol & Port (?)	Туре		
default	TCP:22	IPv4		

- **Step 6** On the **Security Group** page, locate the target security group and click **Manage Rule** in the **Operation** column.
- **Step 7** On the **Inbound Rules** tab, click **Add Rule**. The **Add Inbound Rule** dialog box is displayed.
- **Step 8** Add a security group rule as prompted.

Figure 4-29 Add Inbound Rule

Add Inbound Rule Learn more about security group configuration.						
Some security group rules will not take effect for ECSs with certain specifications. Learn more If you select IP address for Source, you can enter multiple IP addresses, separated with commas (.). Each IP address represents a different security group rule.						
Security Group default						
Priority (?) Action (?) Type Protocol & Port (?) Source (?) Description Operation						
1-100 Allow ~ IPv4 ~ IP address ~ Replicate Delete Example: 22 or 22,24 or 22-3 0.0.0.00 × Replicate Delete						
Add Rule Cancel OK						

Table 4-16 Inbound rule settings

Paramete r	Description	Example Value
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	The security group rule actions. A rule with a deny action overrides another with an allow action if the two rules have the same priority.	Allow
Protocol & Port	The network protocol required for access. The option can be All, TCP , UDP, ICMP , or GRE .	ТСР
	Port: the port on which you wish to allow access to DDS. The default port is 8635. The port ranges from 2100 to 9500 or can be 27017, 27018, or 27019.	8635
Туре	IP address type. Only IPv4 and IPv6 are supported.	IPv4

Paramete r	Description	Example Value
Source	Specifies the supported IP address, security group, and IP address group, which allow access from IP addresses or instances in other security group. Example:	0.0.0/0
	• Single IP address: 192.168.10.10/32	
	• IP address segment: 192.168.1.0/24	
	All IP addresses: 0.0.0.0/0	
	 Security group: sg-abc 	
	IP address group: ipGroup-test	
	If you enter a security group, all ECSs associated with the security group comply with the created rule.	
	For more information about IP address groups, see IP Address Group.	
Descriptio n	(Optional) Provides supplementary information about the security group rule. This parameter is optional.	-
	The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	

Step 9 Click OK.

----End

4.2.4.3 Connecting to a Cluster Instance Using Mongo Shell (Public Network)

In the following scenarios, you can access a DDS instance from the Internet by binding an EIP to the instance.

Scenario 1: Your applications are deployed on an ECS and are not in the same region as the DDS instance.



Figure 4-30 Accessing DDS from ECS across regions

Scenario 2: Your applications are deployed on a cloud server provided by other vendors.



Figure 4-31 Accessing DDS from other cloud servers

This section describes how to use Mongo Shell to connect to a cluster instance over a public network.

You can connect to an instance using an SSL connection or an unencrypted connection. The SSL connection is encrypted and more secure. To improve data transmission security, connect to instances using SSL.

Prerequisites

- For details about how to create and log in to an ECS, see Purchasing an ECS and Logging In to an ECS.
- 2. **Bind an EIP** to the cluster instance and **set security group rules** to ensure that the instance can be accessed from the ECS.
- 3. Install the MongoDB client on the ECS.

For details about how to install a MongoDB client, see How Can I Install a MongoDB Client?

SSL

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

- Step 1 Log in to the management console.
- **Step 2** Click ^(Q) in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the instance name.
- **Step 5** In the navigation pane on the left, choose **Connections**.
- **Step 6** In the **Basic Information** area, click $\stackrel{1}{\rightharpoonup}$ next to the **SSL** field.
- **Step 7** Upload the root certificate obtained in **Step 6** to the ECS.

The following describes how to upload the certificate to a Linux and Windows ECS:

 In Linux, run the following command: scp<IDENTITY_FILE><REMOTE_USER>@<REMOTE_ADDRESS>:<REMOTE_DIR>

D NOTE

- **IDENTITY_FILE** is the directory where the root certificate resides. The file access permission is 600.
- **REMOTE_USER** is the ECS OS user.
- **REMOTE_ADDRESS** is the ECS address.
- **REMOTE_DIR** is the directory of the ECS to which the root certificate is uploaded.
- In Windows, upload the root certificate using a remote connection tool.
- **Step 8** Connect to the instance in the directory where the MongoDB client is located.

Method 1: Using a public network connection address

Example command:

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

Parameter description:

• **Public Network Connection Address**: On the **Instances** page, click the instance to switch to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab. In the **Address** area, obtain the instance connection address from the **Public Network Connection Address** field.

Figure 4-32 Obtaining the public network connection address

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

The format of the public connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

Pay attention to the following parameters in the public connection address:

 Table 4-17 Parameter description

Parameter	Description
rwuser	Account name, that is, the database username.
<password></password>	Password for the database account. Replace it with the actual password.
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively.
	For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25***%21%24 .
192.168. <i>xx.xx</i> .863 5	EIP and port bound to the dds mongos node of the cluster instance
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=adm in	The authentication database of user rwuser must be admin . authSource=admin is fixed in the command.

- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and bandwidth, the cluster certificate is generated using the internal management IP address. --sslAllowInvalidHostnames is needed for the SSL connection through a public network.

Command example:

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

Method 2: Connect to an instance using an EIP.

Example command:

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

Parameter description:

• **DB_HOST** is the EIP bound to the instance to be connected.

You can click the instance name to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the **Public Connection** tab, obtain the EIP bound to the dds mongos node in the **EIP** column.

If there are multiple dds mongos nodes, the EIP of any node can be used to connect to the instance.

Figure 4-33 Obtaining an EIP

Basic Information					
Database Port	8635		:	SSL	▲
Address					
Public Network Conne	ection Add	ress m	ongodb://rwus	er: <password>@7</password>	3635/test?authSource=
		ac	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** is the port of the instance to be connected. The default port number is 8635.

You can click the instance to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

Figure 4-34 Obtaining the port

Basic Information					
Database Port	8635			SSL	
Address					
Public Network Conn	ection Addr	ness	mongodb:	//rwuser: <password>@</password>	8635/test?authSource=
			admin 🗇		
Name/ID	AZ	Private I	EIP	Operation	
dds-ce25_mong 000e813fb5574c	az4	192.168		Change Private IP Ad	ddress Unbind EIP
dds-ce25_mong bad06d1cf2594e	az4	192.168		Change Private IP Ad	ddress Bind EIP

- **DB_USER** is the database user. The default value is **rwuser**.
- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and

bandwidth, the cluster certificate is generated using the internal management IP address. --**sslAllowInvalidHostnames** is needed for the SSL connection through a public network.

Enter the database account password when prompted:

Enter password:

Command example:

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

Step 9 Check the connection result. If the following information is displayed, the connection is successful. mongos>

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

- **Step 1** Log in to the ECS.
- **Step 2** Connect to the instance in the directory where the MongoDB client is located.

Method 1: Using a public network connection address

Example command:

./mongo <Public network address>

Public Network Connection Address: You can click the instance name to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab. In the **Address** area, obtain the instance connection address from the **Public Network Connection Address** field.

Figure 4-35 Obtaining the public network connection address

Private Connection Public Connection					
Basic Information					
Database Port	8635 🖉	SSL	▲		
Address					
Public Network Connection Address		mongodb://rwuser: <password>@7</password>	:8635/test?authSource=		
		admin 🗇			

The format of the public connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

The following table describes the required parameters in the public connection address.

Parameter	Description
rwuser	Account name, that is, the database username.
<password></password>	Password for the database account. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25***%21%24.
192.168. <i>xx.xx</i> .863 5	EIP and port bound to the dds mongos node of the cluster instance
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admi n	The authentication database of user rwuser must be admin . authSource=admin is fixed in the command.

Table 4-18 Parameter description

Command example:

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

Method 2: Using an EIP

Example command:

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

Parameter description:

• **DB_HOST** is the EIP bound to the instance to be connected.

You can click the instance name to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the **Public Connection** tab, obtain the EIP bound to the dds mongos node in the **EIP** column.

If there are multiple dds mongos nodes, the EIP of any node can be used to connect to the instance.
Figure 4-36 Obtaining an EIP

I	Basic Information							
[Database Port	8635	<u> </u>	5	SSL	▲		
/	Address							
F	Public Network Conne	ction Addr	ess m	ongodb://rwuse	er: <password>@7</password>	3635/test?authSource=		
			a	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	5 Bind EIP		

• **DB_PORT** is the port of the instance to be connected. The default port number is 8635.

You can click the instance to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

Figure 4-37 Obtaining the port

Basic Information					
Database Port	863	35 🖉		SSL	
Address					
Public Network Conne	ection Ad	dress n	nongodb://r	wuser: <password>@</password>	8635/test?authSource=
		a	idmin 🗖		
Name/ID	AZ	Private I	EIP	Operation	
dds-ce25_mong 000e813fb5574c	az4	192.168		Change Private IP Add	Iress Unbind EIP

• **DB_USER** is the database user. The default value is **rwuser**.

Enter the database account password when prompted:

Enter password:

Command example:

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

Step 3 Check the connection result. If the following information is displayed, the connection is successful. mongos>

nongos/

----End

4.2.4.4 Connecting to a Cluster Instance Using Robo 3T

To connect to an instance from a local device, you can use Robo 3T to access the instance from the Internet.

This section describes how to use Robo 3T to connect to a cluster instance from a local device. In this section, the Windows operating system (OS) used by the client is used as an example.

Robo 3T can connect to an instance with an unencrypted connection or an encrypted connection (SSL). To improve data transmission security, connect to instances using SSL.

Connection Diagram

Figure 4-38 Connection diagram



Prerequisites

- 1. **Bind an EIP** to the cluster instance and **configure security group rules** to ensure that the instance can be accessed using Robo 3T.
- 2. Install Robo 3T.

For details, see Installing Robo 3T.

SSL

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

Step 1 Run the installed Robo 3T. On the displayed dialog box, click **Create**.

🛃 MongoDB Connection	IS		×
<u>Create, edit, remove, cl</u>	<u>one</u> or reorder connection	s via drag'n'drop.	
Name	Address	Attributes Aut	h. Database / User
			📃 Connect 🛛 Cancel

Figure 4-39 Connections

- **Step 2** In the **Connection Settings** dialog box, set the parameters of the new connection.
 - 1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the DDS DB instance in the **Address** text box.

Figure 4-40 Connection

Connection	Authentication SSH TLS Advanced
Туре:	Direct Connection
Name:	test
Address:	: 8635
	Specify host and port of MongoDB server. Host can be either IPv4. IPv6 or domain name.
	Specify host and port of MongoDB server. Host can be either IPv4, IPv6 or domain name.
From URI	Specify host and port of MongoDB server. Host can be either IPv4, IPv6 or domain name.

2. On the **Authentication** tab, set **Database** to **admin**, **User Name** to **rwuser**, and **Password** to the administrator password you set during the creation of the cluster instance.

Figure 4-41 Authentication

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

3. On the **TLS** tab, select **Use TLS protocol** and select **Self-signed Certificate** for **Authentication Method**.

Figure 4-42 SSL

Connection	Settings						×
Connection	Authentic	ation	SSH	TLS	Advance	≥d	
🗹 Use TLS p	protocol						
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 ho server	ing self- s trusted the comm wever the identity	signed certi l. If self-si unications c re will be r 7.	ficates gned channel 10
🗌 Vse PEM C	ert./Key:	Enable requir	this o es CA-s	ption t igned c	o connect lient cer	: to a MongoI tificates/ke)B that y file.
🗌 Advanced	Options						
1 Iest					[Save	Cancel

- 4. Click Save.
- **Step 3** On the **MongoDB Connections** page, click **Connect** to connect to the cluster instance.

🛃 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 🛛 Cano	el

Figure 4-43 Cluster connection information

Step 4 If the cluster instance is successfully connected, the page shown in **Figure 4-44** is displayed.

Figure 4-44 Cluster connected successfully.

le View Options Wind	ow Help	
<pre>test (3) System admin</pre>	 ♦ Welcome × ♦ db.getCollection('system''' × in 10.154.221.76:8635 admin 	♦ db. getCollection(" system. *** Ж
 Collections (4) 	db.getCollection('system.roles').fin	a(\$)
✓ <mark>System</mark>	🚯 0.089 sec.	
 System.r System.v System.v Functions Users 	Fetched 0 record(s) in 88ms	

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details, see **Enabling and Disabling SSL**.

Step 1 Run the installed Robo 3T. On the displayed dialog box, click **Create**.

🛃 MongoDB Connection	IS			×
<u>Create,</u> edit, remove, <u>cl</u>	<u>one</u> or reorder connection	s via drag'n'drop.		
Name	Address	Attributes	Auth. Database / User	
			📃 C <u>o</u> nnect 🛛 Ca	ncel

Figure 4-45 Connections

- **Step 2** In the **Connection Settings** dialog box, set the parameters of the new connection.
 - 1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the DDS DB instance in the **Address** text box.

Figure 4-46 Connection

Connection	Authentication SSH TLS Advanced
Туре:	Direct Connection
Name:	test
Address:	: 8635
	Specify host and port of MongoDB server. Host can be either IPv4. IPv6 or domain name.
	Specify host and port of MongoDB server. Host can be either IPv4, IPv6 or domain name.
From URI	Specify host and port of MongoDB server. Host can be either IPv4, IPv6 or domain name.

2. On the **Authentication** tab, set **Database** to **admin**, **User Name** to **rwuser**, and **Password** to the administrator password you set during the creation of the cluster instance.

Figure 4-47 Authentication

📃 Connection Se	ettings	×							
Connection	Authentication SSH TLS Advanced								
🗹 Perform aut	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									
1 Iest	Save Cancel								

- 3. Click Save.
- **Step 3** On the **MongoDB Connections** page, click **Connect** to connect to the cluster instance.

Figure 4-48 Cluster connection information

🛃 MongoDB Connections	🛃 MongoDB Connections							
<u>Create, edit, remove, clone</u> or reorder connections via drag'n' drop.								
Name	Address	Attributes Auth. Database	/ User					
📃 test	:8635	TLS 🛛 🔑 admin / rwu	iser					
		Connec	t Cancel					

Step 4 If the cluster instance is successfully connected, the page shown in **Figure 4-49** is displayed.



Robo 3T - 1.4	
File View Options Winds	ow Help
 test (3) System admin 	 ♦ Welcome × ● db.getCollection('system… × ● db.getCollection('system × ■ test ■ 10.154.221.78:8635 ■ admin
Collections (4) Collections (4) System System.k System.r System.v System.v	<pre>db.getCollection('system.roles').find(()) () 0.089 sec.</pre>
	Fetched 0 record(s) in 88ms
> Functions > Users > Iocalconfig	

----End

4.2.5 Connecting to a Cluster Instance Using Program Code

4.2.5.1 Java

If you are connecting to an instance using Java, an SSL certificate is optional, but downloading an SSL certificate and encrypting the connection will improve the security of your instance. SSL is disabled by default for newly created instances, but you can enable SSL by referring to **Enabling or Disabling SSL**. SSL encrypts connections to databases but it increases the connection response time and CPU usage. For this reason, enabling SSL is not recommended.

Prerequisites

Familiarize yourself with:

- Computer basics
- Java code

Obtaining and Using Java

- Download the Jar driver from: https://repo1.maven.org/maven2/org/ mongodb/mongo-java-driver/3.0.4/
- To view the usage guide, visit https://mongodb.github.io/mongo-javadriver/4.2/driver/getting-started/installation/.

Using an SSL Certificate

NOTE

- Download the SSL certificate and verify the certificate before connecting to databases.
- On the Instances page, click the target DB instance name. In the DB Information area on the Basic Information page, click in the SSL field to download the root certificate or certificate bundle.
- For details about how to set up an SSL connection, see the MongoDB Java Driver official document at https://www.mongodb.com/docs/drivers/java/sync/current/ fundamentals/connection/tls/#std-label-tls-ssl.
- Java Runtime Environment (JRE) earlier than Java 8 enables TLS 1.2 only in updated versions. If TLS 1.2 is not enabled for your JRE, upgrade it to a later version to use TLS 1.2 for connection.

If you connect to a cluster instance using Java, the format of code is as follows: mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>? authSource=admin&ssl=true

Parameter	Description	
<username></username>	Current username.	
<password></password>	Password for the current username	
<instance_ip></instance_ip>	If you attempt to access the instance from an ECS, set <i>instance_ip</i> to the private IP address displayed on the Basic Information page of the instance to which you intend to connect.	
	If you intend to access the instance through an EIP, set <i>instance_ip</i> to the EIP that has been bound to the instance.	
	If multiple host addresses are required, list the addresses in the format of <instance_ip1>:<instance_port1>,<instance_ip2>:<instance_p ort2> Example: mongodb:// username:*****@127.***.1:8635,127.***.2:8635/? authSource=admin</instance_p </instance_ip2></instance_port1></instance_ip1>	
<instance_port></instance_port>	Database port displayed on the Basic Information page. Default value: 8635	
<database_name ></database_name 	Name of the database to be connected.	
authSource	Authentication user database. The value is admin .	
ssl	Connection mode. true indicates that the SSL connection mode is used.	

Table 4-19	Parameter	description
------------	-----------	-------------

Use the keytool to configure the CA certificate. For details about the parameters, see **Table 4-20**.

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

Table 4-20	Parameter	description
-------------------	-----------	-------------

Parameter	Description	
<path authority="" certificate="" file="" to=""></path>	Path for storing the SSL certificate.	
<path store="" to="" trust=""></path>	Path for storing the truststore. Set this parameter as required, for example, ./ trust/certs.keystore.	
<password></password>	Custom password.	

Set the JVM system properties in the program to point to the correct truststore and keystore:

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

For details about the Java code, see the following example: 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"); } } }

Connection Without the SSL Certificate

NOTE

You do not need to download the SSL certificate because certificate verification on the server is not required.

If you connect to a cluster instance using Java, the format of code is as follows: mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>? authSource=admin

Parameter	Description
<username></username>	Current username.
<password></password>	Password for the current username
<instance_ip></instance_ip>	If you attempt to access the instance from an ECS, set <i>instance_ip</i> to the private IP address displayed on the Basic Information page of the instance to which you intend to connect.
	If you intend to access the instance through an EIP, set <i>instance_ip</i> to the EIP that has been bound to the instance.
	If multiple host addresses are required, list the addresses in the format of <instance_ip1>:<instance_port1>,<instance_ip2>:<instance_p ort2> Example: mongodb:// username:*****@127.***.1:8635,127.***.2:8635/? authSource=admin</instance_p </instance_ip2></instance_port1></instance_ip1>
<instance_port></instance_port>	Database port displayed on the Basic Information page. Default value: 8635
<database_name ></database_name 	Name of the database to be connected.
authSource	Authentication user database. The value is admin .

