

HaydnCSF

Best Practices

Issue	3.0
Date	2026-03-05



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2026. 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 Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property 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 Cloud 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.

Contents

1 Partner Lead Certification Tests On InnoStage Workbench..... 1
1.1 Certification Test Instructions.....1
1.2 Certification Test Operation Guide.....6
1.2.1 Jointly Initiating a Project In The Partner Center..... 6
1.2.2 Create Solution.....10
1.2.3 Solution design.....27
1.2.4 Test Requirements Submission..... 32
1.2.5 Test Cases Design..... 36
1.2.6 Provision Test Resources..... 42
1.2.7 Test Case Execution..... 43
1.2.8 Generate And Submit The Test Report..... 53
1.2.9 Third-Party Tools.....55

1 Partner Lead Certification Tests On InnoStage Workbench

1.1 Certification Test Instructions

NOTE

- The same solution has been certified and tested on HUAWEI CLOUD. The test report can be reused.
- Function tests, performance tests, and reliability tests ,can contact Huawei TE to provide self-test reports based on HUAWEI CLOUD .
- The partner leads the design and test of the solution. The partner must ensure that the solution design and test results meet business requirements and commercial release requirements.
- The certification test includes the function test, performance test, security test, reliability test, and integration test case template: [Partner Lead Case Template](#). Select and edit the template based on the actual product situation. For details about how to use the template, see [Test Cases Design](#).
- The certification test is performed on the [InnoStage Workbench](#). You are advised to use the Chrome browser to access the solution workbench.

HUAWEI CLOUD Certification Test Contents And Requirements

The test contents include function test, performance test, security test, reliability test, and integration test. The following table lists the general requirements of the certification test. During the execution of test cases, if the execution result does not meet the test requirements, related functions must be developed or rectified.

Table 1-1 General Description of Certification Test Requirements

Test Type	Case Type	Test Requirements
Function test(Mandatory)	1)Manual test case	Generate function cases based on the function list. • The test cases must correspond to the feature list and must cover all core functions under level-2 functions. • The test case must contain detailed operation procedure description, and the test case content must cover the title or function node name. • Test cases must have E2E scenario test cases of the main scenario. • If hardware products