Table 4-21 Parameter description

```
For details about the Java code, see the following example: 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

This section describes how to use the MongoDB client in Python to connect to a cluster instance.

Prerequisites

1. To connect an ECS to an instance, the ECS must be able to communicate with the DDS instance. You can run the following command to connect to the IP address and port of the instance server to test the network connectivity.

curl ip:port

If the message **It looks like you are trying to access MongoDB over HTTP on the native driver port** is displayed, the network connectivity is normal.

- 2. Install Python and third-party installation package **pymongo** on the ECS. Pymongo 2.8 is recommended.
- 3. If SSL is enabled, you need to download the root certificate and upload it to the ECS.

Connection Code

- Enabling 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
- Disabling 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 NOTE

- The authentication database in the URL must be **admin**. That means setting **authSource** to **admin**.
- In SSL mode, you need to manually generate the trustStore file.
- The authentication database must be **admin**, and then switch to the service database.

5 Getting Started with Replica Sets

5.1 Buying a Replica Set Instance

5.1.1 Quick Config

This section describes how to quickly purchase a replica set instance on the management console. DDS provides several recommended configurations to help you purchase a replica set instance within several minutes.

Prerequisites

- You have registered a Huawei ID and enabled Huawei Cloud services.
- Your account balance is greater than or equal to \$0 USD.

Procedure

- **Step 1** Go to the **Quick Config** page.
- **Step 2** On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.

Figure 5-1 Basic configurations

Basic Information						
Billing Mode	Yearly/Monthly	Pay-per-use)			
Region						
	Regions are geographic an	eas isolated from each o	ther. For low network la	tency and quick resource	access, select the near	est region.
Project						
AZ	cn-north-4a	cn-north-4b	cn-north-4c	AZ7	cn-north-4a,cn-nor	th-4b,AZ7
	Deploy your DB instance in	a single AZ or three AZ	s for high availability.			
DB Instance Type ⑦	Cluster	Replica set	Cloud native replica	a set		
	Replica sets deliver reliabil	ity and disaster recovery	they can provide excel	llent reliability and are su	itable for small and medi	um sized enterprise
	Replica sets you can still cr	reate: 49. Increase Quota	а			
Compatible MongoDB Version	5.0 Beta	4.4	4.2	4.0	3.4	
Specifications	General-purpose	Enhanced II				
Recommended Specifications						
	Medium- and Light	weight Databases		Custom		
	2 vCPUs 8GB		2 vCPUs	8GB 🗸		
	100 GB	Ultra-high I/O	10	GB Ultra-high I	/0	
	Maximum Conne	ctions: 1,000	Maximum (Connections: 1,000		
	Currently selected dds.md	ongodb.c6.large.4.repset	2 vCPUs 8GB			
Disk Encryption	Disable	Enable 🙆	0			

Table 5-1 Basic configurations

Parameter	Description		
Billing Mode	Select a billing mode, Yearly/Monthly or Pay-per-use.		
	For yearly/monthly instances		
	 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 Yearly/ Monthly to Pay-per-Use. 		
	NOTE Instances billed on a yearly/monthly basis cannot be deleted. They can only be unsubscribed from. For details, see Billing Termination.		
	For pay-per-use instances		
	 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 Pay-per-Use to Yearly/Monthly. 		
Region	The region where the resource is located.		
	NOTE 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
Project	The project corresponds to the current region and can be changed.
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.
	Instances can be deployed in a single AZ or three AZs.
	• If your service requires low network latency between instances, you deploy the components of the instance in the same AZ. If you select a single AZ to deploy your instance, anti-affinity deployment is used by default. With an anti-affinity deployment, your primary, secondary, and hidden nodes are deployed on different physical machines for high availability.
	• If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the primary, secondary, and hidden nodes are evenly distributed across three AZs.
	NOTE The 3-AZ deployment is not available in all regions. If the 3-AZ option is not displayed on the page for you to buy an instance, try a different region.
DB Instance	Select Replica set .
Туре	A replica set consists of the primary node, secondary node, and hidden node. If a primary node goes down or becomes faulty, a secondary node is automatically assigned to the primary role and continues normal operation. If a secondary node is unavailable, a hidden node will take the role of the secondary to ensure high availability.
Compatible MongoDB Version	 5.0 4.4
	• 4.2
	• 4.0
	• 3.4

Parameter	Description		
CPU Type	 DDS supports x86 and Kunpeng CPU architectures. NOTE This parameter is available only for MongoDB 4.0 and 3.4. You do not need to set this parameter for other versions. The default value is x86. 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 lightworkload 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 ultrahigh 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, medium- and lightweight database specifications and customized specifications are supported. NOTE • The storage space ranges from 10 GB to 5,000 GB.		

Network	
VPC	default_vpc v Q Subnet default_subnet
	After the DDS instance is created, the VPC cannot be changed.
	Available private IP addresses in the subnet: 235
	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 View Project Management (2)
Required Duration and Quanti	ity
Required Duration	1 2 3 4 5 6 7 8 9 months 1 year 2 years 3 years
	Auto-renew Fee deduction and Renewal duration
Quantity	- + 🕥 You can create 49 more DB Instances. Increase Quota

Figure 5-2 Network, Required Duration, and Quantity

 Table 5-2
 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 Virtual Private Cloud User Guide. For details about the constraints on the use of VPCs, see Connection Methods.
	If there are no VPCs available, DDS creates one for you by default.
	NOTE 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 . For more information about enterprise project, see Project Management in <i>Enterprise Management User Guide</i> .
	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 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.
Quantity	The purchase quantity depends on the replica set instance quota. If your current quota does not allow you to purchase the required number of instances, you can apply for increasing the quota as prompted. Yearly/Monthly instances that were purchased in batches have the same specifications except for the instance name and ID.

TADLE 3-3 Required duration and quantity	Table 5	-3 Requ	ired dura	tion and	quantity
---	---------	---------	-----------	----------	----------

Step 3 On the displayed page, confirm the instance details.

- For yearly/monthly instances
 - 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.
- For pay-per-use instances
 - 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.
- **Step 4** Click **Back to Instance List**. 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.

----End

5.1.2 Custom Config

This section describes how to purchase a replica set instance in custom mode on the management console. You can customize the computing resources and storage space of a replica set 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 50 replica set instances.

Prerequisites

- You have registered a Huawei ID and enabled Huawei Cloud services.
- Your account balance is greater than or equal to \$0 USD.
- To display whether the disk is encrypted in the DB instance list, submit a service ticket. In the upper right corner of the management console, choose Service Tickets > Create Service Ticket.
- If you want compute and network resources dedicated to your exclusive use, enable a DeC and apply for DCC resources. Then, you can create DDS

instances. Click 🔍 in the upper left corner and select a region and a project.

NOTE

You will be additionally charged for using DeC. Only pay-per-use replica set instances can be purchased through DeC.

Procedure

- **Step 1** Go to the **Custom Config** page.
- **Step 2** On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.

Figure 5-3 Basic configurations



Parameter	Description		
Billing Mode	Select a billing mode, Yearly/Monthly or Pay-per-use .		
	For yearly/monthly instances		
	 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 Yearly/ Monthly to Pay-per-Use. 		
	NOTE Instances billed on a yearly/monthly basis cannot be deleted. They can only be unsubscribed from. For details, see Billing Termination .		
	For pay-per-use instances		
	 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 Pay-per-Use to Yearly/Monthly. 		
Region	The region where the resource is located.		
	NOTE 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.		
Project	The project corresponds to the current region and can be changed.		

Table 5-4 Billing Mode

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.		
	Instances can be deployed in a single AZ or three AZs.		
	• If your service requires low network latency between instances, you deploy the components of the instance in the same AZ. If you select a single AZ to deploy your instance, anti-affinity deployment is used by default. With an anti-affinity deployment, your primary, secondary, and hidden nodes are deployed on different physical machines for high availability.		
	• If you want to deploy an instance across AZs for disaster recovery, select three AZs. In this deployment mode, the primary, secondary, and hidden nodes are evenly distributed across three AZs.		
	NOTE The 3-AZ deployment is not available in all regions. If the 3-AZ option is not displayed on the page for you to buy an instance, try a different region.		
DB 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.		
	• The instance name can be the same as an existing instance name.		
	 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	Select Replica set .		
Туре	A replica set consists of the primary node, secondary node, and hidden node. If a primary node goes down or becomes faulty, a secondary node is automatically assigned to the primary role and continues normal operation. If a secondary node is unavailable, a hidden node will take the role of the secondary to ensure high availability.		

Parameter	Description
Primary AZ	Select the AZ housing the primary/standby role.
	NOTE This parameter is available when AZ is set to multiple AZs.
Standby AZ	Select the AZ housing the primary/standby role.
	NOTE This parameter is available when AZ is set to multiple AZs.
Compatible	• 5.0
MongoDB	• 4.4
Version	• 4.2
	• 4.0
	• 3.4
Nodes	You can create a three-node, five-node, or seven-node replica set instance.
СРИ Туре	DDS supports x86 and Kunpeng CPU architectures.
	NOTE This parameter is available only for MongoDB 4.0 and 3.4. You do not need to set this parameter for other versions. The default value is x86 .
	 x80 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.
Storage Type	The storage type can be Ultra-high I/O and Extreme SSD for non-DeC users.
	For DeC users, the supported storage types depend on the selected resource type.
	• If you select EVS for Resource Type, Storage Type is set to Cloud SSD.
	• If you select DSS for Resource Type, Storage Type can be set to Common I/O, High I/O, or Cloud SSD.

Parameter	Description		
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. PacksDP 		
	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 lightworkload 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 ultrahigh 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 .		
	For details about the performance data of DB instances of different specifications, see Performance White Paper .		
	If the CPU or memory of a created DB instance cannot meet service requirements, you can change it on the management console. For details, see Changing a Replica Set Instance Class .		
Storage Space	The storage space ranges from 10 GB to 5,000 GB.		
	You can scale up an instance after it is created. For details, see Scaling Up a Replica Set Instance. NOTE		
	 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. 		

Parameter	Description		
Disk	Disabled: Disable encryption.		
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. 		
	NOTE		
	• 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.		
	 To check whether the disk is encrypted, you can view Disk Encrypted in the DB instance list. 		
	 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 Data Encryption Workshop User Guide. 		
	 Disk encryption supports only the AES_256 key algorithm. 		

Figure 5-4 Administrator settings



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 choose More > 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.

Table	5-5	Administrator	settings
-------	-----	---------------	----------

Figure 5-5 Network, Required Duration, and Quantity



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 Connection Methods .
	If there are no VPCs available, DDS creates one for you by default.
	VPC owners can share the subnets in a VPC with one or multiple accounts through Resource Access Manager (RAM). This allows for more efficient use of network resources and reduces O&M costs.
	For more information about VPC subnet sharing, see VPC Sharing in the Virtual Private Cloud User Guide.
	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 .
	NOTE 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.
	NOTE
	• 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.
	• When creating a DB instance, you can select multiple security groups. For better network performance, you are advised to select no more than five security groups. In such a case, the access rules of all the selected security groups apply on the instance.
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.

Table 5-6 Network

Parameter	Description		
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. NOTE For details about how to change a database port, see Changing a Database Port. 		
Cross-CIDR Access	 Configure If a client and a replica set instance are deployed in different CIDR blocks and the client is not in 192.168.0.0/16, 172.16.0.0/24, or 10.0.0.0/8, configure Cross-CIDR Access for the instance to communicate with the client. NOTE To ensure the ECS and the DB instance can communicate with each other, configure the connection by referring to VPC Peering Connection Overview. Up to 30 CIDR blocks can be configured, and each of them can 		
	 overlap but they cannot be the same. That is, the source CIDR blocks can overlap but cannot be the same. The CIDR blocks cannot start with 127. The allowed IP mask ranges from 8 to 32. Skip Configure the CIDR block of the client later. After a DB instance is created, you can configure cross-CIDR access by referring to Configuring Cross-CIDR Access. 		
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 .		

Figure 5-6 Advanced settings

Advanced Settings		
Replica Set Parameter Template	Default-DDS-4.4-Replica	Q View Parameter Template
Show Original Log	0	
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	Predefined tags are recommended for adding the same tag to diffe Tag key Tag value Tag value	erent cloud resources. Create Predefined Tag C View predefined tags
	You can add 20 more tags.	

Table	5-7	Advanced	settings
-------	-----	----------	----------

Parameter	Description
Replica Set Parameter Template	The parameters that apply to the replica set instances. After an instance is created, you can change the parameter template you configured for the instance to bring out the best performance. For details, see Editing a Parameter Template .
Show Original Log	If Show Original Log is enabled, the original slow query logs will be displayed, and the logs will be transferred to an OBS bucket. By default, the system automatically deletes logs from the OBS bucket after 30 days, and the retention period cannot be changed.
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
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.
	If your organization has configured tag policies for DDS, add tags to DB instances based on the policies. If a tag does not comply with the policies, DB instance creation may fail. Contact your organization administrator to learn more about tag policies.
	• 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 must consist of only 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**.

NOTE

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

Step 3 On the displayed page, confirm the instance details.

- For yearly/monthly instances
 - 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.
- For pay-per-use instances
 - 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.
- **Step 4** Click **Back to Instance List**. 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.
 - ----End

5.2 Connecting to a Replica Set Instance

5.2.1 Connection Methods

You can access DDS over private or public networks.

Table 5-8 Connection methods

Method	IP Address	Scenario	Description
DAS	Not required	DAS provides a GUI and allows you to perform visualized operations on the console. SQL execution, advanced database management, and intelligent O&M are available to make database management simple, secure, and intelligent.	 Easy to use, secure, advanced, and intelligent Recommended

Method	IP Address	Scenario	Description
Private network	Private IP address	DDS provides a private IP address by default. If your applications are running on an ECS in the same region, AZ, and VPC subnet as your DDS instance, you are advised to use a private IP address to connect the ECS to your DDS instances.	Secure and excellent performance
Public network	EIP	 If your applications are running on an ECS that is in a different region from the one where the DB instance is located, use an EIP to connect the ECS to your DDS DB instances. If your applications are deployed on another cloud platform, EIP is recommended. 	 Low security For faster transmission and improved security, you are advised to migrate your applications to an ECS that is in the same subnet as your DDS instance and use a private IP address to access the instance.

5.2.2 (Recommended) Connecting to Replica Set Instances Through DAS

5.2.2.1 Overview

DAS provides a GUI and allows you to perform visualized operations on the console. SQL execution, advanced database management, and intelligent O&M are available to make database management simple, secure, and intelligent. You are advised to use DAS to connect to DB instances.

This section describes how to buy a replica set instance on the management console and how to connect to the replica set instance through DAS.

Process

To purchase and connect to a replica set instance, perform the following steps:

- 1. Buy a replica set instance.
- 2. Connect to the replica set instance through DAS.

5.2.2.2 Connecting to a Replica Set Instance Through DAS

Data Admin Service (DAS) enables you to manage DB instances on a web-based console, simplifying database management and improving working efficiency. You can connect and manage instances through DAS. By default, you have the permission required for remote login. It is recommended that you use the DAS service to connect to instances. DAS is secure and convenient.

Procedure

- Step 1 Log in to the management console.
- **Step 2** Click ¹ 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.

- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, locate the target DB instance and click **Log In** in the **Operation** column.

Alternatively, click the target DB instance on the **Instances** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner of the page.

Figure 5-7 Instance management

Renew Change to Yearly/Monthly Unsut	scribe View	r Progress								
All projects	or more filters from t	he pop-up lists. If yo	u enter a keyword v	rithout a filter applied, the system will	search for all insta	nce names matching this keyword.				0 Q P
NameiD 🕀	Description	D8 Instanc	D8 Engine	Status 🕀	Billing Mode	Connection Address Compatible with M	Enterprise	Tags	Operation	
	9 ⁻	Replica set	5.0	Available	Pay-per-Use Created on	mongodb.//nvuserpassword>@192.160	default	-	Log In View Metric More \sim	

Step 5 On the displayed login page, enter the administrator username and password and click **Log In**.

For details about how to manage databases through DAS, see **DDS Instance** Management.

----End

5.2.3 Connecting to a Replica Set Instance over a Private Network

5.2.3.1 Configuring Security Group Rules

A security group is a collection of access control rules for ECSs and DDS instances that have the same security protection requirements and are mutually trusted in a VPC.

To ensure database security and reliability, you need to configure security group rules to allow specific IP addresses and ports to access DDS instances.

You can connect to an instance by configuring security group rules in following two ways:

 If the ECS and instance are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to Connecting to a Replica Set Instance Using Mongo Shell (Private Network).



Figure 5-8 Same security group

• If the ECS and instance are in different security groups, you need to configure security group rules for them, separately.

Figure 5-9 Different security groups



- Instance: Configure an **inbound rule** for the security group associated with the instance.
- ECS: The default security group rule allows all outbound data packets. In this case, you do not need to configure a security group rule for the ECS. If not all traffic is allowed to reach the instance, configure an **outbound** rule for the ECS.

This section describes how to configure an inbound rule for an instance.

Precautions

- By default, an account can create up to 500 security group rules.
- Too many security group rules will increase the first packet latency, so a maximum of 50 rules for each security group is recommended.
- By default, one DDS instance is associated with only one security group.
- DDS allows you to associate multiple security groups to a DB instance. You can apply for the service based on your service requirements. For better network performance, you are advised to select no more than five security groups.

Procedure

Step 1 Log in to the management console.

- **Step 2** Click ¹ in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the instance name. The **Basic Information** page is displayed.
- **Step 5** In the **Network Information** area on the **Basic Information** page, click the security group.

Figure 5-10 Security Group

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

You can also choose **Connections** in the navigation pane on the left. On the **Private Connection** tab, in the **Security Group** area, click the security group name.

Figure 5-11 Security Group

Security Group		
Security Group	default 🖉	
Inbound Rules(6)	Outbound Rules(3)	
Security Group	Protocol & Port (?)	Туре
default	TCP:22	IPv4

- **Step 6** On the **Security Group** page, locate the target security group and click **Manage Rule** in the **Operation** column.
- **Step 7** On the **Inbound Rules** tab, click **Add Rule**. The **Add Inbound Rule** dialog box is displayed.

Step 8 Add a security group rule as prompted.

Figure 5-12 Add Inbound Rule					
Add Inbound Rule Learn more about security group configuration.	×				
Some security group rules will not take effect for ECSs with certain specifications. Learn more If you select IP address for Source, you can enter multiple IP addresses, separated with commas (.). Each IP address represents a different security group rule.					
Security Group default You can import multiple rules in a batch.					
Priority ⑦ Action ⑦ Type Protocol & Port ⑦ Source ⑦ Description Operation					
1-100 Allow ~ IPv4 ~ IP rotocols / TCP (Cus ~ IP address ~ Replicate Delete Example: 22 or 22,24 or 22-3 0.0.0.00 × Replicate Delete					
Add Rule Cancel OK					

Table 5-9 Indound rule settings	Table	5-9	Inbound	rule	settings
---------------------------------	-------	-----	---------	------	----------

Paramete r	Description	Example
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	The security group rule actions. A rule with a deny action overrides another with an allow action if the two rules have the same priority.	Allow
Protocol & Port	The network protocol required for access. Available options: TCP , UDP , ICMP , or GRE	ТСР
	Port: the port on which you wish to allow access to DDS. The default port is 8635. The port ranges from 2100 to 9500 or can be 27017, 27018, or 27019.	8635
Туре	IP address type. Only IPv4 and IPv6 are supported.	IPv4

Paramete r	Description	Example
Source	Specifies the supported IP address, security group, and IP address group, which allow access from IP addresses or instances in other security group. Example:	0.0.0/0
	• Single IP address: 192.168.10.10/32	
	• IP address segment: 192.168.1.0/24	
	All IP addresses: 0.0.0.0/0	
	 Security group: sg-abc 	
	 IP address group: ipGroup-test 	
	If you enter a security group, all ECSs associated with the security group comply with the created rule.	
	For more information about IP address groups, see IP Address Group.	
Descriptio n	(Optional) Provides supplementary information about the security group rule. This parameter is optional.	-
	The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	

Step 9 Click OK.

----End

5.2.3.2 Connecting to a Replica Set Instance Using Mongo Shell (Private Network)

Mongo shell is the default client for the MongoDB database server. You can use Mongo Shell to connect to DB instances, and query, update, and manage data in databases. DDS is compatible with MongoDB. Mongo Shell is a part of the MongoDB client. To use Mongo Shell, download and install the MongoDB client first, and then use the Mongo shell to connect to the DB instance.

By default, a DDS instance provides a private IP address. If your applications are deployed on an ECS and are in the same region and VPC as DDS instances, you can connect to DDS instances using a private IP address to achieve a fast transmission rate and high security.

This section describes how to use Mongo Shell to connect to a replica set instance over a private network.

The MongoDB client can connect to an instance with an unencrypted connection or an encrypted connection (SSL). To improve data transmission security, connect to instances using SSL.
Prerequisites

- 1. For details about how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
- Install the MongoDB client on the ECS. To ensure successful authentication, install the MongoDB client of the same version as the target instance.
 For details about how to install a MongoDB client, see How Can I Install a MongoDB Client?
- 3. The ECS can communicate with the DDS instance. For details, see **Configuring Security Group Rules**.

SSL Connection

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

- Step 1 Log in to the management console.
- **Step 2** Click ^(Q) in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the instance name.
- **Step 5** In the navigation pane on the left, choose **Connections**.
- **Step 6** In the **Basic Information** area, click $\stackrel{L}{\rightharpoonup}$ next to the **SSL** field.
- **Step 7** Upload the root certificate to the ECS to be connected to the instance.

The following describes how to upload the certificate to a Linux and Windows ECS:

 In Linux, run the following command: scp
 scp</li

D NOTE

- **IDENTITY_FILE** is the directory where the root certificate resides. The file access permission is 600.
- **REMOTE_USER** is the ECS OS user.
- **REMOTE_ADDRESS** is the ECS address.
- **REMOTE_DIR** is the directory of the ECS to which the root certificate is uploaded.
- In Windows, upload the root certificate using a remote connection tool.
- **Step 8** Connect to a DDS instance.

Method 1: Using the private HA connection address (recommended)

DDS provides the HA connection address. Using this address to connect to a replica set instance improves data read/write performance and prevents errors reported when data is written from the client after a primary/standby switchover.

Example command:

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

Parameter description:

• **Private HA Connection Address**: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 5-13 Obtaining the private HA connection address

ate 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	J Learn more

The format of the private HA connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

Pay attention to the following parameters in the private HA address:

Table 5-10 Param	neter description
------------------	-------------------

Parameter	Description
rwuser	Account name, that is, the database username.
<password></password>	Password for the database account. Replace it with the actual password.
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively.
	For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25*** %21%24 .

Parameter	Description
192.168.xx.xx:8635,192.1 68.xx.xx:8635	IP addresses and ports of the nodes of the replica set instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin&repli caSet=replica	 The authentication database of user rwuser must be admin. authSource=admin is fixed in the command.
	 replica in replicaSet=replica is the name of a replica set. The default replica set of Huawei Cloud DDS is replica.

- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: The replica set certificate is generated using the internal management IP address to ensure that internal communication does not occupy resources such as the user IP address and bandwidth. -sslAllowInvalidHostnames is needed for the SSL connection through a private network.

Command example:

./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

NOTE

- If you connect to an instance over a private HA address, add double quotation marks before and after the connection information.
- For details about the HA connection, see **Connecting to a Replica Set Instance for Read and Write Separation and High Availability**.

If the following information is displayed, the instance is successfully connected: replica:PRIMARY>

Run the following command to access the local database:

use local

Information similar to the following is displayed:

switched to db local

Run the following command to query replica set oplog:

db.oplog.rs.find()

Method 2: Using the private HA connection address (user-defined database and account)

Example command:

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

Parameter description:

• **Private HA Connection Address**: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.



vate Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	L T	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

The format of the obtained private HA connection address is as follows:

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

The following table lists the required parameters in the private HA address.

Table 5-11 Parameter information
--

Parameter	Description		
rwuser	Database username. The default value is rwuser . You can change the value to the username based on your service requirements.		
<password></password>	Password for the database username. Replace it with the actual password.		
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively.		
	For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25*** %21%24 .		
192.168.xx.xx:8635,192. 168.xx.xx:8635	IP addresses and ports of the nodes of the replica set instance to be connected.		
test	The name of the test database. You can set this parameter based on your service requirements.		

Parameter	Description
authSource=admin&rep licaSet=replica	 The authentication database of user rwuser is admin.
	 In replica in replicaSet=replica, replica indicates that the instance type is replica set and the format cannot be changed.
	NOTE If you use a user-defined database for authentication, change the authentication database in the HA connection address to the name of the user-defined database. In addition, replace rwuser with the username created in the user-defined database.

- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: The replica set certificate is generated using the internal management IP address to ensure that internal communication does not occupy resources such as the user IP address and bandwidth. -sslAllowInvalidHostnames is needed for the SSL connection through a private network.

For example, if you create a user-defined database **Database** and user **test1** in the database, the connection command is as follows:

./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: Connect to a single node.

You can also use the private IP address of a primary or secondary node to access the replica set instance. This method affects the read/write performance when **a primary/standby switchover** occurs.

Example command:

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

Parameter description:

• **DB_HOST** is the private IP address of the primary or secondary node of the instance to be connected.

Primary node: You can read and write data on it.

Secondary node: You can only read data from it.

On the **Instances** page, click the instance to go to the **Basic Information** page. Choose **Connections**. On the **Private Connection** tab, obtain the IP address of the corresponding node.

Basic Information						
Database Port	8635 L			VPC		default_vpc
SSL		Ł		Subnet		default_subnet (
Address						
Cross-CIDR Act	cess		Disabled Enable			
Private HA Con	nection Address Comp	atible with MongoDB	mongodb://rwuser: <pas< td=""><td>sword>@ XXXXXXXX</td><td></td><td>🗱 dest?authSource=admin&replicaSet=replica \mathscr{Z} 🗇 Learn more</td></pas<>	sword>@ XXXXXXXX		🗱 dest?authSource=admin&replicaSet=replica \mathscr{Z} 🗇 Learn more
			Note The paramete	rs in orange are variable	s and need to be n	nodified based on service requirements. For details, click Learn more.
Q Select or	ne or more filters from	the pop-up lists. If you e	enter a keyword without a	filter applied, the syster	n will search for al	I names matching this keyword.
Name/ID	Role	AZ	Private IP Address	EIP	Operation	
dds-3707_r f2672eb8d7.	Secondary	cn-north-4a	192.	Onbound	Change Priva	te IP Address Bind EIP
dds-3707_r 62921741af.	Primary	cn-north-4a	192	Onbound	Change Priva	te IP Address Bind EIP
dds-3707_r 8cec491e6	Hidden	cn-north-4a	192. ******	-	Change Priva	le IP Address

Figure 5-15 Obtaining the IP address of a node

• **DB_PORT** is the database port. The default value is 8635.

You can click the instance to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Private Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

Figure 5-16 Obtaining the port

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

- **DB_USER** is the database user. The default value is **rwuser**.
- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: The replica set certificate is generated using the internal management IP address to ensure that internal communication does not occupy resources such as the user IP address and bandwidth. -sslAllowInvalidHostnames is needed for the SSL connection through a private network.

Enter the database account password when prompted:

Enter password:

Command example:

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

If the following information is displayed, the corresponding node is successfully connected:

- The primary node of the replica set is connected. replica:PRIMARY>
- The secondary node of the replica set is connected. replica:SECONDARY>

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

- **Step 1** Log in to the ECS.
- Step 2 Connect to a DDS instance.

Method 1: High-availability connection (recommended)

DDS provides the HA connection address. Using this address to connect to a replica set instance improves read/write performance and prevents errors reported when data is written from the client after a primary/standby switchover.

Example command:

./mongo "<Private HA Connection Address>"

Private HA Connection Address: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 5-17 Obtaining the private HA connection address

vate Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	ج ۲	Subnet	dds-st-test-subnet-2 ()
Auto-switch Private II Address	P		
Address			
Cross-CIDR Access	Disabled Enable		
Private HA Connectio	on Address mongodb://rwuser: <password>@*</password>		//test?authSource=admin&replicaSet=replica 🗇 Learn more

The format of the private HA connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

Pay attention to the following parameters in the private HA address:

Parameter	Description		
rwuser	Account name, that is, the database username.		
<password></password>	Password for the database account. Replace it with the actual password.		
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively.		
	For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25*** %21%24 .		
192.168.xx.xx:8635,192.168 .xx.xx:8635	IP addresses and ports of the nodes of the replica set instance to be connected.		
test	The name of the test database. You can set this parameter based on your service requirements.		
authSource=admin&replica Set=replica	• The authentication database of user rwuser must be admin . authSource=admin is fixed in the command.		
	 replica in replicaSet=replica is the name of a replica set. The default replica set of Huawei Cloud DDS is replica. 		

Table 5-12 Parameter description

Command example:

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

If the following information is displayed, the instance is successfully connected: replica:PRIMARY>

Run the following command to access the local database:

use local

Information similar to the following is displayed:

switched to db local

Run the following command to query replica set oplog:

db.oplog.rs.find()

Method 2: Private HA connection (user-defined database and account)

Example command:

./mongo "<Private HA Connection Address>"

Private HA Connection Address: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.



asic Information				
atabase Port	8635 🖉	VPC	dds-st-test-vpc	
5L	ج ح	Subnet	dds-st-test-subnet-2 ()	
uto-switch Private II ddress	P 💽			
ddress				
ross-CIDR Access	Disabled Enable			

The format of the obtained private HA connection address is as follows:

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

The following table lists the required parameters in the private HA address.

Parameter	Description
rwuser	Database username. The default value is rwuser . You can change the value to the username based on your service requirements.
<password></password>	Password for the database username. Replace it with the actual password.
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively.
	For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25***%21%24 .
192.168.xx.xx:8635,192.1 68.xx.xx:8635	IP addresses and ports of the nodes of the replica set instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.

Table 5-13 Parameter information

Parameter	Description
authSource=admin&repli caSet=replica	• The authentication database of user rwuser is admin .
	 In replica in replicaSet=replica, replica indicates that the instance type is replica set and the format cannot be changed.
	NOTE If you use a user-defined database for authentication, change the authentication database in the HA connection address to the name of the user-defined database. In addition, replace rwuser with the username created in the user-defined database.

For example, if you create a user-defined database **Database** and user **test1** in the database, the connection command is as follows:

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

Method 3: Connect to a single node.

You can also use the private IP address of a primary or secondary node to access the replica set instance. This method affects the read/write performance when a primary/standby switchover occurs.

Example command:

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

Parameter description:

• **DB_HOST** is the private IP address of the primary or secondary node of the instance to be connected.

Primary node: You can read and write data on it.

Secondary node: You can only read data from it.

On the **Instances** page, click the instance to go to the **Basic Information** page. Choose **Connections**. On the **Private Connection** tab, obtain the IP address of the corresponding node.

В	Basic Information									
D	atabase Port	8635 <i>Q</i>			V	PC .	default_vpc			
S	SL	t t			S	ibnet	default_subne			
A	ddress									
С	ross-CIDR Acces	5		Disabled Enable						
Private HA Connection Address Compatible with MongoDB				mongodb://rwuser: <pas< td=""><td>sword>@</td><td>rariables and need to be</td><td>e modified based</td><th>uthSource=admin&r on service requirem</th><td>eplicaSet=replica &</td><td>은</td></pas<>	sword>@	rariables and need to be	e modified based	uthSource=admin&r on service requirem	eplicaSet=replica &	은
	Q Select one of	or more filters from the p	op-up lists. If you e	enter a keyword without a	a filter applied, the	e system will search for	all names matchi	ing this keyword.		
	Name/ID	Role	AZ	Private IP Address	EIP	Operation				
	dds-3707_r f2672eb8d7	Secondary	cn-north-4a	192.	Onbound	Change Pri	ivate IP Address	Bind EIP		
	dds-3707_r 62921741af	Primary	cn-north-4a	192	Our Contract Out Contract Ou	Change Pri	ivate IP Address	Bind EIP		
	dds-3707_r 8cec491e6	Hidden	cn-north-4a	192.		Change Pri	ivate IP Address			

Figure 5-19 Obtaining the IP address of a node

• **DB_PORT** is the database port. The default value is 8635.

You can click the instance to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Private Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

Figure 5-20 Obtaining the port

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

• **DB_USER** is the database user. The default value is **rwuser**.

Command example:

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

Enter the database account password when prompted:

Enter password:

If the following information is displayed, the corresponding node is successfully connected:

- The primary node of the replica set is connected. replica:PRIMARY>
- The secondary node of the replica set is connected. replica:SECONDARY>

----End

5.2.3.3 Connecting to Read Replicas Using Mongo Shell

Mongo shell is the default client for the MongoDB database server. You can use Mongo Shell to connect to DB instances, and query, update, and manage data in databases. DDS is compatible with MongoDB. Mongo Shell is a part of the MongoDB client. To use Mongo Shell, download and install the MongoDB client first, and then use the Mongo shell to connect to the DB instance.

By default, a DDS instance provides a private IP address. If your applications are deployed on an ECS and are in the same region and VPC as DDS instances, you can connect to DDS instances using a private IP address to achieve a fast transmission rate and high security.

This section describes how to use Mongo Shell to connect to a read replica over a private network.

You can connect to a read replica using an SSL connection or an unencrypted connection. The SSL connection is encrypted and more secure. To improve data transmission security, connect to instances using SSL.

Prerequisites

- 1. For details about how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
- 2. Install the MongoDB client on the ECS. To ensure successful authentication, install the MongoDB client of the same version as the target instance.
 - For details about how to install a MongoDB client, see How Can I Install a MongoDB Client?
- 3. The ECS can communicate with the DDS instance. For details, see **Configuring Security Group Rules**.

SSL Connection

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

- **Step 1** On the **Instances** page, click the instance name.
- **Step 2** In the navigation pane on the left, choose **Connections**.
- Step 3 In the Basic Information area, click 📥 next to the SSL field.
- **Step 4** Upload the root certificate to the ECS to be connected to the instance.

The following describes how to upload the certificate to a Linux and Windows ECS:

 In Linux, run the following command: scp<IDENTITY_FILE><REMOTE_USER>@<REMOTE_ADDRESS>:<REMOTE_DIR>

D NOTE

- **IDENTITY_FILE** is the directory where the root certificate resides. The file access permission is 600.
- **REMOTE_USER** is the ECS OS user.
- **REMOTE_ADDRESS** is the ECS address.
- **REMOTE_DIR** is the directory of the ECS to which the root certificate is uploaded.
- In Windows, upload the root certificate using a remote connection tool.
- **Step 5** Connect to a DDS instance. The DDS console provides the read replica connection address. You can use this address to connect to the read replica.

Example command:

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

Parameter description:

• Read Replica Connection Address: On the Instances page, click the instance to go to the Basic Information page. Choose Connections. Click the Private Connection tab. In the Address area, obtain the connection address of the read replica instance.

Figure 5-21 Obtaining the read replica connection address

Private Connection	Public Conr	nection				
Basic Information						
Database Port	8635 🖉		VPC	dds-st-	test-vpc	
SSL	O ₹		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>		1:8635/test?auth	Source=admin&replicaSet=replic	a 🗂 Learn more
Read replica {1} Conn	ection Address	mongodb://rwuser: <password>@</password>	est?authSourc	e=admin 🗇		
Read replica {2} Conn	ection Address	mongodb://rwuser: <password>@</password>	'test?authSour	ce=admin 🗇		

The format of the read replica connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

Pay attention to the following parameters in the read replica connection address:

Parameter	Description
rwuser	Account name, that is, the database username.
<password></password>	Password for the database account. Replace it with the actual password.
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively.
	For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25*** %21%24 .
192.168.xx.xx:8635	IP address and port of the read replica of the replica set instance.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user rwuser must be admin . authSource=admin is fixed in the command.

 Table 5-14 Parameter description

- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: The replica set certificate is generated using the internal management IP address to ensure that internal communication does not occupy resources such as the user IP address and bandwidth. -sslAllowInvalidHostnames is needed for the SSL connection through a private network.

Command example:

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

NOTE

When connecting to an instance using the read replica connection address, add double quotation marks (") before and after the connection information.

If the following information is displayed, the instance is successfully connected: replica:SECONDARY>

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

- **Step 1** Log in to the ECS.
- **Step 2** Connect to a DDS instance. The DDS console provides the read replica connection address. You can use this address to connect to the read replica.

Example command:

./mongo "<Read replica connection address>"

Read Replica Connection Address: On the **Instances** page, click the instance to go to the **Basic Information** page. Choose **Connections**. Click the **Private Connection** tab. In the **Address** area, obtain the connection address of the read replica instance.

Figure 5-22 Obtaining the read replica connection address

Private Connection	Public Conn	ection				
Basic Information						
Database Port	8635 🖉		VPC	dds-st	-test-vpc	
SSL	7		Subnet	dds-st	-test-subnet-2	
Auto-switch Private I	P Address					
Address						
Cross-CIDR Access		Disabled Enable				
Private HA Connectio	on Address	mongodb://rwuser: <password>@</password>		1:8635/test?auth	nSource=admin&replicaSet=replic	a 🗇 Learn more
Read replica {1} Con	nection Address	mongodb://rwuser: <password>@</password>	est?authSourc	e=admin 🗇		
Read replica {2} Con	nection Address	mongodb://rwuser: <password>@</password>	'test?authSour	rce=admin 🗇		

The format of the read replica connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

mongodb://rwuser:<*password>@192.168.xx.xx:8635*/**test?authSource=admin**
Pay attention to the following parameters in the private HA address:

Parameter	Description			
rwuser	Account name, that is, the database username.			
<password></password>	Password for the database account. Replace it with the actual password.			
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively.			
	For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25*** %21%24 .			
192.168.xx.xx:8635	IP address and port of the read replica of the replica set instance.			
test	The name of the test database. You can set this parameter based on your service requirements.			
authSource=admin	The authentication database of user rwuser must be admin . authSource=admin is fixed in the command.			

Table	5-15	Parameter	description
-------	------	-----------	-------------

Command example:

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

If the following information is displayed, the instance is successfully connected: replica:SECONDARY>

----End

5.2.4 Connecting to a Replica Set Instance over a Public Network

5.2.4.1 Binding and Unbinding an EIP

After you create an instance, you can bind an EIP to it to allow external access. If later you want to prohibit external access, you can also unbind the EIP from the DB instance.

Precautions

- Deleting a bound EIP does not mean that the EIP is unbound.
- Before accessing a database, apply for an EIP on the VPC console. Then, add an inbound rule to allow the IP addresses or IP address ranges of ECSs. For details, see **Configuring Security Group Rules**.

• In the replica set instance, only primary and secondary nodes can have an EIP bound. To change the EIP that has been bound to a node, you need to unbind it from the node first.

Binding an EIP

- Step 1 Log in to the management console.
- **Step 2** Click ^(Q) in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the replica set instance name.
- Step 5 In the navigation pane on the left, choose Connections. Click the Public
 Connection tab. In the Basic Information area, locate the node you want to bind an EIP to and click Bind EIP in the Operation column.

Figure 5-23 Binding an EIP

Private (Connection Public Connection						
Basi	ic Information			SSL	• +		
Add	1855 For 8635 12						
Publi	c Network Connection Address Unbound						
,	Name/ID	Role	AZ	Private IP Address	EIP	Operation	
8		Secondary	az2		Unbound	Change Private IP Address	Bind EIP
8		Primary	az2		Unbound	Change Private IP Address	Bind EIP
8		Hidden	az2		-	Change Private IP Address	

You can also locate the node in the **Node Information area** on the **Basic Information** page and click **Bind EIP** in the **Operation** column.

Figure 5-24 Binding an EIP

Node Information									
Charge Secondary Hodes State									
Q. Select one or more filters from the pop-up lasts. If you enter a keywood without a filter applied, the system will search for all names matching this keyword.									
Name/ID	Role	Status	AZ	Private IP Address	EIP	Operation			
dds-3707_replica_node_1 f2672eb8d750427fbf767deabef87eacno02	Secondary	Available	cn-north-4a		Unbound	Restart: View Metric: More Y			
dds-3707_replica_node_2 62921741af3443a9bf52d15116cccf33no02	Primary	Available	cn-north-4a		Unbound	View Metric Change Private IP Address Bind EIP			
dds-3707_replica_node_3 8cec491e65c44b4ebc19c1b144413bd8no02	Hidden	Available	cn-north-4a			Restart View Metric Change Private IP Address			

Step 6 In the displayed dialog box, all available unbound EIPs are listed. Select the required EIP and click **OK**. If no available EIPs are displayed, click **View EIP** and create an EIP on the VPC console.

Figure 5-25 Selecting an EIP

For security purpoutbound and in	poses, after bindi bound rules in th	ng the EIP, use <mark>SSL</mark> to con e security group.	nnect to the database and add	
lode Information	Node Name		Status	
			Available	
elect EIP				(
EIP		Status	Bandwidth	
•			5 Mbit/s	
0		⊗ Unbound	5 Mbit/s	
0		🕲 Unbound	88 Mbit/s	
Sever EID				

Step 7 Locate the target node. In the EIP column, you can view the EIP that was bound.To unbind an EIP from the instance, see Unbinding an EIP.

----End

Unbinding an EIP

- Step 1 Log in to the management console.
- **Step 2** Click ^(Q) in the upper left corner and select a region and a project.
- Step 3 Click = in the upper left corner of the page and choose Databases > Document Database Service.
- **Step 4** On the **Instances** page, click the replica set instance that has been bound with an EIP.
- Step 5 In the navigation pane on the left, choose Connections. Click the Public Connection tab. In the Basic Information area, locate the node and click Unbind EIP in the Operation column.

Figure 5-26 Unbinding an EIP

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

You can also locate the node in the **Node Information area** on the **Basic Information** page and click **Unbind EIP** in the **Operation** column.

Step 6 In the displayed dialog box, click Yes.

To bind an EIP to the instance again, see **Binding an EIP**.

----End

5.2.4.2 Configuring Security Group Rules

A security group is a collection of access control rules for ECSs and DDS instances that have the same security protection requirements and are mutually trusted in a VPC.

To ensure database security and reliability, you need to configure security group rules to allow specific IP addresses and ports to access the instance.

If you attempt to connect to an instance through an EIP, you need to configure an inbound rule for the security group associated with the instance.

Precautions

- By default, an account can create up to 500 security group rules.
- Too many security group rules will increase the first packet latency, so a maximum of 50 rules for each security group is recommended.
- By default, one DDS instance is associated with only one security group.
- DDS allows you to associate multiple security groups to a DB instance. You can apply for the service based on your service requirements. For better network performance, you are advised to select no more than five security groups.

Procedure

Step 1 Log in to the management console.

Step 2 Click ^Q in the upper left corner and select a region and a project.

- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the instance name. The **Basic Information** page is displayed.
- **Step 5** In the **Network Information** area on the **Basic Information** page, click the security group.

Figure 5-27 Security Group

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

You can also choose **Connections** in the navigation pane on the left. On the **Public Connection** tab, in the **Security Group** area, click the security group name.

Figure 5-28 Security Group

Constitut Constant						
Security Group						
Security Group	default 🖉					
Inbound Rules(6)	Outbound Rules(3)					
Security Group	Protocol & Port (?)	Туре				
default	TCP:22	IPv4				

- **Step 6** On the **Security Group** page, locate the target security group and click **Manage Rule** in the **Operation** column.
- **Step 7** On the **Inbound Rules** tab, click **Add Rule**. The **Add Inbound Rule** dialog box is displayed.
- **Step 8** Add a security group rule as prompted.

Figure 5-29 Add Inbound Rule

Add Inbou	Add Inbound Rule Learn more about security group configuration.							
Some sec If you sele	curity group rules will n ect IP address for Sour	ot take effect for ECS: ce, you can enter mul	s with certain specifications. Learn mo tiple IP addresses, separated with cor	ne mmas (,). Each IP address represents	a different security g	roup rule.		
Security Group You can import m	default ultiple rules in a batch.							
Priority 💿	Action (?)	Туре	Protocol & Port 💿	Source 💿	Description	Operation		
1-100	Allow ~	IPv4 v	Protocols / TCP (Cus V Example: 22 or 22,24 or 22-3	IP address ✓ 0.0.0.0/0 × ✓		Replicate Delete		
			🕀 Add Rule	3				
					(Cancel OK		

Paramete r	Description	Example
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	The security group rule actions. A rule with a deny action overrides another with an allow action if the two rules have the same priority.	Allow
Protocol & Port	The network protocol required for access. The option can be All , TCP , UDP , ICMP , or GRE .	ТСР
	Port: the port on which you wish to allow access to DDS. The default port is 8635. The port ranges from 2100 to 9500 or can be 27017, 27018, or 27019.	8635
Туре	IP address type. Only IPv4 and IPv6 are supported.	IPv4
Source	 Specifies the supported IP address, security group, and IP address group, which allow access from IP addresses or instances in other security group. Example: Single IP address: 192.168.10.10/32 IP address segment: 192.168.1.0/24 All IP addresses: 0.0.0.0/0 Security group: sg-abc IP address group: ipGroup-test If you enter a security group, all ECSs associated with the security group comply with the created rule. For more information about IP address groups, see IP Address Group Overview. 	0.0.0/0
Descriptio n	(Optional) Provides supplementary information about the security group rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

Step 9 Click OK.

----End

5.2.4.3 Connecting to a Replica Set Instance Using Mongo Shell (Public Network)

In the following scenarios, you can access a DDS instance from the Internet by binding an EIP to the instance.

Scenario 1: Your applications are deployed on an ECS and are not in the same region as the DDS instance.

Figure 5-30 Accessing DDS from ECS across regions



Scenario 2: Your applications are deployed on a cloud server provided by other vendors.



Figure 5-31 Accessing DDS from other cloud servers

This section describes how to use Mongo Shell to connect to a replica set instance through an EIP.

You can connect to an instance using an SSL connection or an unencrypted connection. The SSL connection is encrypted and more secure. To improve data transmission security, connect to instances using SSL.

Prerequisites

- 1. For details about how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
- 2. **Bind an IP** to the replica set instance and **configure security group rules** to ensure that the replica set instance can be accessed from an ECS.
- Install the MongoDB client on the ECS.
 For details about how to install a MongoDB client, see How Can I Install a MongoDB Client?

NOTE

The version of the installed MongoDB client must be the same as the instance version.

SSL Connection

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

- Step 1 Log in to the management console.
- **Step 2** Click ^(Q) in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the instance name.
- **Step 5** In the navigation pane on the left, choose **Connections**.
- **Step 6** In the **Basic Information** area, click $\stackrel{\perp}{\rightharpoonup}$ next to the **SSL** field.
- **Step 7** Upload the root certificate to the ECS to be connected to the instance.

The following describes how to upload the certificate to a Linux and Windows ECS:

 In Linux, run the following command: scp
 scp</li

D NOTE

- IDENTITY_FILE is the directory where the root certificate resides. The file access permission is 600.
- **REMOTE_USER** is the ECS OS user.
- **REMOTE_ADDRESS** is the ECS address.
- **REMOTE_DIR** is the directory of the ECS to which the root certificate is uploaded.
- In Windows, upload the root certificate using a remote connection tool.
- **Step 8** Connect to the instance in the directory where the MongoDB client is located.

Method 1: Using a public network connection address

Example command:

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

Parameter description:

• **Public Network Connection Address**: On the **Instances** page, click the instance to switch to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. Click the **Public Connection** tab and obtain the public network connection address.

Figure 5-32 Obtaining the public network connection address

Basic Information								
Database Port	8635 🖉			SSL		● ₹		
Auto-switch Private IP Address								
Address								
Public Network Connectio	n Address	mongo	db://rwuser: <passw< td=""><td>vord>@10.1</td><td>in familier</td><td>st?authSourc</td><td>e=admin 🗖 I</td><td>earn more</td></passw<>	vord>@10.1	in familier	st?authSourc	e=admin 🗖 I	earn more
		Note	The parameters in	n orange are varia	bles and ne	ed to be mo	dified based o	n service req
		uireme	nts. For details, clic	k Learn more.				

The format of the public connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

Pay attention to the following parameters in the public network connection address:

Parameter	Description
rwuser	Account name, that is, the database username.
<password></password>	Password for the database account. Replace it with the actual password.
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively.
	For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25*** %21%24 .
192.168.xx.xx:8635	The EIP and port bound to the node of the replica set instance.

 Table 5-17
 Parameter description

Parameter	Description
authSource=admin	The authentication database of user rwuser must be admin . authSource=admin is fixed in the command.

- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: The replica set certificate is generated using the internal management IP address to ensure that internal communication does not occupy resources such as the user IP address and bandwidth. -sslAllowInvalidHostnames is needed for the SSL connection through a public network.

Command example:

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

NOTE

- If you connect to an instance over a public HA address, add double quotation marks before and after the connection information.
- To improve read and write performance and prevent errors from being reported when data is written from the client after a primary/standby switchover. For details about how to connect to an instance in HA mode, see **Connecting to a Replica Set Instance for Read and Write Separation and High Availability**.

Method 2: Using an EIP

Example command:

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

Parameter description:

• **DB_HOST** is the EIP bound to the instance node to be connected.

On the **Instances** page, click the instance to go to the **Basic Information** page. Choose **Connections** > **Public Connection** and obtain the EIP of the corresponding node.

• **DB_PORT** is the database port. The default port number is 8635.

You can click the instance to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

Figure 5-33 Obtaining the port

E	asic Information					
C	atabase Port	8635			SSL	
-	ddress					
P	ublic Network Conne	ction Add	ress	mongodb://rw admin 🗇	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** is the database user. The default value is **rwuser**.
- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: The replica set certificate is generated using the internal management IP address to ensure that internal communication does not occupy resources such as the user IP address and bandwidth. -sslAllowInvalidHostnames is needed for the SSL connection through a public network.

Enter the database account password when prompted:

Enter password:

Command example:

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

- **Step 9** Check the connection result. If the following information is displayed, the connection is successful.
 - The primary node of the replica set is connected. replica:PRIMARY>
 - The secondary node of the replica set is connected. replica:SECONDARY>

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

- Step 1 Log in to the ECS.
- **Step 2** Connect to a DDS instance.

Method 1: Using a public network connection address

Example command:

./mongo "<Public network address>"

Public Network Connection Address: On the **Instances** page, click the instance to switch to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. Click the **Public Connection** tab and obtain the public network connection address.

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

Figure 5-34 Obtaining the public network connection address

The format of the public connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

Pay attention to the following parameters in the public connection address:

Parameter	Description
rwuser	Account name, that is, the database username.
<password></password>	Password for the database account. Replace it with the actual password.
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively.
	For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25*** %21%24 .
192.168.xx.xx:8635	The EIP and port bound to the node of the replica set instance.
authSource=admin	The authentication database of user rwuser must be admin . authSource=admin is fixed in the command.

Table 5-18 Parameter description

Command example:

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

D NOTE

- If you connect to an instance over a public HA address, add double quotation marks before and after the connection information.
- To improve read and write performance and prevent errors from being reported when data is written from the client after a primary/standby switchover, you are advised to connect to an instance using the HA connection address. For details, see **Connecting to a Replica Set Instance for Read and Write Separation and High Availability**.

Method 2: Using an EIP

Example command:

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

Parameter description:

- **DB_HOST** is the EIP bound to the instance node to be connected.
 - On the **Instances** page, click the instance to go to the **Basic Information** page. Choose **Connections** > **Public Connection** and obtain the EIP of the corresponding node.
- **DB_PORT** is the database port. The default port number is 8635.

You can click the instance to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

Figure 5-35 Obtaining the port

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

• **DB_USER** is the database user. The default value is **rwuser**.

Enter the database account password when prompted:

Enter password:

Command example:

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

- **Step 3** Check the connection result. If the following information is displayed, the connection is successful.
 - The primary node of the replica set is connected. replica:PRIMARY>
 - The secondary node of the replica set is connected. replica:SECONDARY>

----End

5.2.4.4 Connecting to a Replica Set Instance Using Robo 3T

To connect to an instance from a local device, you can use Robo 3T to access the instance from the Internet.

This section describes how to use Robo 3T to connect to a replica set instance from a local device. In this section, the Windows operating system (OS) used by the client is used as an example.

Robo 3T can connect to an instance with an unencrypted connection or an encrypted connection (SSL). To improve data transmission security, connect to instances using SSL.

Connection Diagram



Figure 5-36 Connection diagram

Prerequisites

- 1. Bind an EIP to the ECS and configure security group rules.
 - a. Bind an EIP to the replica set instance.
 - For details about how to bind an EIP, see **Binding and Unbinding an EIP**.
 - b. Obtain the IP address of a local device.
 - c. Configure security group rules.

Add the IP address obtained in **1.b** and the instance port to the inbound rule of the security group.

For details about how to configure security group rules, see **Configuring Security Group Rules**.

- d. Run the ping command to ping the EIP bound in **1.a** to ensure that the EIP is accessible through your local device.
- 2. Install Robo 3T.
 - a. For details, see Installing Robo 3T.

SSL

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

Step 1 Run the installed Robo 3T. On the displayed dialog box, click **Create**.

Figure 5-37 Connections

!	🛃 MongoDB Connections					×
Ľ	<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 - Cance	1

Step 2 In the **Connection Settings** dialog box, set the parameters of the new connection.

1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the DDS DB instance in the **Address** text box.

Figure 5-38 Connection

📃 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 eithe IPv4, IPv6 or domain name.	nr
From URI	Import connection details from MongoDB URI connection str	ing
1 <u>T</u> est	Save	icel

2. On the **Authentication** tab, set **Database** to **admin**, **User Name** to **rwuser**, and **Password** to the administrator password you set during the creation of the cluster instance.

Figure 5-39 Authentication

Connection S	ettings)
Connection	Authentication SSH TLS Advanced	
🗹 Perform aut	thentication	
Database	admin	
	The admin database is unique in MongoDB. Users with	
User Name	rwuser	
Password	<u>۱</u>	•
Auth Mechanism	SCRAM-SHA-1	\sim
Manually sp	pecify visible databases	
i <u>T</u> est	Save Cano	el

3. On the **TLS** tab, select **Use TLS protocol** and select **Self-signed Certificate** for **Authentication Method**.

Figure 5-40 SSL

📃 Connection Settings			
Connection Authentic	vation SSH TLS Advanced		
🗹 Use TLS protocol			
Authentication Method: Self-signed Certificate 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.			
	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			
1 Iest	Save Cancel		

- 4. Click Save.
- **Step 3** On the **MongoDB Connections** page, click **Connect** to connect to the replica set instance.

🛃 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	
			📃 C <u>o</u> nnect 🛛 Cancel	

Step 4 If the replica set instance is successfully connected, the page shown in Figure 5-42 is displayed.

Figure 5-42 Connection succeeded

🍨 Robo 3T - 1.4		
File View Options Wind	ow Help	
🛃 • 📄 🔒 🕨 💷	22	
 test (3) System System 	♦ Welcome × ♦ db.getCollection('system'''×	• db. getCollection(' system. *** *
 Collections (4) 	db.getCollection('system.roles').fin	d(∯)
Y System	🕔 0.089 sec.	
 system.k system.r system.u system.v 	Fetched 0 record(s) in 88ms	
> Functions > Users >] local		
> 🗏 config		

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details, see **Enabling and Disabling SSL**.

Step 1 Run the installed Robo 3T. On the displayed dialog box, click **Create**.

Figure 5-43 Connections

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

Step 2 In the **Connection Settings** dialog box, set the parameters of the new connection.

1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the DDS DB instance in the **Address** text box.

Figure 5-44 Connection

📃 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 eithe: IPv4, IPv6 or domain name.	r
From URI	Import connection details from MongoDB URI connection stri	ng
1 <u>T</u> est	Save Can	cel

2. On the **Authentication** tab, set **Database** to **admin**, **User Name** to **rwuser**, and **Password** to the administrator password you set during the creation of the cluster instance.

Figure 5-45 Authentication

	Settings	×
Connection	Authentication SSH TLS Advanced	
🗹 Perform au	thentication	
Database	admin	
	The admin database is unique in MongoDB. Users wi	th
User Name	rwuser	
Password		Ś
Auth Mechanis	m SCRAM-SHA-1	\sim
🗌 Manually s	pecify visible databases	
<u>1</u> est	Save	ancel

- 3. Click Save.
- **Step 3** On the **MongoDB Connections** page, click **Connect** to connect to the replica set instance.

5				
🛃 MongoDB Connections				×
<u>Create, edit, remove, clone</u> or :	reorder connections via drag'n'	drop.		
Name	Address	Attributes	Auth. Database / User	
📃 test	:8635	TLS	🔎 admin / rwuser	
L			Connect Cano	.e]

Figure 5-46 Replica set connection information

Step 4 If the replica set instance is successfully connected, the page shown in **Figure 5-47** is displayed.

Figure 5-47 Connection succeeded

e View Options Wind	low Help
• 📄 🖬 🕨 🔳	32
 test (3) System admin Collections (4) System 	♦ Welcome × ♦ db.getCollection('system''' × ♦ db.getCollection('system.''' ×
	📑 test 🗮 10. 154. 221. 78:8635 📄 admin
	<pre>db.getCollection('system.roles').find(())</pre>
	() 0.089 sec.
> system.r	Fetched 0 record(s) in 88ms
> system.u	
> system.v	
> Functions	
> Users	
> 🗐 local	
> 🗟 config	

----End

5.2.5 Connecting to a Replica Set Instance Using Program Code

5.2.5.1 Java

If you are connecting to an instance using Java, an SSL certificate is optional, but downloading an SSL certificate and encrypting the connection will improve the security of your instance. SSL is disabled by default for newly created instances, but you can enable SSL by referring to **Enabling or Disabling SSL**. SSL encrypts connections to databases but it increases the connection response time and CPU usage. For this reason, enabling SSL is not recommended.

Prerequisites

Familiarize yourself with:

- Computer basics
- Java code

Obtaining and Using Java

- Download the Jar driver from: https://repo1.maven.org/maven2/org/ mongodb/mongo-java-driver/3.0.4/
- To view the usage guide, visit https://mongodb.github.io/mongo-javadriver/4.2/driver/getting-started/installation/.

Using an SSL Certificate

NOTE

- Download the SSL certificate and verify the certificate before connecting to databases.
- In the **DB Information** area on the **Basic Information** page, click $\stackrel{l}{\rightharpoonup}$ in the **SSL** field to download the root certificate or certificate bundle.
- For details about how to set up an SSL connection, see the MongoDB Java Driver official document at https://www.mongodb.com/docs/drivers/java/sync/current/ fundamentals/connection/tls/#std-label-tls-ssl.
- Java Runtime Environment (JRE) earlier than Java 8 enables TLS 1.2 only in updated versions. If TLS 1.2 is not enabled for your JRE, upgrade it to a later version to use TLS 1.2 for connection.

Use Java to connect to the replica set. The format of the Java code is as follows: mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>? authSource=admin&replicaSet=replica&ssl=true

Parameter	Description	
<username></username>	Current username.	
<password></password>	Password for the current username	
<instance_ip></instance_ip>	If you attempt to access the instance from an ECS, set <i>instance_ip</i> to the private IP address displayed on the Basic Information page of the instance to which you intend to connect.	
	If you intend to access the instance through an EIP, set <i>instance_ip</i> to the EIP that has been bound to the instance.	
<instance_port></instance_port>	Database port displayed on the Basic Information page. Default value: 8635	
<database_name ></database_name 	Name of the database to be connected.	
authSource	Authentication user database. The value is admin .	

Table 5-19 Parameter description
Parameter	Description
ssl	Connection mode. true indicates that the SSL connection mode is used.

Use the keytool to configure the CA certificate. For details about the parameters, see **Table 5-20**.

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

Table 5-20 Parameter description

Parameter	Description
<path authority="" certificate="" file="" to=""></path>	Path for storing the SSL certificate.
<path store="" to="" trust=""></path>	Path for storing the truststore. Set this parameter as required, for example, ./ trust/certs.keystore.
<password></password>	Custom password.

Set the JVM system properties in the program to point to the correct truststore and keystore:

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

For details about the Java code, see the following example:

```
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");
     }
  }
}
```

Connection Without the SSL Certificate

NOTE

You do not need to download the SSL certificate because certificate verification on the server is not required.

Connect to a replica set instance using Java. The Java link format is as follows: mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>? authSource=admin&replicaSet=replica

Table 5-21 Parameter descriptic

Parameter	Description
<username></username>	Current username.
<password></password>	Password for the current username
<instance_ip></instance_ip>	If you attempt to access the instance from an ECS, set <i>instance_ip</i> to the private IP address displayed on the Basic Information page of the instance to which you intend to connect.
	If you intend to access the instance through an EIP, set <i>instance_ip</i> to the EIP that has been bound to the instance.
<instance_port></instance_port>	Database port displayed on the Basic Information page. Default value: 8635
<database_name ></database_name 	Name of the database to be connected.
authSource	Authentication user database. The value is admin .

For details about the Java code, see the following example:

```
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");
     }
  }
```

}

5.2.5.2 Python

This section describes how to connect to a replica set instance using Python.

Prerequisites

1. To connect an ECS to an instance, the ECS must be able to communicate with the DDS instance. You can run the following command to connect to the IP address and port of the instance server to test the network connectivity.

curl ip:port

If the message **It looks like you are trying to access MongoDB over HTTP on the native driver port** is displayed, the network connectivity is normal.

- 2. Install Python and third-party installation package **pymongo** on the ECS. Pymongo 2.8 is recommended.
- 3. If SSL is enabled, you need to download the root certificate and upload it to the ECS.

Connection Code

Enabling 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
 Disabling 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
```

NOTE

- The authentication database in the URL must be **admin**. That means setting **authSource** to **admin**.
- In SSL mode, you need to manually generate the trustStore file.
- The authentication database must be **admin**, and then switch to the service database.

6 Getting Started with Single Nodes

6.1 Connecting to a Single Node Instance

6.1.1 Connection Methods

You can access DDS over private or public networks.

Table 6-1 Connection methods

Metho d	IP Address	Scenario	Description
DAS	Not required	DAS provides a GUI and allows you to perform visualized operations on the console. SQL execution, advanced database management, and intelligent O&M are available to make database management simple, secure, and intelligent.	 Easy to use, secure, advanced, and intelligent Recommended
Private netwo rk	Private IP address	DDS provides a private IP address by default. If your applications are running on an ECS in the same region, AZ, and VPC subnet as your DDS instance, you are advised to use a private IP address to connect the ECS to your DDS instances.	Secure and excellent performance

Metho d	IP Address	Scenario	Description
Public netwo rk	EIP	 If your applications are running on an ECS that is in a different region from the one where the DB instance is located, use an EIP to connect the ECS to your DDS DB instances. If your applications are deployed on another cloud platform, EIP is recommended. 	 Low security For faster transmission and improved security, you are advised to migrate your applications to an ECS that is in the same subnet as your DDS instance and use a private IP address to access the instance.

6.1.2 (Recommended) Connecting to a Single Node Instance Through DAS

6.1.2.1 Overview

DAS provides a GUI and allows you to perform visualized operations on the console. SQL execution, advanced database management, and intelligent O&M are available to make database management simple, secure, and intelligent. You are advised to use DAS to connect to DB instances.

This section decribes how to connect to a single node instance through DAS.

Process

To connect to a single node instance, perform the following steps:

1. Connect to a single node instance through DAS.

6.1.2.2 Connecting to a Single Node Instance Through DAS

Data Admin Service (DAS) enables you to manage DB instances on a web-based console, simplifying database management and improving working efficiency. You can connect and manage instances through DAS. By default, you have the permission required for remote login. It is recommended that you use the DAS service to connect to instances. DAS is secure and convenient.

Procedure

Step 1 Log in to the management console.

Step 2 Click ^(Q) 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.

- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, locate the target DB instance and click **Log In** in the **Operation** column.

Alternatively, click the target DB instance on the **Instances** page. On the displayed **Basic Information** page, click **Log In** in the upper right corner of the page.

Figure 6-1 Instance management

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 ↓Ξ	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 👻

Step 5 On the displayed login page, enter the administrator username and password and click **Login**.

For details about how to manage databases through DAS, see **DDS Instance Management**.

----End

6.1.3 Connecting to a Single Node Instance over a Private Network

6.1.3.1 Configuring a Security Group

A security group is a logical group. It provides access control policies for the ECSs and instances that have the same security protection requirements and are mutually trusted in a VPC.

To ensure database security and reliability, you need to configure security group rules to allow specific IP addresses and ports to access DDS instances.

You can connect to an instance by configuring security group rules in following two ways:

 If the ECS and instance are in the same security group, they can communicate with each other by default. No security group rule needs to be configured. Go to Connecting to a Single Node Instance Using Mongo Shell (Private Network).

Figure 6-2 Same security group



• If the ECS and instance are in different security groups, you need to configure security group rules for them, separately.

Figure 6-3 Different security groups



- Instance: Configure an **inbound rule** for the security group associated with the instance.
- ECS: The default security group rule allows all outbound data packets. In this case, you do not need to configure a security group rule for the ECS. If not all traffic is allowed to reach the instance, configure an **outbound** rule for the ECS.

This section describes how to configure an inbound rule for an instance.

Precautions

- By default, an account can create up to 500 security group rules.
- Too many security group rules will increase the first packet latency, so a maximum of 50 rules for each security group is recommended.
- By default, one DDS instance is associated with only one security group.
- DDS allows you to associate multiple security groups to a DB instance. You can apply for the service based on your service requirements. For better

network performance, you are advised to select no more than five security groups.

Procedure

- Step 1 Log in to the management console.
- **Step 2** Click ^(Q) in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the instance name. The **Basic Information** page is displayed.
- **Step 5** In the **Network Information** area on the **Basic Information** page, click the security group.

Figure 6-4 Security Group

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

You can also choose **Connections** in the navigation pane on the left. On the **Private Connection** tab, in the **Security Group** area, click the security group name.

Figure 6-5 Security Group

Security Group		
Security Group	default 🖉	
Inbound Rules(6)	Outbound Rules(3)	
Security Group	Protocol & Port (?)	Туре
default	TCP:22	IPv4

- **Step 6** On the **Security Group** page, locate the target security group and click **Manage Rule** in the **Operation** column.
- **Step 7** On the **Inbound Rules** tab, click **Add Rule**. The **Add Inbound Rule** dialog box is displayed.
- **Step 8** Add a security group rule as prompted.

Figure 6-6 Add Inbound Rule

Add Inbour	nd Rule Learn	more about secu	rity group configuration.			×
Some sec If you sele	urity group rules will no oct IP address for Sourc	it take effect for ECSs æ, you can enter mult	with certain specifications. Learn mo iple IP addresses, separated with con	re nmas (,). Each IP address represent:	s a different security g	roup rule.
Security Group	default ultiple rules in a batch.					
Priority (?)	Action (?)	Туре	Protocol & Port ?	Source 🕐	Description	Operation
1-100	Allow ~	IPv4 v	Protocols / TCP (Cus V Example: 22 or 22,24 or 22-3	IP address ✓ 0.0.0.0/0 × ✓		Replicate Delete
			⊕ Add Rule			Cancel

Table 6-2 Inbound rule settings

Paramete r	Description	Example
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	The security group rule actions. A rule with a deny action overrides another with an allow action if the two rules have the same priority.	Allow
Protocol & Port	The network protocol required for access. Available options: TCP , UDP , ICMP , or GRE	ТСР
	Port: the port on which you wish to allow access to DDS. The default port is 8635. The port ranges from 2100 to 9500 or can be 27017, 27018, or 27019.	8635
Туре	IP address type. Only IPv4 and IPv6 are supported.	IPv4

Paramete r	Description	Example
Source	Specifies the supported IP address, security group, and IP address group, which allow access from IP addresses or instances in other security group. Example:	0.0.0/0
	• Single IP address: 192.168.10.10/32	
	• IP address segment: 192.168.1.0/24	
	All IP addresses: 0.0.0.0/0	
	Security group: sg-abc	
	IP address group: ipGroup-test	
	If you enter a security group, all ECSs associated with the security group comply with the created rule.	
	For more information about IP address groups, see IP Address Group.	
Descriptio n	(Optional) Provides supplementary information about the security group rule. This parameter is optional.	-
	The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	

Step 9 Click OK.

----End

6.1.3.2 Connecting to a Single Node Instance Using Mongo Shell (Private Network)

Mongo shell is the default client for the MongoDB database server. You can use Mongo Shell to connect to DB instances, and query, update, and manage data in databases. DDS is compatible with MongoDB. Mongo Shell is a part of the MongoDB client. To use Mongo Shell, download and install the MongoDB client first, and then use the Mongo shell to connect to the DB instance.

By default, a DDS instance provides a private IP address. If your applications are deployed on an ECS and are in the same region and VPC as DDS instances, you can connect to DDS instances using a private IP address to achieve a fast transmission rate and high security.

This section describes how to use Mongo Shell installed on a Linux ECS to connect to a single node instance over a private network.

You can connect to an instance using an SSL connection or an unencrypted connection. The SSL connection is encrypted and more secure. To improve data transmission security, connect to instances using SSL.

Prerequisites

- 1. For details about how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
- Install the MongoDB client on the ECS.
 For details about how to install a MongoDB client, see How Can I Install a MongoDB Client?
- 3. The ECS can communicate with the DDS instance. For details, see ECS.

SSL

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

- Step 1 Log in to the management console.
- **Step 2** Click ¹ in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the instance name.
- **Step 5** In the navigation pane on the left, choose **Connections**.
- **Step 6** In the **Basic Information** area, click $\stackrel{\perp}{\rightharpoonup}$ next to the **SSL** field.
- Step 7 Import the root certificate to the Linux or Windows ECS. For details, see How Can I Import the Root Certificate to a Windows or Linux OS?
- **Step 8** Connect to a DDS instance.

Using a private IP address

Example command:

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

Parameter description:

• **DB_HOST** is the private IP address of the instance to be connected.

On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. On the **Private Connection** tab, obtain the IP address of the corresponding node.

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** is the database port. The default port number is 8635.

You can click the instance name to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Private Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

Figure 6-7 Obtaining the port

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

- **DB_USER** is the database user. The default value is **rwuser**.
- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: To ensure that the internal communication of the single nodes does not occupy resources such as the user IP address and bandwidth, the single node certificate is generated using the internal management IP address. --sslAllowInvalidHostnames is needed for the SSL connection over private networks.

Command example:

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

Enter the database password when prompted:

Enter password:

Step 9 Check the connection result. If the following information is displayed, the connection is successful. replica:PRIMARY>

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

- **Step 1** Log in to the ECS.
- **Step 2** Connect to a DDS instance.

Using a private IP address

Example command:

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

Parameter description:

• **DB_HOST** is the private IP address of the instance to be connected.

On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. On the **Private Connection** tab, obtain the IP address of the corresponding node.

Node Information



• **DB_PORT** is the database port. The default port number is 8635.

You can click the instance name to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Private Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

Figure 6-8 Obtaining the port

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

• **DB_USER** is the database user. The default value is **rwuser**.

Command example:

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

Enter the database password when prompted:

Enter password:

Step 3 Check the connection result. If the following information is displayed, the connection is successful. replica:PRIMARY>

----End

6.1.4 Connecting to a Single Node Instance over a Public Network

6.1.4.1 Binding and Unbinding an EIP

After you create an instance, you can bind an EIP to it to allow external access. If later you want to prohibit external access, you can also unbind the EIP from the instance.

Precautions

- Deleting a bound EIP does not mean that the EIP is unbound.
- Before accessing a database, apply for an EIP on the VPC console. Then, add an inbound rule to allow the IP addresses or IP address ranges of ECSs. For details, see **Configuring a Security Group**.
- To change the EIP that has been bound to a node, unbind it from the node first.

Binding an EIP

Step 1 Log in to the management console.

- **Step 2** Click ¹ in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the single node instance name.
- Step 5 In the navigation pane on the left, choose Connections. Click the Public
 Connection tab. In the Basic Information area, locate the node you want to bind an EIP to and click Bind EIP in the Operation column.

Figure 6-9 Binding an EIP

Private Connection	Public Connect	tion			
Basic Information					
Database Port	8635 🖉			SSL	<u>क</u>
Address					
Public Network Connect	tion Address Ur	nbound			
Name/ID	AZ	Private IP Address	Private Domain	EIP	Operation
dds-d629_single_nod	e_1 az1	192.	d42ec4836de74		Change Private IP Address More 🛦 Change Private Domain Name
					Bind EIP

You can also locate the node in the **Node Information** area on the **Basic Information** page and click **Bind EIP** in the **Operation** column.

Figure 6-10 Binding an 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 Private IP Address More 🔺
						Change Private Domain Name
						Bind EIP

Step 6 In the displayed dialog box, all available unbound EIPs are listed. Select the required EIP and click **OK**. If no available EIPs are displayed, click **View EIP** and create an EIP on the VPC console.

Figure 6-11 Selecting an EIP

For security purp outbound and in	boses, after bindir bound rules in the	ng the EIP, use SSL to con e security group.	inect to t	the database and add	
lode Information	Node Name	Node Name		Status	
			A)	vailable	
elect EIP					C
EIP		Status		Bandwidth	
		Onbound		5 Mbit/s	
0		⊗ Unbound		5 Mbit/s	
0		🕲 Unbound		88 Mbit/s	

Step 7 In the **EIP** column, you can view the EIP that was bound.

To unbind an EIP from the instance, see **Unbinding an EIP**.

----End

Unbinding an EIP

Step 1 Log in to the management console.

- **Step 2** Click \bigcirc in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the single node instance name.
- Step 5 In the navigation pane on the left, choose Connections. Click the Public
 Connection tab. In the Basic Information area, locate the node and click Unbind EIP in the Operation column.

Figure 6-12 Unbinding an EIP

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

You can also locate the node in the **Node Information area** on the **Basic Information** page and click **Unbind EIP** in the **Operation** column.

Step 6 In the displayed dialog box, click Yes.

To bind an EIP to the instance again, see **Binding an EIP**.

----End

6.1.4.2 Configuring a Security Group

A security group is a logical group. It provides access control policies for the ECSs and instances that have the same security protection requirements and are mutually trusted in a VPC.

To ensure database security and reliability, you need to configure security group rules to allow specific IP addresses and ports to access DDS instances.

If you attempt to connect to an instance through an EIP, you need to configure an inbound rule for the security group associated with the instance.

Precautions

- By default, an account can create up to 500 security group rules.
- Too many security group rules will increase the first packet latency, so a maximum of 50 rules for each security group is recommended.

- By default, one DDS instance is associated with only one security group.
- DDS allows you to associate multiple security groups to a DB instance. You can apply for the service based on your service requirements. For better network performance, you are advised to select no more than five security groups.

Procedure

- Step 1 Log in to the management console.
- **Step 2** Click ¹ in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the instance name. The **Basic Information** page is displayed.
- **Step 5** In the **Network Information** area on the **Basic Information** page, click the security group.

Figure 6-13 Security Group

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

You can also choose **Connections** in the navigation pane on the left. On the **Public Connection** tab, in the **Security Group** area, click the security group name.

Figure 6-14 Security Group

Security Group		
Security Group	default 🖉	
Inbound Rules(6)	Outbound Rules(3)	
Security Group	Protocol & Port (?)	Туре
default	TCP:22	IPv4

- **Step 6** On the **Security Group** page, locate the target security group and click **Manage Rule** in the **Operation** column.
- **Step 7** On the **Inbound Rules** tab, click **Add Rule**. The **Add Inbound Rule** dialog box is displayed.
- **Step 8** Add a security group rule as prompted.

Figure 6-15 Add Inbound Rule

Add Inbound Rule Learn more about security group configuration.						
Some see If you see	curity group rules will no ect IP address for Sourc	ot take effect for ECS: ce, you can enter mul	s with certain specifications. Learn mo tiple IP addresses, separated with cor	re nmas (,). Each IP address represe	ents a different security g	group rule.
Security Group	default nultiple rules in a batch.					
Priority 🕐	Action ⑦	Туре	Protocol & Port 🕐	Source 🕐	Description	Operation
1-100	Allow ~	IPv4 v	Protocols / TCP (Cus V Example: 22 or 22,24 or 22-3	IP address ✓ 0.0.0.0/0 × ✓		Replicate Delete
			⊕ Add Rule		(Cancel

Table 6-3 Inbound rule settings

Paramete r	Description	Example Value
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default priority is 1 and has the	1
	highest priority. The security group rule with a smaller value has a higher priority.	
Action	The security group rule actions.	Allow
	A rule with a deny action overrides another with an allow action if the two rules have the same priority.	
Protocol & Port	The network protocol required for access. The option can be All , TCP , UDP , ICMP , or GRE .	ТСР
	Port: the port on which you wish to allow access to DDS. The default port is 8635. The port ranges from 2100 to 9500 or can be 27017, 27018, or 27019.	8635
Туре	IP address type. Only IPv4 and IPv6 are supported.	IPv4

Paramete r	Description	Example Value
Source	Specifies the supported IP address, security group, and IP address group, which allow access from IP addresses or instances in other security group. Example:	0.0.0/0
	• Single IP address: 192.168.10.10/32	
	• IP address segment: 192.168.1.0/24	
	All IP addresses: 0.0.0.0/0	
	Security group: sg-abc	
	IP address group: ipGroup-test	
	If you enter a security group, all ECSs associated with the security group comply with the created rule.	
	For more information about IP address groups, see IP Address Group .	
Descriptio n	(Optional) Provides supplementary information about the security group rule. This parameter is optional.	-
	The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	

Step 9 Click OK.

----End

6.1.4.3 Connecting to a Single Node Instance Using Mongo Shell (Public Network)

In the following scenarios, you can access a DDS instance from the Internet by binding an EIP to the instance.

Scenario 1: Your applications are deployed on an ECS and are not in the same region as the DDS instance.



Figure 6-16 Accessing DDS from ECS across regions

Scenario 2: Your applications are deployed on a cloud server provided by other vendors.



Figure 6-17 Accessing DDS from other cloud servers

This section describes how to use Mongo Shell to connect to a single node instance through an EIP.

You can connect to an instance using an SSL connection or an unencrypted connection. The SSL connection is encrypted and more secure. To improve data transmission security, connect to instances using SSL.

Prerequisites

- 1. For details about how to create and log in to an ECS, see **Purchasing an ECS** and **Logging In to an ECS**.
- 2. **Bind an EIP** to the single node instance and **configure security group rules** to ensure that the EIP can be accessed from the ECS.
- 3. Install the MongoDB client on the ECS.

For details about how to install a MongoDB client, see How Can I Install a MongoDB Client?

SSL

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

- Step 1 Log in to the management console.
- **Step 2** Click ^(Q) in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the instance name.
- **Step 5** In the navigation pane on the left, choose **Connections**.
- Step 6 In the Basic Information area, click 📥 next to the SSL field.
- Step 7 Import the root certificate to the Linux or Windows ECS. For details, see How Can I Import the Root Certificate to a Windows or Linux OS?
- **Step 8** Connect to the instance in the directory where the MongoDB client is located.

Using an EIP

Example command:

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

Parameter description:

• **DB_HOST** is the EIP bound to the instance to be connected.

On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**> **Public Connection** and obtain the EIP of the corresponding node.

Figure 6-18 Obtaining an EIP

Basic Info	ormati	on							
Database F	Port		8635 🖉			SS	L	▲	
Address									
Public Net	work C	onnectio	n Address	Unbound					
						1			
Name/II	D	AZ	Private	Private	EIP		Operation		
n kana Mana	2	az2	192.16	a4f871	🕲 Unbo	und	Change Private IP	Address More 👻	

• **DB_PORT** is the database port. The default port number is 8635.

You can click the instance name to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

Figure 6-19 Obtaining the port

Basic Information					
Database Port	863	5 🖉		SSL	→ ±
Address					
Public Network Conr	ection Add	Iress	mongodb://n	wuser: <password>6</password>	8635/test?authSource=
Name/ID	AZ	Private I	EIP	Operation	
dds-ce25_mong 000e813fb5574c	az4	192.168		Change Private IP Add	ress Unbind EIP
dds-ce25_mong bad06d1cf2594e	az4	192.168		Change Private IP Add	ress Bind EIP

- **DB_USER** is the database user. The default value is **rwuser**.
- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: To ensure that the internal communication of the single nodes does not occupy resources such as the user IP address and bandwidth, the single node certificate is generated using the internal management IP address. --sslAllowInvalidHostnames is needed for the SSL connection through a public network.

Command example:

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

Enter the database password when prompted:

Enter password:

Step 9 Check the connection result. If the following information is displayed, the connection is successful. replica:PRIMARY>

----End

Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

- **Step 1** Log in to the ECS.
- **Step 2** Connect to a DDS instance.

Using an EIP

Example command:

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

Parameter description:

• **DB_HOST** is the EIP bound to the instance to be connected.

On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**> **Public Connection** and obtain the EIP of the corresponding node.

Figure 6-20 Obtaining an EIP

Basic Informati	on							
Database Port		8635 🖉			SS	L	▲	
Address								
Public Network C	onnectio	on Address	Unbound					
Name/ID	AZ	Private	Private	EIP		Operation		
	az2	192.16	a4f871	🕲 Unbour	nd	Change Private IP A	Address More 👻	

• **DB_PORT** is the database port. The default port number is 8635.

You can click the instance name to go to the **Basic Information** page. In the navigation pane on the left, choose **Connections**. On the displayed page, click the **Public Connection** tab and obtain the port from the **Database Port** field in the **Basic Information** area.

Figure 6-21 Obtaining the port

Basic Information					
Database Port	8635			SSL	—
Address					
Public Network Conn	ection Addr	ess	mongodb:// admin 🗂	/rwuser:~password>≪	8635/test?authSource=
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** is the database user. The default value is **rwuser**.

Command example:

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

Enter the database password when prompted:

Enter password:

Step 3 Check the connection result. If the following information is displayed, the connection is successful.

----End

6.1.4.4 Connecting to a Single Node Instance Using Robo 3T

If you want to connect to an instance from a local device, you can bind an EIP to the instance and use Robo 3T to connect to the instance over a public network.

This section describes how to use Robo 3T to connect to a single node instance from a local device. In this section, the Windows operating system (OS) used by the client is used as an example.

Robo 3T can connect to an instance with an unencrypted connection or an encrypted connection (SSL). To improve data transmission security, connect to instances using SSL.

Connection Diagram



Figure 6-22 Connection diagram

Prerequisites

- 1. **Bind an EIP** to the single node instance and **configure security group rules** to ensure that the instance can be accessed using Robo 3T.
- Install Robo 3T.
 Install Robo 3T. For details, see How Can I Install Robo 3T?

SSL

NOTICE

If you connect to an instance over the SSL connection, enable SSL first. Otherwise, an error is reported. For details about how to enable SSL, see **Enabling and Disabling SSL**.

Step 1 Run the installed Robo 3T. On the displayed dialog box, click **Create**.

MongoDB Connections					×
	,, .,	1			
Lreate, edit, remove, clone or	reorder connections via drag n	drop.			
Name	Address	Attributes	Auth.	Database / U	Íser
			L	📃 C <u>o</u> nnect	Cancel

Figure 6-23 Connections

- **Step 2** In the **Connection Settings** dialog box, set the parameters of the new connection.
 - 1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the DDS DB instance in the **Address** text box.

Figure 6-24 Connection

Connection	Authentication SSH TLS Advanced
Type:	Direct Connection
Name:	test
Address:	: 8635
	Specify host and port of MongoDB server. Host can be either
	Specify host and port of MongoDB server. Host can be either IPv4, IPv6 or domain name.

2. On the **Authentication** tab, set **Database** to **admin**, **User Name** to **rwuser**, and **Password** to the administrator password you set during the creation of the cluster instance.

Figure 6-25 Authentication

Connection S	ettings	×						
Connection	Authentication SSH TLS Advanced							
🗹 Perform authentication								
Database admin								
	The admin database is unique in MongoDB. Users with							
User Name	rwuser							
Password	<u>نه</u>	2						
Auth Mechanism	SCRAM-SHA-1	\sim						
Auth Mechanism SCRAM-SHA-1 ~								
i <u>T</u> est	Save Cano	el						

3. On the **TLS** tab, select **Use TLS protocol** and select **Self-signed Certificate** for **Authentication Method**.

Figure 6-26 SSL

Connection	Settings							×
Connection	Authentic	ation	SSH	TLS	Advanc	ed		
🗹 Use TLS protocol								
Authenticati	on Method:	Self-signed Certificate						\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 ho server	ing self s truste the com wever th identity	-signed cer d. If self- nunication: ere will b, y.	rtificates -signed s channel e no	
🗌 Vse PEM C	ert./Key:	Enable requir	this o es CA-s	ption t igned c	o connec lient ce:	t to a Mons tificates,	goDB that /key file.	
🗌 Advanced	Options							
1 Iest						Save	Canc	el

- 4. Click Save.
- **Step 3** On the **MongoDB Connections** page, click **Connect** to connect to the single-node instance.

•				
🛃 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

Figure 6-27 Single node connection information

Step 4 If the single-node instance is successfully connected, the page shown in Figure 6-28 is displayed.

Figure 6-28 Single node connected





Unencrypted Connection

NOTICE

If you connect to an instance over an unencrypted connection, disable SSL first. Otherwise, an error is reported. For details about how to disable SSL, see **Enabling and Disabling SSL**.

Step 1 Run the installed Robo 3T. On the displayed dialog box, click **Create**.

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

Figure 6-29 Connections

- **Step 2** In the **Connection Settings** dialog box, set the parameters of the new connection.
 - 1. On the **Connection** tab, enter the name of the new connection in the **Name** text box and enter the EIP and database port that are bound to the DDS DB instance in the **Address** text box.

Figure 6-30 Connection

Connection	Authentication SSH TLS Advanced
Туре:	Direct Connection
Name:	test
Address:	: 8635
	IPv4. IPv6 or domain name.
	IPv4, IPv6 or domain name.
From URI	IPv4, IPv6 or domain name.

2. On the **Authentication** tab, set **Database** to **admin**, **User Name** to **rwuser**, and **Password** to the administrator password you set during the creation of the cluster instance.

Figure 6-31 Authentication

📃 Connection Se	ettings	×					
Connection 4	Authentication SSH TLS Advanced						
🗹 Perform auth	nentication						
Database	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>I</u> est	Save Cancel						

3. On the **TLS** tab, select **Use TLS protocol** and select **Self-signed Certificate** for **Authentication Method**.

Figure 6-32 SSL

Connection	Settings							×
Connection	Authentic	ation	SSH	TLS	Advanc	ed		
✓ Use TLS protocol								
Authentication Method:		Self-signed Certificate			\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 ho server	ing self- s trusted the comm wever the identity	-signed cer d. If self- munications ere will be 7.	tificates signed channel no	
🗌 Vse PEM C	ert./Key:	Enable requir	this o es CA-s	ption t igned c	o connect lient cer	t to a Mong tificates/	oDB that key file.	
Advanced Options								
1 Iest						Save	Cance	el

- 4. Click Save.
- **Step 3** On the **MongoDB Connections** page, click **Connect** to connect to the single-node instance.

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

Figure 6-33 Single node connection information

Step 4 If the single node instance is successfully connected, the page shown in Figure 6-34 is displayed.



le View Options Winde	ow Help	
<pre>test (3) System admin</pre>	 ♦ Welsome × ♦ db.getCollection('system''' × ≥ test = 10.154.221.78:8635 ≥ admin 	db.getCollection('system." *
Collections (4) Collections (4) Collections (4) System System.k System.k System.v System.v Collections	<pre>db.getCollection('system.roles').fin</pre>	α((∮))
	Fetched 0 record(s) in 88ms	
> Config		

----End

6.1.5 Connecting to a Single Node Instance Using Program Code

6.1.5.1 Java

If you are connecting to an instance using Java, an SSL certificate is optional, but downloading an SSL certificate and encrypting the connection will improve the security of your instance. SSL is disabled by default for newly created DB instances. You can enable SSL by referring to **Enabling or Disabling SSL**. SSL encrypts connections to databases but it increases the connection response time and CPU usage. Therefore, you are advised not to enable SSL.

Prerequisites

Familiarize yourself with:

- Computer basics
- Java code

Obtaining and Using Java

- Download the Jar driver from: https://repo1.maven.org/maven2/org/ mongodb/mongo-java-driver/3.0.4/
- To view the usage guide, visit https://mongodb.github.io/mongo-javadriver/4.2/driver/getting-started/installation/.

Using an SSL Certificate

NOTE

- Download the SSL certificate and verify the certificate before connecting to databases.
- On the Instances page, click the target DB instance name. In the DB Information area on the Basic Information page, click in the SSL field to download the root certificate or certificate bundle.
- For details about how to set up an SSL connection, see the MongoDB Java Driver official document at https://www.mongodb.com/docs/drivers/java/sync/current/ fundamentals/connection/tls/#std-label-tls-ssl.
- Java Runtime Environment (JRE) earlier than Java 8 enables TLS 1.2 only in updated versions. If TLS 1.2 is not enabled for your JRE, upgrade it to a later version to use TLS 1.2 for connection.

Connect to a single node instance using Java. The format of the Java link is as follows:

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

Parameter	Description
<username></username>	Current username.
<password></password>	Password for the current username
<instance_ip></instance_ip>	If you attempt to access the instance from an ECS, set <i>instance_ip</i> to the private IP address displayed on the Basic Information page of the instance to which you intend to connect.
	If you intend to access the instance through an EIP, set <i>instance_ip</i> to the EIP that has been bound to the instance.
<instance_port></instance_port>	Database port displayed on the Basic Information page. Default value: 8635
<database_name ></database_name 	Name of the database to be connected.

Table 6-4 Parameter description

Parameter	Description
authSource	Authentication user database. The value is admin .
ssl	Connection mode. true indicates that the SSL connection mode is used.

Use the keytool to configure the CA certificate. For details about the parameters, see **Table 6-5**.

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

Table 6-5 Parameter description

Parameter	Description
<path authority="" certificate="" file="" to=""></path>	Path for storing the SSL certificate.
<path store="" to="" trust=""></path>	Path for storing the truststore. Set this parameter as required, for example, ./ trust/certs.keystore.
<password></password>	Custom password.

Set the JVM system properties in the program to point to the correct truststore and keystore:

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

For details about the Java code, see the following example: public class Connector { public static void main(String[] args) { tru {

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>?</database_name></instance_port></instance_ip></password></username>	
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")	

}

}

Connection Without the SSL Certificate

D NOTE

You do not need to download the SSL certificate because certificate verification on the server is not required.

Connect a single node using Java. The Java link format is as follows: mongodb://<username>:<password>@<instance_ip>:<instance_port>/<database_name>? authSource=admin

Table 6-6	Parameter	description
-----------	-----------	-------------

Parameter	Description
<username></username>	Current username.
<password></password>	Password for the current username
<instance_ip></instance_ip>	If you attempt to access the instance from an ECS, set <i>instance_ip</i> to the private IP address displayed on the Basic Information page of the instance to which you intend to connect.
	If you intend to access the instance through an EIP, set <i>instance_ip</i> to the EIP that has been bound to the instance.
<instance_port></instance_port>	Database port displayed on the Basic Information page. Default value: 8635
<database_name></database_name>	Name of the database to be connected.
authSource	Authentication user database. The value is admin .

Example script in 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");

} }

}

6.1.5.2 Python

This section describes how to connect to a single node instance using Python.

Prerequisites

1. To connect an ECS to an instance, the ECS must be able to communicate with the DDS instance. You can run the following command to connect to the IP address and port of the instance server to test the network connectivity.

curl ip:port

If the message **It looks like you are trying to access MongoDB over HTTP on the native driver port** is displayed, the network connectivity is normal.

- 2. Install Python and third-party installation package **pymongo** on the ECS. Pymongo 2.8 is recommended.
- 3. If SSL is enabled, you need to download the root certificate and upload it to the ECS.

Connection Code

```
    Enabling 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
```

```
Disabling 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
```

NOTE

- The authentication database in the URL must be **admin**. That means setting **authSource** to **admin**.
- In SSL mode, you need to manually generate the trustStore file.
- The authentication database must be **admin**, and then switch to the service database.

Logging In to and Logging Out of the DDS Console

Prerequisites

You need to have an account on the cloud platform before you can use DDS

For the first time you use DDS, apply for an account at the official website. After the application is successful, your account has permissions to access the DDS service, as well as all other cloud services.

Logging In to the DDS Console

- Step 1 Open Huawei Cloud official website
- **Step 2** Click **Console** on the upper right of the page. The Huawei Cloud management console login page is displayed.
- Step 3 Enter account information as prompted and click Log In.

The login is successful.

Step 4 Click ^(Q) in the upper left corner and select a region and a project.

If you want to use computing and network resources exclusively, you need to **Enabling a DeC** and **Applying for DCC Resources**. After enabling a DeC, you can select the DeC region and project.

You will be additionally charged for using DeC.

Step 5 Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.

----End

Logging Out of the DDS Console

Step 1 On any page of the DDS console, click the username in the upper right corner.

Step 2 In the displayed dialog box, click **Log Out**.

----End
8 Example: Buying and Connecting to a DDS Instance

8.1 Connecting to a DB Instance Using Mongo Shell

This section describes how to create a DB instance, use Mongo Shell to connect to the DB instance over a private network, and read data from and write data to the DB instance.

- Step 1: Buy a DB Instance
- Step 2: Buy an ECS
- Step 3: Configure Security Group Rules
- Step 4: Connect to a DDS Cluster Instance Using Mongo Shell
- Step 5: Create a Database and Writing Data to the Database

Step 1: Buy a DB Instance

- 1. Go to the **Custom Config** page.
- 2. On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.

Basic Information					
Billing Mode	Yearly-Worthy Pageor-use				
Region					
	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 AZ4 AZ1.AZ2.AZ3				
	Deploy your DB instance in a single AZ or three AZs for high availability.				
D8 Instance Name	ddm-8591				
DB Instance Type (9)	Cituster Replice set Cloud native replice set				
	Clusters offer more robust performance than replica sets and more flexible scaling options. The high-availability and flexible scaling they provide r	make them an excellent choice for large enterprises.			
	Clusters of community edition you can still oreate: 10. Increase Quota				
Compatible MongoLis Version	5.0 4.4 4.0 3.4				
Storage Type	Utra-Nigh I/O				
Specifications	General-purpose Einhanced II				
d.d					
aas mongos					
Node Class	vCPU Memory	Maximum Connections			
	2 vCPUs 8 GB	2,000			
	4 vCPUs 18 GB	4,000			
	S VCPUN 32 GB	16,000			
	0 18 vCPUs 84 GB	18,000			
	32 vCPUs 128 GB	18,000			
	0 84 vCPUs 258 08	18,000			
	Currently selected dds.mongodb.o8.large.4.mongos 2 vCPUs 8 GB				
Nodes	- 2 + The quantity ranges from 2 to 32.				
Parameter Template	Default-DDS-4.4-Mongos V Q View Parameter Template				
Parameter Template	Defaul-003-4-4-Mongos v O Vere Parameter Temptate				
Parameter Template	Default-2005-14-Mongos v 0 Ver Planneter Template				
Parameter Template shard Node Class	Catest-0054-4-Kenges V Q View Presenter Tempton v0PU Memory	Madmun Connections			
Parameter Template shard Node Class	Octual COS4-4-Monges View Presentor Tempto vCPU Memory (a) -coPu 108 	Maximum Connections 2.000			
Paramatar Templata shard Node Class	Octual COS4 4 40mps View Presmetr Tempton vCPU (Memory 0 1x0mp 16 06 1 x0mp 15 06 1 x0mp 15 06	Maximum Convections 2.000 2.000			
Paramater Template shard Node Class	Arkust 0054 4 40mps View Presmetr Tempton vCPU (Memory 2 vCPu (a 16 6) 2 vCPu (a 16 6) 4 vCPU (a 16 6) 	Maximum Connections 2000 2000			
Parameter Template shard Noos Class	Notesh COSL4.440mps View Presmer Tempter vCPU (Memory 0 0 2x2ma (16.08) 2 x2ma (16.08) 4 x2ma (16.08) 4 x2ma (16.08) 4 x2ma (16.08) 4 x2ma (16.08)	Maximum Cammetina 2000 2000 4000 4000			
Paramèter Tampiata Shard Node Class	vCPU Memory • View Presenter Temptee • vCPU Memory • 2x4Pau 16 08 • 2x4Pau 19 08 • 4x4Pau 19 08 • 4x4Pau 19 08 • 4x4Pau 19 08 • 4x4Pau 19 08 • 4x4Pau 19 08	Maximum Connections 2000 2000 4000 4000			
Parameter Tampiate Shard Node Class	Market 0054-4.40mgms Q: Valee Presenter Tempter vCH19 (Memory @ @: 2xxReg (# 08	Maximum Connections 2,000 2,000 4,000 4,000 10,000 10,000 10,000			
Parameter Tampiala shard Noce Class	Notesh COS4-4-Kongas Q. View Research Tangton VCRU Memory Image: Cost of the Cost	Maximum Connections 2,000 2,000 4,000 4,000 1,000 1,000 1,000 1,000			
Parameter Vengela shard Nock Class	Video Cost-44-Genges Q Video Russman Trimpton VidEO J Monecry Image: Cost Cost Cost Cost Cost Cost Cost Cost	Maximum Connections 2.000 2.000 4.000 4.000 6.000 6.000 6.000			
Personan Tempida shard Nose Oss	Vite Presser Texplet vCPU 1 Memory © 2xCPU 18 08 2xCPU 18 08 2xCPU 18 08 4xCPU 18 08 4xCPU 18 08 5xCPU 18 08	Maximum Cammetinus 2000 2000 2000 4000 4000 4000 4000 4000 4000 4000 4000			
Personal Fondate	uklask 00054 4.4 kmpgs View Presmer Tempter uCPU (Memory 0 0 2.4 cPu (Memory 0 4.4 cPu (Memory 0 4.4 cPu (Memory 0 4.4 cPu (Memory)	National Convertions 2000			
Personan Pengina shared None Class	Column 2004 + 4.4mpgs Q. Vale Presenter Temples vCPU 3 Manager Image: Column 2 and Column 2 an	Maximum Connections. 2000 2000 4000 <t< th=""></t<>			
Persenter Constant	VCPU [Memory • VCPU [Memory • O Note Presenter Temples • CCPU [Memory • O Note Presenter Temples • O CCPU [Memory • O Note Presenter Temples • O CCPU [Memory • O Note Presenter Temples • O CCPU [Memory • O Note Presenter Temples • O CCPU [Memory • O Note Presenter Temples • O CCPU [Memory • O COPU [Memory • O D • O D • O D • O D • O D • O D • O D	Maximum Convections 2xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx			
Personen Fongole shared Notes Casa Biorege Roace	Columb COSL 4.4 Alerges C Vide Presenter Temples VCPU Memory © 2-0-DNa 6 08 2 -0-DNa 10 08 4 -0-DNa 10 08 4 -0-DNa 10 08 5 -0.00 100 200 200 200 400 400 000 5 -0.00 100 200 200 200 400 400 000 5 -0.00 100 200 200 200 400 400 000 5	Maximum Camerations 2000 2000 4000			
Personan Tempote shard Nose Oss Donge Socie Nose Persona Tempote	Linkuk 0024 4 4 kerges Q Mark 2024 4 4 kerges Q Mark 2024 4 kerges Q	Mathema Cameetinas 2000			
Personar Tempta	Linkusk COS4.44.4mgm CPU (Memory) 2.0cPu (16.08) 2.0cPu (16.08)	Maximum Cannottins 2000 2001 2002 2003 4.000 5.000 5.000 5.000 5.000 5.000 5.000 5.000 5.000 5.000 5.000 5.000 5.000 5.000 5.000 5.000 5.000 5.000<			
Personen Troppet	Linkenk COS4.4.40regat 	Maximum Cannotins 2000 2000 400			
Persenen Tempote shared Rose Class Burraye Soste Roses Perseneur Tempote Config Nase Class	Columb COS4.44.0002 C Mater Research Tangles • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary • CFU1 Manary	Maximum Cannottins. 2000 2000 4			
Personen Tompole shared Rose Cass Burrye Soece Notes Parameter Tompole Notes Notes	Cutud COS4 4400000 C Use # Research Tangton • CFUI [Manary • · · · · · · · · · · · · · · · · · · ·	Maximum Convestions 2000 2001 2002 4000			
Personer Tempote shard Tess Cass Bronge Base Personer Tempote Config Tess Cass Storage Base	Columb C024 4 4 breggt 	Mathema Cannotations 2000			
Personen Troppete shard Nose Osss Duringe Sosse Noses Parament Tampota config Nose Casss	Columb COS 4 4 4 Anges Columb COS 4 4 4 Anges Columb COS 4 4 4 4 Anges Columb CO	Maximum Cannottins 2000 2001 2002 2003 4000			
Personer Tempte shard Note Class Dornge Space Notes Personer Tempte Notes Dornge Space	Columb COS 4.4 Arranges Columb COS 4.4 Arranges Columb COS	Maxteura Cannetins 2000 2001 2001 4000			

Figure 8-1 Basic configurations

Figure 8-2 Administrator settings

Administrator Password Configure Skip Administrator New Password Confirm Password

Figure 8-3 Network and required duration

Network	
VPC	default_vpc View VPC
	After the DDS instance is created, the VPC cannot be changed.
Subnet	default_subnet
	Available private IP addresses in the subnet: 148
Security Group	defaulti contraction of the 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 ③
	To encrypt transmission, enable SSL.
Database Port	Default port: 8635
Enterprise Project	
Enterprise Project	Select- V Q View Project Management (2)
Pequired Duration and Quant	titu.
Required Duration and Quart	
Required Duration	1 2 3 4 5 6 7 8 9 months 1 year 🛄 2 years 🛄 3 years 🛄
	Auto-renew Fee deduction and Renewal duration
Quantity	- 1 + 🕐 You can create 10 more DB instances. Increase Quota

Figure 8-4 Advanced settings

Advanced Settings	
Show Original Log	0
Automated Backup	0
Retention Period	- 7 + Enter an integer from 1 to 732.
Time Window	00:00 - 01:00 V GMT+08:00
Maintenance Window	Skip Configure ③
Tags	Predefined tags are recommended for adding the same tag to different cloud resources. Create Predefined Tag C View predefined tags
	Tag key Tag value
	You can add 20 more tags.

- 3. On the displayed page, confirm the instance details.
 - For yearly/monthly instances
 - If you need to modify the settings, click **Previous**.
 - If you do not need to modify the settings, read and agree to the service agreement and click **Pay Now** to go to the payment page and complete the payment.
 - For pay-per-use instances
 - If you need to modify the settings, click **Previous**.
 - If you do not need to modify the settings, read and agree to the service agreement and click **Submit** to start creating the instance.
- 4. Click **Back to Instance List**. Click **Back to Instance List**. You can view and manage the DB instance on the **Instances** page.

- When a DB 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.

Step 2: Buy an ECS

- 1. Go to the **Buy ECS** page.
- 2. Configure basic settings and click **Next: Configure Network**. Keep the region and AZ of the ECS the same as those of the DDS instance to be connected.

Figure 8-5 Basic configurations

 Configure Basic Setti 	ings — (2) Configure Network — (3	 Configure Advanced Settings — (4) Confirm				
Billing Mode	Yearly/Monthly Pay-per-use	Spot price (2)					
Region	CN-Hong Kong *						
	For low network latency and quick resource access, set	lect the region nearest to your target users. Le	am how to select a region.				
AZ	Random AZ1	A22 (?)					
CBLArchitecture	VIII KUIDAAA						
CPO Architecture	Kunpeng (r)						
Specifications	Latest generation vCPUs All	✓ Memory	All 👻 Flav	or Name Q			
	General computing-plus General computing	Memory-optimized High-perform	nance computing Ultra-high I/O	GPU-accelerated ⑦			
	Flavor Name	vCPUs Memory(GiB) ↓Ξ	CPU 1Ξ	Assured / Maximum Bandwidth ⑦ ↓Ξ	Packets Per Second (PP5) ⑦ ↓Ξ	IPv6	
	Flavor Name o c6.large.2	vCPUs Memory(GiB) ↓Ξ 2 vCPUs 4 GIB	CPU JE Intel Cascade Lake 3.0GHz	Assured / Maximum Bandwidth ⑦ ↓≡ 1.2 / 4 Gbit/s	Packets Per Second (PP5) ⑦ J≡ 400,000	IPv6 Yes	
	Flavor Name © c6.large.2 c6.large.4	vCPUs Memory(GiB) ↓Ξ 2 vCPUs 4 GIB 2 vCPUs 8 GIB	CPU JE Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz	Assured / Maximum Bandwidth ⑦ ↓Ξ 1.2 / 4 Gbit/s 1.2 / 4 Gbit/s	Packets Per Second (PP5) ⑦ 4Ξ 400,000 400,000	IPv6 Yes	
	Flavor Name c6large.2 c6large.4 c6xlarge.2 	vCPUs Memory(GIB) ↓Ξ 2 vCPUs 4 GIB 2 vCPUs 8 GIB 4 vCPUs 8 GIB	CPU JE Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz	Assured / Maximum Bandwidth ⑦ J田 12 / 4 Gbit/s 12 / 4 Gbit/s 2.4 / 8 Gbit/s	Packets Per Second (PPS) ① 4 400,000 400,000 800,000	IPv6 Yes Yes	
	Flavor Name @ c5.large.2 c6.large.4 c6.starge.2 c6.starge.2 c6.starge.2	vCPUs Memory(GiB) 4E 2 vCPUs 4 GiB 2 vCPUs 8 GiB 2 vCPUs 8 GiB 4 vCPUs 8 GiB 4 vCPUs 16 GiB 4 vCPUs 16 GiB	CPU 4E Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz Intel Cascade Lake 3.0GHz	Assured / Maximum Bandwidth ⑦ ↓ ↓ 12/4 6.0h/s 12/4 6.0h/s 24/8 6.0h/s 24/8 6.0h/s	Packets Per Second (PPS) ① JE 400,000 400,000 800,000 800,000 800,000	IPv6 Yes Yes Yes	_
	Risor Name Image: Charge 2 charge 4 charge 2	vCPUs Memory(GB). ↓Ξ 2 vCPUs 4 GB 2 vCPUs 4 GB 2 vCPUs 8 GB 4 vCPUs 8 GB 4 vCPUs 16 GB 8 vCPUs 16 GB	CPU 4 Intel Cascade Lake 30GHz Intel Cascade Lake 30GHz Intel Cascade Lake 30GHz Intel Cascade Lake 30GHz Intel Cascade Lake 30GHz	Assured / Maximum Bandwidth ① JE 12/4 Gb/js 12/4 Gb/js 24/8 Gb/js 24/8 Gb/js 45/15 Gb/js	Packets Per Second (PPS) ① 上目 400,000 400,000 800,000 800,000 1,500,000	IING Yes Yes Yes Yes	
	Flavor Name	vCPUs Memory(G8) 4E 2 vCPUs 4 G8 2 vCPUs 8 G8 4 vCPUs 8 G8 4 vCPUs 16 G8 8 vCPUs 16 G8 8 vCPUs 16 G8 8 vCPUs 25 G8	CPU JE Intel Cascade Lake 30GHz	Assured / Macimum Bandwidth (1) 12 12 / 4 Gbb/s 12 / 4 Gbb/s 24 / 8 Gbb/s 24 / 8 Gbb/s 45 / 15 Gbb/s 45 / 15 Gbb/s 45 / 15 Gbb/s	Packets Per Second (PPS) ① JE 400,000 400,000 800,000 1,500,000 1,500,000	IPv6 Yes Yes Yes Yes Yes	
	Flavor Name @ c6.large.2 c6.large.4 c6.slarge.4 c6.slarge.4 c6.slarge.4 c6.slarge.4 c6.slarge.4 c6.slarge.4 c6.slarge.4 c6.slarge.4 c6.slarge.4	vCPUs MemoryGBB JE 2 vCPUs 4 GB 2 vCPUs 4 GB 4 vCPUs 8 GB 4 vCPUs 8 GB 4 vCPUs 16 GB 8 vCPUs 16 GB 8 vCPUs 16 GB 1 vCPUs 12 GB 1 vCPUs 12 GB	CPU JB Intel Cascade Lake 30GHz Intel Cascade Lake 30GHz	Assured / Mastrum Bandweldth ① 4년 12/4 GBUs 12/4 GBUs 24/8 GBUs 24/8 GBUs 24/8 GBUs 45/15 GBUs 45/15 GBUs 7/17 GBUs	Padets Per Second (PPD) ① E 400,000 400,000 800,000 1,550,000 1,500,000 2,000,000	INVE Ves Ves Ves Ves Ves	4 4
	Rearr Name et clarge 2 et clarge 4 et clarge 4 et clarge 4 et clarge 4 et clarge 4 et clarge 2 et clarge 2 et clarge 2 et clarge 2 et clarge 2 et clarge 2 et clarge 2 et clarge 2 et clarge 2 et clarge 2	vCPUs MemoryGB3 JE 2 vCPUs 4 GB 2 vCPUs 6 GB 4 vCPUs 16 GB 8 vCPUs 16 GB 8 vCPUs 16 GB 12 vCPUs 24 GB	CPU JE Intel Cascole Lake 200Hz Intel Cascole Lake 200Hz	Assend / Machine Bundwidth ① 4년 12/4 GBA5 12/4 GBA5 24/8 GBA5 24/8 GBA5 45/15 GBA5 7/17 GBA5	Padeta Per Second (PPG) ① E 400,000 400,000 100,000 1,000,000 1,000,000 2,000,000	ind Vis Vis Vis Vis Vis Vis	E < <
	Flavor Name	vcPub MemoryGBB # 2 vcPub 4 GB 2 vcPub 8 GB 4 vcPub 8 GB 4 vcPub 16 GB 8 vcPub 16 GB 8 vcPub 2 GB 12 vcPub 24 GB	CPU JE Intel Cascade Lake 2004z Intel Cascade Lake 2004z	Assend / Maximum Bandweldh ① 4년 12/4 GBA 12/4 GBA 24/8 GBA 24/8 GBA 43/15 GBA 43/15 GBA 7/17 GBA	Paders Per Second (PPS) (D) # 400,000 400,000 600,000 1,540,000 1,540,000 2,000,000	PM Yes	E 4 0

Figure 8-6 Selecting an image

Image	Public image Private image Strared image Marketplace image
	♦ CentOS ▼ CentOS & 2 6401(4006) ▼ C
Host Security	Enable 🕥
System Disk	High I/O + 08 IOPS limit 2,120, IOPS limit 2,120
	🕑 Add Dela Dilk. You can attach 23 more dials.
	Data daka addet to a Linux ECS can be initialized using a wizard script.
antity — 1	+ ECS Price (7) Net: Configure N

3. Configure the ECS network information and click **Next: Configure Advanced Settings**. Keep the VPC and security group of the ECS the same as those of the DDS instance to be connected.

Figure 8-7 Network settings

< Elastic Cloud Ser	rver						Assured Purch	hase 🎯 Flexi Purchase
(1) Configure Basic Settings -	Configure Network	- (3) Configure Advanced 5	Settings — ④ Con	firm				
Network	vpc-lest01(192,168.8.016) • C submet/set01(192,168.8.016) • Available private IP addresses: 200 Cmatter VPC							
Extension NIC	Add NIC NICs you can still add: 1							
Security Group	Security Group endang (1865):25-162-642-662-662-662-662-662-662-662-662-6							
	Security Group Name	Priority	Action	Protocol & Port (?)	Туре	Source 🕥	Description	
		1	Permit	TCP: 8000	IPv4	0.0.0.0/0	-	
		1	Permit	TCP: 8635	IPv4	0.0.0.0/0	**	
		1	Permit	TCP: 8080	IPv4	0.0.0.0/0		
		1	Permit	UDP: 111	IPv4	0.0.0.0/0	Create by sfs turbo	
		1	Permit	TCP: 111	IPv4	0.0.0.0/0	Create by sfs turbo	

Figure 8-8 Selecting an EIP

Auto assign Use existing Not required	
Dynamic BGP Static BGP	
Bandwidth 🔞 🔽 Traffic 🖓 Traffic Shared bandwidth For heavy/stable traffic	
Billed based on total traffic irrespective of usage duration; configurable maximum bandwidth size.	
5 10 20 50 100 Custom - 1 + The bandwidth can be from 1 to 30	00 Mbit/s.
Release with ECS 📀	
	 Auto assign Use existing Not required ? Dynamic BGP Static BGP Greater than or equal to 99 95% service availability rate Bandwidth For heavy/stable traffic For heavy/stable traffic Binded based on total traffic irrespective of usage duration; configurable maximum bandwidth size. 5 10 20 50 100 Custom 1 + The bandwidth can be from 1 to 3 Free Anti-DDoS protection Release with ECS ?

4. Configure the ECS password and click **Next: Confirm**.

Figure 8-9 Advanced settings

Configure Basic Settings -	Configure Network 3 Configure Advanced Settings 4 Confirm
ECS Name	ecs-aba9 Allow duplicate name If you are creating multiple ECSs at the same time, automatic naming and customizable naming are available for you to 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 vault. A vault is a container that stores backups for servers. Create new Use existing Not required ??
Cloud Eye	Enable Detailed Monitoring From ⑦ O Enable 1-minute fined-grained monitoring of ECS metrics, such as CPU, memory, network, disk, and process.
ECS Group (Optional)	Anti-affinity
	-Select ECS group-
	Create ECS Group

5. Confirm the configurations and click **Submit**.

Figure 8-10 Confirming the configurations

Configuration	Basic 🖉							
	Billing Mode	Pay-per-use	Region	Hong Kong	AZ	AZ2		
	System Disk	General computing-plus collarge.2 2 vCPUs 4 GIB High I/O, 40 GIB	Image	CentOS 7.6 640it	Host Security	Disabled		
	Network 🖉							
	VPC	default_vpc (192.168.0.0/16)	Security Group	default	Primary NIC	default_subnet (192.168.0.0/24)		
		cyname our i conc oy, name i oanoweer, rinneys						
	Advanced 🖉							
	ECS Name	ecs-e5d6-test	Login Mode	Password	ECS Group			
Launch Template	Save as Launch	Template						
Enterprise Project	default	C Create Enterprise Project	0					
Quantity	- 1 +	You can create a maximum of 20 ECSs. Learn how to increase quot						9
Agreement	I have read and	agree to the Service Level Agreement and Image Disclaimer.						0
ECS Price	/hour + EIP Traffic Pric	e /G8					Previous Sub	mit

6. View the purchased ECS.

Step 3: Configure Security Group Rules

Step 1 Log in to the management console.

- **Step 2** Click ¹ in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the instance name. The **Basic Information** page is displayed.
- **Step 5** In the **Network Information** area on the **Basic Information** page, click the security group.

 Network Information

 VPC
 dds-st-test-wpc

 Security Group
 Sys-default **2**

 Database Port
 a635 **2**

You can also choose **Connections** in the navigation pane on the left. On the **Private Connection** tab, in the **Security Group** area, click the security group name.

Figure 8-12 Security Group

Figure 8-11 Security Group

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

- **Step 6** On the **Security Group** page, locate the target security group and click **Manage Rule** in the **Operation** column.
- **Step 7** On the **Inbound Rules** tab, click **Add Rule**. The **Add Inbound Rule** dialog box is displayed.
- **Step 8** Add a security group rule as prompted.

Figure 8-13 Add Inbound Rule

Add Inbound Rule Learn more about security group configuration.					
1 Inbound rules allow incoming traffic to i	instances associated with the s	ecurity group.			
Security Group Sys-default You can import multiple rules in a batch.					
Protocol & Port ?	Туре	Source 🕐	Description	Operation	
TCP Example: 22 or 22-30	IPv4 💌	IP address •		Operation 👻	
	⊕ Ad	d Rule			
	1	OK Cancel			

 Table 8-1 Inbound rule settings

Paramete r	Description	Example Value
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default priority is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	The security group rule actions. Deny rules take precedence over allow rules of the same priority.	Allow
Protocol & Port	The network protocol required for access. Available options: TCP , UDP , ICMP , or GRE	ТСР
	Port: the port on which you wish to allow access to DDS. The default port is 8635. The port ranges from 2100 to 9500 or can be 27017, 27018, or 27019.	8635
Туре	IP address type. Only IPv4 and IPv6 are supported.	IPv4

Paramete r	Description	Example Value
Source	Specifies the supported IP address, security group, and IP address group, which allow access from IP addresses or instances in other security groups. Example: • Single IP address: 192.168.10.10/32	0.0.0/0
	 IP address segment: 192.168.1.0/24 All IP addresses: 0.0.0.0/0 	
	 Security group: sg-abc 	
	• IP address group: ipGroup-test If you enter a security group, all ECSs associated with the security group comply with the created rule.	
	For more information about IP address groups, see IP Address Group Overview.	
Descriptio n	(Optional) Provides supplementary information about the security group rule.	-
	The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	

Step 9 Click OK.

----End

Step 4: Connect to a DDS Cluster Instance Using Mongo Shell

- SSL Connection
- Step 1 Log in to the management console.
- **Step 2** Click ^(Q) in the upper left corner and select a region and a project.
- **Step 3** Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- **Step 4** On the **Instances** page, click the instance name.
- **Step 5** In the navigation pane on the left, choose **Connections**.
- **Step 6** In the **Basic Information** area, click $\stackrel{\perp}{
 m mathbf{lem:ssl}}$ next to the **SSL** field.
- **Step 7** Upload the root certificate to the ECS to be connected to the instance.

The following describes how to upload the certificate to a Linux and Windows ECS:

• In Linux, run the following command:

scp

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

NOTE

- **IDENTITY_FILE** is the directory where the root certificate resides. The file access permission is 600.
- **REMOTE_USER** is the ECS OS user.
- **REMOTE_ADDRESS** is the ECS address.
- **REMOTE_DIR** is the directory of the ECS to which the root certificate is uploaded.
- In Windows, upload the root certificate using a remote connection tool.
- **Step 8** Connect to the instance in the directory where the MongoDB client is located.

Method 1: Using the private HA connection address (recommended)

DDS provides a private HA connection address that consists of IP addresses and ports of all dds mongos nodes in a cluster instance. You can use this address to connect to the cluster instance to improve availability of the cluster instance.

Command:

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

Parameter description:

• **Private HA Connection Address**: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 8-14 Obtaining the private HA connection address

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

The format of the private HA connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

The following table lists the required parameters in the private HA address.

Parameter	Description	
rwuser	Database username	
<password></password>	Password for the database username. Replace it with the actual password.	
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively.	
	For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25*** %21%24 .	
192.168.***.***:8635,192. 168.***.***:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.	
test	The name of the test database. You can set this parameter based on your service requirements.	
authSource=admin	The authentication database of user rwuser must be admin . authSource=admin is fixed in the command.	

Table 8-2 Parameter information

- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and bandwidth, the cluster certificate is generated using the internal management IP address. --sslAllowInvalidHostnames is needed for the SSL connection through a private network.

Command example:

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

Method 2: Using the private HA connection address (user-defined database and account)

Command:

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

Parameter description:

• **Private HA Connection Address**: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 8-15 Obtaining the private HA connection address

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>		/test?authSource=admin&replicaSet=replica 🗗 Learn more

The format of the obtained private HA connection address is as follows:

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

The following table lists the required parameters in the private HA address.

Parameter	Description
rwuser	Database username. The default value is rwuser . You can change the value to the username based on your service requirements.
<password></password>	Password for the database username. Replace it with the actual password.
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively.
	For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25*** %21%24 .
192.168.***.***:8635,192. 168.***.***:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user rwuser is admin . NOTE If you use a user-defined database for authentication, change the authentication database in the HA connection address to the name of the user-defined database. In addition, replace rwuser with the username created in the user-defined database.

Table 8-3 Parameter information

- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and bandwidth, the cluster certificate is generated using the internal management IP address. --sslAllowInvalidHostnames is needed for the SSL connection through a private network.

For example, if you create a user-defined database **Database** and user **test1** in the database, the connection command is as follows:

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

Method 3: Using a private IP address

Command:

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

Parameter description:

 DB_HOST is the IP address of the dds mongos node of the cluster instance to be connected.

Click the instance name. On the **Basic Information** page, choose **Connections** > **Private Connection**, obtain the private IP address of the dds mongos node on the **dds mongos** tab in the **Node Information** area.



Basic Informa	ition					
Database Port	8635	o O		VPC	dds-st-test-vpc	
SSL	0	±		Subnet	dds-st-test-subnet	
Address						
Private HA Conne	ection Address (Compatible with MongoDB	mongodb://rwuser: <pass< th=""><th>sword>@10211001000000</th><th>Learn more</th><th></th></pass<>	sword>@10211001000000	Learn more	
			Note The parameters	s in orange are variables and r	need to be modified based on service requirements. For details,	click Lea
Node Informat	tion shard	config				
Name/ID	AZ	Private IP Address	EIP	Operation		
dds-5c63 72656654	az2	19:2000000000000000000000000000000000000	Outpound	Change Private IP Address	Bind EIP	
dds-5c63 6f493319e	az2	192888888888	S Unbound	Change Private IP Address	Bind EIP	

• **DB_PORT** is the port of the instance to be connected. The default port is 8635.

Click the instance name. On the **Basic Information** page, choose **Connections**. On the **Private Connection** tab, obtain the database port information in the **Database Port** field in the **Basic Information** area.

Figure 8-17 Obtaining the port

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

- **DB_USER** is the database user. The default value is **rwuser**.
- **FILE_PATH** is the path for storing the root certificate.
- --sslAllowInvalidHostnames: To ensure that the internal communication of the cluster does not occupy resources such as the user IP address and bandwidth, the cluster certificate is generated using the internal management IP address. --sslAllowInvalidHostnames is needed for the SSL connection through a private network.

Enter the password of the database account if the following information is prompted:

Enter password:

Command example:

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

Step 9 Check the connection result. If the following information is displayed, the connection is successful. mongos>

----End

- Unencrypted Connection
- **Step 1** Connect to the ECS.
- **Step 2** Connect to the instance in the directory where the MongoDB client is located.

Method 1: Using the private HA connection address (recommended)

Command:

./mongo " <Private HA Connection Address>"

Private HA Connection Address: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 8-18 Obtaining the private HA connection address

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>		/test?authSource=admin&replicaSet=replica 🗗 Learn more

The format of the private HA connection address is as follows. The database username **rwuser** and authentication database **admin** cannot be changed.

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

The following table lists the required parameters in the private HA address.

Parameter	Description
rwuser	Database username.
<password></password>	Password for the database username. Replace it with the actual password. If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively. For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25***%21%24.
192.168.xx.xx:8635,192.1 68.xx.xx:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.
authSource=admin	The authentication database of user rwuser must be admin . authSource=admin is fixed in the command.

Table 8-4 Parameter information

Command example:

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

Method 2: Using the private HA connection address (user-defined database and account)

Command:

./mongo "<Private HA Connection Address>"

Private HA Connection Address: On the **Instances** page, click the instance name. The **Basic Information** page is displayed. Choose **Connections**. Click the **Private Connection** tab and obtain the connection address of the current instance from the **Private HA Connection Address** field.

Figure 8-19 Obtaining the private HA connection address

vate Connection	Public Connection		
Basic Information			
Database Port	8635 🖉	VPC	dds-st-test-vpc
SSL	J ₹	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

The format of the obtained private HA connection address is as follows:

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

The following table lists the required parameters in the private HA address.

Parameter	Description
rwuser	Database username. The default value is rwuser . You can change the value to the username based on your service requirements.
<password></password>	Password for the database username. Replace it with the actual password.
	If the password contains at signs (@), exclamation marks (!), dollar signs (\$), or percent signs (%), replace them with hexadecimal URL codes (ASCII) %40, %21, %24, and %25 respectively.
	For example, if the password is ****@%***!\$, the corresponding URL code is ****%40%25***%21%24 .
192.168.xx.xx:8635,192.1 68.xx.xx:8635	IP addresses and ports of the dds mongos nodes of the cluster instance to be connected.
test	The name of the test database. You can set this parameter based on your service requirements.

Table 8-5 Parameter information

Parameter	Description
authSource=admin	The authentication database of user rwuser is admin .
	NOTE If you use a user-defined database for authentication, change the authentication database in the HA connection address to the name of the user-defined database. In addition, replace rwuser with the username created in the user-defined database.

For example, if you create a user-defined database Database and user test1 in the database, the connection command is as follows:

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

Method 3: Using a private IP address

Command:

```
./mongo --host <DB HOST> --port <DB PORT> -u <DB USER> -p --
authenticationDatabase admin
```

Parameter description:

DB_HOST is the IP address of the dds mongos node of the cluster instance to be connected.

Click the instance name. On the **Basic Information** page, choose **Connections** > **Private Connection**, obtain the private IP address of the dds mongos node on the **dds mongos** tab in the **Node Information** area.

Private Connection	Public Connection								
Basic Information									
Database Port	8635 🖉		VPO	C	dds-st-test-vpc				
SSL	▲		Sub	onet	dds-st-test-subnet (192.168.0.0/16)				
Address									
Private HA Connection	n Address Compatible wi	th MongoDB mongodb	://rwuser: <mark><password< mark="">>@</password<></mark>		i635/test?authSource=admin 🗗 Learn more				
	Note The parameters in orange are variables and need to be modified based on service requirements. For details, clic								
		k Learn m	iore.						
Node Information									
dds mongos	shard config								
Q Select one or	more filters from the pop	up lists. If you enter a ke	word without a filter ap	plied, the systen	n will search for all names matching this keyword.	-			
Name/ID	AZ	Private IP Address	Private Domain	EIP	Operation				
dds-log-1 54008dcc	az1	192.	54008dcc1b0f4a	🕲 Unbo	Change Private IP Address More 💌				
dds-log-1 8b1e902	az1	192.1	8b1e902ad7f347f	O Unbo	Change Private IP Address More 👻				

Figure 8-20 Obtaining the private IP address

• **DB_PORT** is the port of the instance to be connected. The default port is 8635.

Click the instance name. On the **Basic Information** page, choose **Connections**. On the **Private Connection** tab, obtain the database port information in the **Database Port** field in the **Basic Information** area.

Figure 8-21 Obtaining the port

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

• **DB_USER** is the database user. The default value is **rwuser**.

Enter the password of the database account if the following information is prompted: Enter password:

Command example:

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

Step 3 Check the connection result. If the following information is displayed, the connection is successful. mongos>

----End

Step 5: Create a Database and Writing Data to the Database

Step 1 Create a database.

use dbname

dbname: indicates the name of the database to be created.

Figure 8-22 Creating a database



Step 2 After a database is created, insert data into the database so that you can view the database in the database list.

Figure 8-23 Inserting data

replica:	PRIMARY>	db.user.i	nsert({	"key1":"	value1"}	-)
WriteRes	ult({ "nI	nserted"	: 1 })			
replica:	PRIMARY>	show dbs				
admin	0.000GB					
local	0.004GB					
test	0.000GB					
test001	0.000GB					
replica:	PRIMARY>					

There are three system databases created by default: **admin**, **local**, and **test**. If you directly insert data without creating a database, the data is inserted to the **test** database by default.

Figure 8-24 Viewing the database

replic	a:PRIMARY>	show	dbs	
admin	0.000GB			
local	0.004GB			
test	0.000GB			

Step 3 View data in the database.





----End

8.2 Connecting to a DDS Instance Through an EIP

This section uses a DDS replica set instance and Windows operating system as an example to describe how to buy a DDS instance, bind an EIP, set a security group, and connect to the DDS instance using the Robo 3T tool in your local environment. The procedures are as follows:

- Step 1: Buy a DB Instance
- Step 2: Bind an EIP
- Step 3: Configure a Security Group
- Step 4: Connect to a DDS Instance

Step 1: Buy a DB Instance

- 1. Go to the **Custom Config** page.
- 2. On the displayed page, select a billing mode and configure information about your DB instance. Then, click **Next**.

Figure 8-26 Basic configurations



Figure 8-27 Administrator settings

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

Figure 8-28 Network, Required Duration, and Quantity

Network	
VPC	default_vpc 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 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 ③
	▲ To encrypt transmission, enable SSL.
Database Port	Default port: 8635
Cross-CIDR Access	Configure Skip Only configure creek CIDP secore if the CIDP block is 100 168 0.01
	the replica set instance.
Enterprise Project	
Enterprise Project	Select View Project Management (2)
Required Duration and Quantity	y Contraction of the second
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

Figure 8-29 Advanced settings

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 73	12.
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	to add the same tags to different cloud resources. C $\;$ View predefined tags
	Tag key Tag value	
	You can add 20 more tags.	

- 3. On the displayed page, confirm the instance details.
 - For yearly/monthly instances
 - 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.
 - For pay-per-use instances
 - 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.
- 4. Click **Back to Instance List**. 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.

Step 2: Bind an EIP

- 1. Log in to the management console.
- 2. Click 💿 in the upper left corner and select a region and a project.
- 3. Click in the upper left corner of the page and choose **Databases** > **Document Database Service**.
- 4. On the **Instances** page, click the instance. The **Basic Information** page is displayed.
- 5. In the **Node Information** area, locate the row that contains the primary node and click **Bind EIP**.
- 6. In the displayed dialog box, select the purchased EIP and click **OK**.
- 7. After the binding is successful, view the EIP in the **Node Information** area.

Step 3: Configure a Security Group

- 1. In the **Network Information** area on the **Basic Information** page, check the database port of the DB instance.
- 2. In the **Network Information** area, click the security group name.
- 3. On the **Security Groups** page, click the security group name.
- 4. Click the **Inbound Rules** tab and click **Add Rule**. In the displayed dialog box, add an inbound rule for the database port.

Step 4: Connect to a DDS Instance

1. Access the Robo 3T download address https://robomongo.org/download and click Download Studio 3T Free Today.

Figure 8-30 Downloading page



2. In the displayed dialog box, enter required information and click **Download Studio 3T for Windows** to download **studio-3t-x64.zip**.



- 3. Decompress the downloaded package and double-click the **studio-3t-x64.exe** file in the decompressed directory to start the installation.
- 4. After the installation is complete, start the tool, as shown in **Figure 8-32**.

Figure 8-32 Main window

Studio 3T for MongoDB - Full product trial File Edit Database Collection Index Document	GridFS View	Help										_	×
Connect Collection IntelliShell SQL A	igregate Map-	Reduce Compare	C. Schema	Reschema	Tasks	Export	Import	(kaka) Data Masking	SQL Migration	- 💄	s Roles) Feedback	
Search Open Connections (Ctrl+P) ad	< Quickstard	r Connection Manage New Connection N Citck here to filter corr Name	er ww.Group mections DB Ser	Edit	Delete C	lone	Import	Export To	्रि ।।दा Shortcut	X Al marte	r. Get a ate commor	n tasks.	^
Operations 2	. ^	Show on startup Quick Optic Theme (requires n Ø show What's Jautomatically Enable Sessio	DITS estart): Sam New tab afte r open Conne n Restore	e as system * er updating S ection Mana <u>c</u>	✓ itudio 3T ger at startup			Connect Help Get G Knc G Free G Joir P Stu	Close and Learnin ting started wiedge base e MongoDB course the 3T communit dio 3T features dio 3T fips and tric	g s ks			~

5. On the **Connection Manager** page, click **New Connection**.

Figure 8-33 Connection manager

<	Quickstart										
•	Quickstart	Connection M New Connection Click here to filte Name	Anager New Group r connections	Edit	Delete	<u>C</u> lone	Import	Export	L N To URI	0 matches	a l marter. Get a
			If you have a co can paste it here Paste your co URI: Manually com	nnection stri e and Studio onnection str	ng (<u>SRV</u> 3T will a ing (SRV	or standard uuto-configur or standard), e.g. for <u>yo</u> r re your conn) here:	<u>ur Mongol</u>	<u>DB Atlas</u> de ings for you	ployment, you u.	automate common tasks.
		Show on start							Next	Cancel	
		Quick O Theme (requ Show W	ptions iires restart): Sam /hat's New tab afte	e as system ' er updating S	✓ itudio 3T				Getting st Knowledg Free Mon Join the 3	arted ge base goDB courses T community	-
^		Automa	tically open Conne Seccion Restore	ection Mana	ger at sta	rtup		d	Studio 3T	tips and tricks	
			Jession nestore					-			

- 6. Connect to a DB instance **automatically** or **manually**.
 - Method 1: Connect to a DB instance automatically.
 - i. In the dialog box that is displayed, enter the URI, replace <password>, and click Next.

NOTE

How to obtain the URI:

On the **Instances** page, click the target DB instance name. On the **Basic Information** page, click **Connections**. In the **Public Connection** area, obtain the public connection address from **Address**.

Figure 8-34 Entering the URI

File Edit Database Co	ellection Index	Document GridFS	View Help											
Connect Collection	n IntelliShell	SQL Aggregate	Map-Reduce	[=] <u>≡</u> Compare	C) Schema	Reschema	Tasks	Export	Import	Data Masking	SQL Migration	2 Users	Roles	(==) Feedback
Search Open Connection () () () () () () () () () () () () ()	(Ctrl+F) [direct]	aA (c	In New Co If you has @ Poste y URI: [O Manua	e a connection it here and St our connectio mongodbi//rw Ily configure n	n string (SI udio 3T wi n string (SI user: <pas ny connecti ny connecti</pas 	+ C C+ W or standard a usto-configu W or standard word>@10.15 on settings B. dustar in the), e.g. for <u>y</u> re your con) here: 4.218.10:86	OT our Mong nection se	DB Atlas ttings for tthSource= Next	deployment, you ou.	ature that helps y Task Manager e a new task	al ou automat	e common 1	tasks.
Operations		2 ^	Q Th	uick Optic me (requires r Show What's Automaticall Enable Sessio	DITS estart): Sa New tab a y open Cor on Restore	me as system fter updating S inection Manag	v itudio 3T ger at startu	ip		Help Get E Kno Fre Join Join Stu Stu Stu	and Learning ting started weledge base e MongoDB courses in the 3T community dio 3T features dio 3T tips and tricks dio 3T Power User ma sure times	inual: hidder	n gems that	will

ii. On the Server tab, click OK in the displayed dialog box.

Figure 8-35 Server

onnect Collection IntelliShell SQL Aggregate	Connection name: Connection group: <pre>croot level></pre>	Migration Users Roles Feedback
arch Open Connections (ChrisP) MA (The Treplica) [direct] > Admin > bdmin > bbb > cccc > cccc > cccal > bt ext1 > text2001	Server Autoentication SSL SSH Proy IntelliShell Mongc08 Tools Advanced	JCt trial e that helps you automate common tasks. k 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	nted base oD8 courses community eatures

iii. Click the Authentication tab.

Figure 8-36 Authentication

Studio 3T for MongoDB - Full product 1	nial Decument GridES	C New Connection	× – –	×
Connect Collection IntelliShell	SQL Aggregate	Connection name: Connection group: <root level=""></root>	Migration Users Roles Feedback	
Search Open Connections (Ctrl+F)	aA < Qu	Server Authentication SSL SSH Proxy IntelliShell MongoDB Tools Adv	inced	
 ➤ E (ceplica set: replica) (direct) > E admin > E bbb > E config > E local > E local 		Authentication Mode: legacy (SCRAM-SHA-1) Yoo have chosen an authentication method which might mails your Mongold instance Reserver's the <u>Mongold Sourch</u> Checklin to help secure your databamo). User name: revuer Password:	Ict trial	^
> E test001		Authentication DB: admin The database where the user is defined	re that helps you automate common tasks.	l
		D⊋	k Manager	l
			new task	l
		Always show the authentication database of the user account Newsy show all databases and collections defined in roles of the user account (Manusk) it calcional vibile databases by their names ① Databases: admin.test Databases vibile for non-admin users (comma-separated)	e Learning ted base ob cornes communty satures te and tricks	
Operations	2 ^	Test Connection S	ve Cancel ower User manual: hidden gems that will	~
安全组	dds-st-test-secu	ty-group 🖉	NR425C (Critering on Alternation of the Criteria State	

iv. Click Test Connection to check whether the connection is successful.

Figure 8-37 Test Connection

onnect Collection IntelliShell SQL Aggre	gate	Connection Connection	rame: group: <root level=""> athentication SSL SSH Proxy IntelliShell MonooDB To</root>	ols Advanced	~	B			
(in [replica set replica] [direct] > ⊜ asa > ⊜ admin > ⊜ bbb > ⊜ cc	Que	Authentie You have Please res	Connecting Testing connection	Termen	× v	uct trial			
> © config > ≥ local > ⊜ test > ⊜ test		User nar Passwon Authentic	Uperation Initializing connection Connecting as rower Reading server status from connection Detecting accessible databases Detecting MongoDB server version Detecting MongoDB server feature compatibility version Connected] ♦ 🕚	re that helps you automate common tasks. k Manager new task				
		☑ Alway ☑ Alway ☑ Manua Database	Tilde details OK y vervensenser vervenser er v	Cancel		Learning ned base of course comunity extures so and trids			

v. Click the SSL tab and select Use SSL protocol to connect.

If SSL data encryption is disabled, skip this step and go to 6.viii.

Figure 8-38 SSL

onnection group:	<root< th=""><th>level</th><th>></th><th></th><th></th><th></th><th></th><th></th><th>~</th></root<>	level	>						~
erver Authentic	ation	SSL	SSH	Proxy	IntelliShell	MongoDB Tools	Advanced		
<mark>⊡</mark> se SSL proto	col to c	onne	ct						
⊖Use own <u>R</u> oot	CA file	(ss	CAFile	e)					
O Accept server	SSL cer	tificat	es trus	sted by	the <u>o</u> peratin	g system			
Accept any ser	ver SSI	_ certi	ficates						
Use Client Cert	tificate	(ss	IPEMK	eyFile)					
Client Certificate:								Ē	
Passphrase:								۲	
✓ My client certif	icate is	not	protect	ted by a	a passphrase				
Select SSL/TLS:	TLS							~ 1	
Allow invalid h	ostnam	nes (sslAllo	wInvali	dHostnames) 🚺			
Use Server Na	me Ind	icatio	n (Adv	anced)	6				
SNI Host Name:					-				

vi. Select **Use own Root CA file (--sslCAFile)**, import the certificate, and select **Allow invalid hostnames**.

Download the SSL certificate and verify the certificate before connecting to databases.

On the **Instances** page, click the target DB instance name. In the **DB Information** area on the **Basic Information** page, click $\stackrel{l}{\checkmark}$ in the **SSL** field to download the root certificate or certificate bundle.

Figure	8-39	Entering	SSL	information

onnection group	<pre>c <root <="" lev="" pre=""></root></pre>	el≻					~
erver Authenti	cation SS	SSH	Proxy	IntelliShell	MongoDB Tools	Advanced	
Use SSL prot	ocol to con	nect					1
Use own Roc	t CA file (-	sslCAFil	e)				
C:\Users\)/C	ownload	ds ca.crt	1			<u>a</u> (
Accept server	r SSL certifi	ates tru	isted by	the operatin	g system		
Accept any set	erver SSL ce	rtificate	s				
Use Client Ce	rtificate (ssiPEMK	(eyFile)				
Client Certificate	:						a
Passphrase:							
My client cert	ificate is no	t protec	ted by a	a passphrase			
Select SSL/TLS:	TLS						0
			1990 - 20				
Allow invalid	hostnames	(sslAlle	owInvali	dHostnames) 🚺		
Use Server N	ame Indica	ion (Ad	vanced)				
SNI Host Name				·			
Sivi Host Ivallie.							

vii. Click Test Connection to check whether the connection is successful.

onnectio	on group: <roo< th=""><th>t level</th><th>></th><th></th><th></th><th></th><th></th><th>~</th></roo<>	t level	>					~
Server	Authentication	SSL	SSH	Proxy	IntelliShell	MongoDB Tool	s Advanced	
Use	s 🙆 Connectir	ng -						×
Use	o Testing conn	ection						
CAU								
							Canadura	
OALLE	p Operation	onner	tion by				OK	
Acce	Configuring	SSL o	onnecti	on			OK	
Use	C Connecting	to ser	ver				ок	
clime c	Authenticati	ing as	rwuser				ок	En e
Client C	Reading se	rver st	atus fro	m con	nection		ок	LQ
Passph	ra Detecting a	ccessil	ble data		ок			
My c	Detecting N	longo	DB serv	er ver	sion		ок	
	Detecting N	longo	DB serv	er fea	ture compati	bility version	ок	
Select S	Connected						OK	
	v							
Use	s							
SNI Ho	s Hide detai	ls				ОК	Cancel	
						10	1994) - 1994)	

Figure 8-40 Checking the SSL connection

viii. After the check is successful, click **Save**.

Figure 8-41 Connection information

Connection Ma	anager								×
New Connection	New Group	Edit	Delete	Clone	Import	Export	To URI		t trial
Click here to filter	connections							1 m	atch
Name	DB Server		Security			Last Acce	ssed	Shortcut	
Es	"e langée		🔑 rwuser	@ admin					
									inager
									ask
Show on startu	p					Co	innect	Close	ask
☑ Show on startu C	P Quick Options					Co		Close Getting sta	red tobse
☑ Show on startu C	p Quick Options heme (requires restart	t): Sam	e as system			Co		Close Getting sta Knowledge Free Mong	rask ning rted base oDB courses
Show on startu C Ti 8	p Quick Options heme (requires restart ☑ show What's New	t): Sam	e as system er updating	studio 3T		Co		Close Getting sta Knowledge Free Mong Join the 31	rask rning rted base ooB courses community
Show on startu	p Quick Options heme (requires restart ☑ Show What's New ☑ Automatically ope	t): Sam tab aft	e as system er updating ection Man	Studio 3T ager at start	tup	Co	inpect	Close Getting sta Knowledge Free Mong Join the 31 Studio 31 f	ask ming rted base obB courses community eatures
Show on startu C Ti 8 8	p Quick Options heme (requires restart I Show What's New I Automatically ope □ Enable Session Res	t): Sam tab aft n Conn store	e as system er updating ection Man) Studio 3T ager at start	tup	Co	inpect	Close Getting sta Knowledge Free Mong Join the 31 Studio 31 Studio 31	ask rning rted ebase comsets community eatures ips and tricks

ix. On the connection information page, click **Connect** to connect to the replica set instance. After the replica set instance is successfully connected, **Figure 8-42** is displayed.

Figure 8-42 Connection succeeded

file Edit Database Collection Inc	dex Document GridFS View	Help			
onnect Collection Intellish	nell SQL Aggregate Map-	Be 🗾 🚱 号 Reduce Compare Schema Reschema	Tasks Export Import	t Data Masking SQL Migration Users	Roles Feedback
earch Open Connections (Ctrl+F)	aA < Quickstart				
25 rep[ics set rep[ics] [direct] > ⊖ asa > ⊖ direct > ⊖ beb > ⊖ ecc > ⊖ beb > ⊖ beb		Welcome to Stu Get started with the tool using Recent Connections Intercent Funders (1997) (1	udio 3T - F our detailed Knowle B	Full product trial edge Base. Tasks Task is feature that helps you automate 0 tasks set. Dopen Task Manager Dopen Task Manager Dopen Task Manager	common tasks.
		Create a free MongoDB cluster in the	cloud	Help and Learning	
		Quick Options Theme (requires restart): Same as system V Show What's New tab after updating St Automatically open Connection Manage	Judio 3T er at startup	 Getting started Knowledge base Free MongoD8 courses Join the 3T community Studio 3T features Studio 3T finit and tricks 	
Operations	2 ^	Enable Session Restore		Studio 3T Power User manual: hidden	gems that will

- Method 2: Manually connect to a DB instance.
 - i. In the displayed dialog box, select **Manually configure my** connection settings and click Next.

Figure 8-43 Manual connection mode

💽 Studio 31	for MongoDB - Full produ	ct trial														-	\times
File Edit E	atabase Collection Inde	x Documer	nt GridFS	View Help													
Connect •	Collection IntelliShel	I SQL A	Aggregate	Map-Reduce	Compare	Contraction Contra	Reschema	Tasks	Export	Import	Data Maskin	g SQL Migra	tion	L Users	Roles) Feedback	
Search Oper	Connections (Ctrl+F)	a	A < Q	uickstart													
				Con	nection Manay	ler Hew Group	Edit	Delete		Impor	t Egport	L N To URI	×	al marter.	Get a		^
				Click he	re to filter cor	nections						C	matches				
					if; ca	ou have a 1 paste it h Paste your URI:	connection st ere and Studi connection st	ring (<u>SRV o</u> o 3T will au ring (SRV o	<u>r standard)</u> to-configur r standard	i, e.g. for <u>y</u> e your cor) here:	our MongoDE Inection settin	<u>8 Atlas</u> deploym gs for you.	nt, you	automate	common	tasks.	
					۲	Manually c	onfigure my c	onnection s	ettings								
				Show	v on start						N	ext Ci	incel				
				Q	uick Opti	ons					1	Getting started Knowledge base		-			
				Th	eme (requires 1. Show What	restart): Sa	me as system	V Studio 2T			88	Free MongoDB c Ioin the 3T comr	ourses nunity				1
				2	Automatical	y open Cor	nection Mana	iger at start	up		d	Studio 3T feature	is				
Operations		-	2 ^		Enable Sessi	on Restore					d'	Studio 3T tips an	d tricks				~

ii. On the Server tab, set Server and Port.

NOTE

Server: EIP. Port: database port.

Figure 8-44 Server

Rew Connection	×
Connection name:	
Connection group: <root level=""></root>	~
Server Authentication SSL SSH Proxy IntelliShell MongoDB Tools Advanced	
Connection Type: Standalone	~
Server: D P	ort:
Read-Only Lock 1	
From URI Use this option to import connection details from a connection strin	ig / URI
Io UKI Use this option to export complete connection details to a connection	on string / URI
Test Connection Save	Cancel

iii. Click the Authentication tab and select Legacy(SCRAM-SHA-1).

Figure 8-45 Authentication

唇 New Connection		×
Connection name:		
Connection group: <ro< td=""><td>ot level></td><td>~</td></ro<>	ot level>	~
Server Authentication	SSL SSH Proxy IntelliShell MongoDB Tools Advanced	
Authentication Mode:	Legacy (SCRAM-SHA-1)	~
You have chosen an aut	None	
Please refer to the Mon	Basic (SCRAM-SHA-256)	
	X.509	
User name:	Kerberos (GSSAPI) - Studio 3T Ultimate	
Password:	LDAP (PLAIN) - Studio 3T Ultimate	
	Aws identity and Access Management (IAW) - Studio ST Olumate	
Authentication DB:		
	The database where the user is defined	
Always show the au	thentication database of the user account	
Always show all da	tabases and collections defined in roles of the user account	
Manually list additi	onal visible databases by their names 👔	
_ ·		
Test Connection	<u>S</u> ave	Cancel

iv. Set User name, Password, and Authentication DB.

Figure 8-46 Authentication

onnecu	on group: <ro< th=""><th>ot level</th><th>></th><th></th><th></th><th></th><th></th><th>~</th></ro<>	ot level	>					~
Server	Authentication	SSL	SSH	Proxy	IntelliShell	MongoDB Tools	Advanced	
Authen	tication Mode:	Legac	y (SCRA	M-SHA	1)			3
You ha Please i	ve chosen an aut refer to the <u>Mon</u>	thentical 20DB Se	tion met curity C	thod wh hecklist	ich might mak to help secure	re your MongoDB ins your database(s).	tance vulnerable	to attacks.
User n	ame:	rwuse	r,					
Passwo	ord:	••••	•••••	••••				•
Authen	tication DB:	admin	2					
		The da	tabase	where	the user is d	efined		
			C	3				
Alwa	ays show the au	uthentic	ation d	atabase	of the user	account		
☑ Alwa ☑ Alwa	ays show the au ays show all da nually list additi	uthentic tabases	ation d and co	atabase ollection	of the user is defined in	account roles of the user a nes 1	ccount	
☑ Alwa ☑ Alwa ☑ Mar Databa	ays show the au ays show all da nually list additi ases: admin te	uthentic tabases onal vis	ation d and co ible da	atabase bliection tabases	e of the user ns defined in s by their nar	account roles of the user a nes 1	ccount	

v. Click Test Connection to check whether the connection is successful.

Figure 8-47 Test Connection

	group: <root< th=""><th>t level></th><th></th><th></th><th></th><th></th><th>× ×</th></root<>	t level>					× ×
Server Au	uthentication	SSL SSH	Proxy	IntelliShell	MongoDB Tools	Advanced	
Authentic	🔁 Connectin	9					×
You have Please rei	Testing conn	ection					acks.
User nar	Operation				5	Status	
Passwore	Initializing c	onnection			c	Ж	
	Connecting	to server			0	ОК	
	Authenticati	ng as rwus	er		0	ок	
Authentie	Reading ser	rver status	from con	nection	(DK	
	Detecting a	ccessible d	atabases		(DK	
	Detecting N	longoDB s	erver ver	sion	(DК	
	Detecting N	longoDB s	erver fea	ture compati	bility version (ок	
	Connected				(ОК	
							_
🗹 Alway							
🗹 Alway	Hide detail	s			ОК	Cancel	
Manu Manu	n y nacadanao n		atabase.	y uncur man	nes 😈		

vi. Click the SSL tab and select Use SSL protocol to connect.

NOTE

If SSL data encryption is disabled, skip this step and go to **6.ix**.

Figure 8-48 SSL

Connection name: Connection group: eroot level> Server Authentication SSL SSH Proxy IntelliShell MongoDB Tools Advanced Use SSL protocol to connect Use own Root CA file (sslCAFile) Accept server SSL certificates trusted by the gperating 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: ILS Allow invalid hostnames (sslAllowInvalidHostnames) CNI Host Name:	Connectio	n									
connection group: <root level=""> Server Authentication SSL SSH Proxy IntelliShell MongoDB Tools Advanced Server Authentication SSL SSH Proxy IntelliShell MongoDB Tools Advanced Server SSL protocol to connect Use own Root CA file (sslCAFile) Server SSL certificates trusted by the gperating system Accept server SSL certificates trusted by the gperating system Accept any server SSL certificates Use Client Certificate (sslPEMKeyFile) Client Certificate is not protected by a passphrase Select SSL/TLS: TLS Allow invalid hostnames (sslAllowInvalidHostnames) SNI Host Name:</root>	ion name:										
Server Authentication SSL SSH Proxy IntelliShell MongoDB Tools Advanced Use SSL protocol to connect Use own Root CA file (sslCAFile) Accept server SSL certificates trusted by the gperating 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 Allow invalid hostnames (sslAllowInvalidHostnames) SNI Host Name:	ion group	<roc< th=""><td>ot level</td><td>></td><td></td><td></td><td></td><td></td><td></td><td>~</td><td></td></roc<>	ot level	>						~	
Use SSL protocol to connect Use own Root CA file (sslCAFile) 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 Allow invalid hostnames (sslAllowInvalidHostnames) SNI Host Name:	Authent	cation	SSL	SSH	Proxy	IntelliShell	MongoDB Tools	Advanced			
Use own Root CA file (sslCAFile) 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 Allow invalid hostnames (sslAllowInvalidHostnames) Use Server Name Indication (Advanced) SNI Host Name:	SSL prot	ocol to	conne	ect		1	1		1		
Accept server SSL certificates trusted by the <u>operating system</u> 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 Allow invalid hostnames (sslAllowInvalidHostnames) Use Server Name Indication (Advanced) SNI Host Name:	own <u>R</u> oc	t CA fil	e (s	slCAFile	e)						
 Accept server SSL certificates trusted by the <u>operating system</u> <u>Accept any server SSL certificates</u> Use Client Certificate (sslPEMKeyFile) Client Certificate: Passphrase: 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: 										Q (i
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 Allow invalid hostnames (sslAllowInvalidHostnames) Use Server Name Indication (Advanced) SNI Host Name:	ept serve	SSL ce	ertifica	tes tru	sted by	the <u>o</u> peratin	g system				
Use Client Certificate (sslPEMKeyFile) Client Certificate: Passphrase: 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:	ept any s	rver S	SL cert	ificates							
Client Certificate: Passphrase: 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:	e Client Ce	rtificate	e (ss	IPEMK	eyFile)						
Passphrase: 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: 	Certificate	:								Q (Ð
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:	hrase:									•	Ð
Select SSL/TLS: TLS Allow invalid hostnames (sslAllowInvalidHostnames) Use Server Name Indication (Advanced) SNI Host Name:	client cer	ificate	is not	protec	ted by a	a passphrase	÷				
Allow invalid hostnames (sslAllowInvalidHostnames) Use Server Name Indication (Advanced) SNI Host Name:	SSL/TLS:	TLS							\sim	1	
Use Server Name Indication (Advanced)	w invalid	hostna	mes (-	-sslAllc	wInvali	dHostnames)				
Use Server Name Indication (Advanced)							•				
SNI Host Name:	Server N	ame In	dicatio	on (Adv	anced)	1					
	ost Name										
Lest Lonnection Save Cance	onnection						1	Cave		ancel	

vii. Select **Use own Root CA file (--sslCAFile)**, import the certificate, and select **Allow invalid hostnames**.

NOTE

Download the SSL certificate and verify the certificate before connecting to databases.

On the $\ensuremath{\mathsf{Instances}}$ page, click the target DB instance name. In the $\ensuremath{\mathsf{DB}}$

Information area on the **Basic Information** page, click $\stackrel{l}{\checkmark}$ in the **SSL** field to download the root certificate or certificate bundle.

Figure	8-49	Entering	SSL	information

	stootiev						Ť	
erver Authenti	cation SSI	SSH	Proxy	IntelliShell	MongoDB Too	ols Advanced		
Use SSL prote	ocol to con	nect						
🖲 Use own Roo	t CA file (sslCAFil	e)					
C:\Users\	\D	ownload	ds ca.crt	10			Q	•
Accept server	SSL certific	ates tru	isted by	the operatin	g system			
Accept any se	rver SSL ce	rtificate	s					
Use Client Ce	rtificate ((evFile)					
Client Certificate	:	2011 2111	(cyrne y					6
Passphrase:							۲	6
✓ My client cert	ificate is no	t protec	ted by a	passphrase				6
Select SSL/TLS:	TLS		,				0	
Allow invalid	hostnames	(sslAlle	owInvali	dHostnames) 🚯			
				-				
Use Server N	ame Indicat	ion (Ad	vanced)	•				
SNI Host Name:								

viii. Click Test Connection to check whether the connection is successful.

		- <u>14</u>		
erver A	thentication SSL SSH Proxy IntelliS	hell MongoDB Tools	Advanced	
⊡ Use S	🔁 Connecting		×	
O Use o	Testing connection			
C:\Us				
Accen	Operation	c	tatus	
	Initializing connection	с С	K	
Accep	Configuring SSL connection	c	ĸ	
Use C	Connecting to server	C	к	
Client Co	Authenticating as rwuser	c	ĸ	ER Ø
client Ce	Reading server status from connection	C	K	LQ @
Passphra	Detecting accessible databases	C	ĸ) ک
My di	Detecting MongoDB server version	C	ĸ	
	Detecting MongoDB server feature con	npatibility version C	ĸ	
Select SS	Connected	C	ĸ	•
Use S				
SNI Host	Hide details	ОК	Cancel	
	Hide details	OK	Cancel	

Figure 8-50 Checking the SSL connection

ix. After the check is successful, click **Save**.

Figure 8-51 Connection information

Connection Ma	anager								×	~	
New Connection	Tew Group	Edit	Delete	Clone	Import	Export	To URI			t trial	
Click here to filter	connections								1 match		
Name	DB Serve	r	Security			Last Acce	ssed	Shortcut		1	
Ee	"a large		🔑 rwuser	@ admin							
										magar	
										inager	
										ask	
Show on startu	qu					Co	nnect	Clo	se	ask rning	
Show on startu	P Quick Options	5				Co	nnect	Clo Gettin	ise ig started ledge bas	ing rning e	
Show on startu	up Quick Options	5 art): Sam	e as system	▼		Co	nnect	Cle Gettin Knowl	ise g started ledge bas	rning courses	
Show on startu C Ti	₽ Quick Options heme (requires resta I Show What's Ne	S art): Sam	e as system	Studio 3T		Co		Clo Gettin Knowl Free M	ise g started ledge bas MongoDB në 3T com	rning e courses amunity	
Show on startu C Ti 8	up Quick Options heme (requires resta ☑ Show What's Ne ☑ Automatically op	5 art): Sam w tab aft	e as system er updating ection Man.	Studio 3T	tup	Co	npect	Cle Gettin Knowl Free M Join th Studio	ise Ig started ledge bas MongoDB ne 3T con o 3T featu	rning e courses muulty res	
Show on startu C Ti S S C	P Quick Option: heme (requires resta ✓ Show What's Ne ✓ Automatically op □ Enable Session R	5 art): Sam w tab aft ien Conn iestore	e as system er updating ection Man	Studio 3T ager at start	tup	Co	npect	Clo Gettin Knowl Free N Join th Studic Studic Studic	ise Ing started ledge bas MongoDB ne 3T con o 3T featu o 3T featu o 3T tips a	e courses annunity res und tricks	

x. On the connection information page, click **Connect** to connect to the replica set instance. After the replica set instance is successfully connected, **Figure 8-52** is displayed.

Figure 8-52 Connection succeeded

ile Edit Database Collection In	dex Document Grid	S View Help												
onnect Collection Intellist	hell SQL Aggrega	e Map-Reduce	 Compare	Contraction Contra	Reschema	Tasks	Export	Import	Data Masking	SQL Migration	Lusers	Roles	Feedback	
arch Open Connections (Ctrl+F)	aA <	Quickstart												
\$ repics set repica Sired > as > b as > b bb > b bb > b bb > b ccc > b config >		C C S S	Welcc Set started Recent Cor In forward In Create a no Create a no Create a for Quick Optic heme (requires i Sonow What's Automatical Parable Sector	with the mection 0.154.218.11 moments eg section Mar w connects see MongoD DDS restart): Sai s New tab a' y open Con on Restrice	to St tool using bases ager on B duster in the me as system `` ther updating S nection Manage	cloud cloud	D 3T a	- F	Gull pro dge Base. Tasks Tasks if o tasks III o III o III o III o III o III o III o III o III o III o III o III o III o III o III IIII IIII IIII III IIII IIII IIII IIII	S a fadure that helps set. pen Task Manager zeste a new task and Learning tiog started onledge base # Mongold scores an In B 21 Community did 31 Testart Starters did 31 Testart Starters	ial vou automate	e common	tasks.	
perations	古 ^								🖑 Stu	idio 3T Power User m	anual: hidder	gems that	t will	
9 Getting Started with Common Practices

After purchasing and connecting to a DB instance, you can view common practices to better use DDS.

Practic e	Document	Description
Data Backup s	Configuring an Automated Backup Policy	DDS backs up data automatically based on the automated backup policy you set. Regularly backing up your database is recommended. If your database becomes faulty or data is corrupted, you can restore it from backups.
		The automated backup policy for DDS is enabled by default.
	Creating a Manual Backup	This practice describes how to create a manual backup. Creating a backup for a DB instance helps ensure data can be restored if needed, ensuring data reliability.
Data Restor ations	Restoring Data to a New Instance	DDS allows you to restore an existing automated or manual backup to a new instance. The restored data is the same as the backup data.
		When you restore an instance from a backup file, a full backup file is downloaded from OBS and then restored to the instance at an average speed of 40 MB/s.
	Restoring Data to the Original Instance	DDS allows you to restore an existing automated or manual backup to an original instance. The restored data is the same as the backup data.
		When you restore an instance from a backup file, a full backup file is downloaded from OBS and then restored to the instance at an average speed of 40 MB/s.

Table 9-1 Common practices

Practic e	Document	Description
	Restoring Data to a Point in Time	DDS allows you to restore cluster and replica set instances to a point in time. When you enter the point in time that you want to restore the instance to, DDS downloads the most recent full backup file from OBS to the instance. Then, incremental backups are also restored to the specified point in time on the instance. Data is restored at an average speed of 30 MB/s.
Data Migrati on	Migrating Data Using mongoexport and mongoimport	mongoexport and mongoimport are backup and restoration tools provided by the MongoDB client. You can install a MongoDB client on the local device or ECS and use the mongoexport and mongoimport tools to migrate your on-premises MongoDB databases or other cloud MongoDB databases to DDS instances. Before migrating data from a MongoDB database to DDS, transfer data to a .json file using the mongoexport tool. This practice describes how to import the data from the JSON files to DDS using the mongoimport tool on the ECS or from some other devices that can access DDS.
	Migrating Data Using mongodump and mongorestor e	mongodump and mongorestore are backup and restoration tools provided by the MongoDB client. You can install a MongoDB client on the local device or ECS and use the mongodump and mongorestore tools to migrate your on-premises MongoDB databases or other cloud MongoDB databases to DDS instances.
	From Other Cloud MongoDB to DDS	DRS helps you migrate MongoDB databases from other cloud platforms to DDS instances on the current cloud. With DRS, you can perform real-time migration tasks with minimal downtime. Services and databases remain operational during a migration.
	From On- Premises MongoDB to DDS	DRS helps you migrate data from on-premises MongoDB databases to DDS instances on the current cloud. With DRS, you can perform real-time migration tasks with minimal downtime. Services and databases remain operational during a migration.
	From ECS- hosted MongoDB to DDS	DRS helps you migrate data from MongoDB databases on ECSs to DDS instances on the current cloud. With DRS, you can perform real-time migration tasks with minimal downtime. Services and databases remain operational during a migration.
	From DDS to MongoDB	This practice describes how to migrate data from a DDS instance to an on-premises MongoDB database.

Practic e	Document	Description
Instanc e Modifi cations	Changing an Instance Name	This practice describes how to change an instance name to identify different instances.
	Changing an Instance Class	This practice describes how to change the class of a cluster, replica set, or single node instance.
	Scaling Up Storage Space	This practice describes how to scale up the storage space of an instance. If you scale up the storage space of an instance, the backup space increases accordingly.
Data Securit y	Enabling or Disabling SSL	Secure Socket Layer (SSL) is an encryption-based Internet security protocol for establishing an encrypted link between a server and a client. It provides privacy, authentication, and integrity to Internet communications. SSL:
		• Authenticates users and servers, ensuring that data is sent to the correct clients and servers.
		• Encrypts data to prevent it from being intercepted during transfer.
		• Ensures data integrity during transmission. After SSL is enabled, you can establish an encrypted connection between your client and the instance you want to access to improve data security.
	Changing a Security Group	This practice describes how to change a security group for cluster and replica set instances.
Logs	Error Logs	DDS log management allows you to view database- level logs, including warning- and error-level logs generated during database running, which help you analyze system problems.
	Slow Query Logs	Slow query logs record statements that exceed operationProfiling.slowOpThresholdMs (500 seconds by default). You can view log details and statistics to identify statements that are executing slowly and optimize the statements. You can also download slow query logs for service analysis.
	Audit Logs	An audit log records operations performed on your databases and collections. The generated log files are stored in OBS. Auditing logs can enhance your database security and help you analyze the cause of failed operations.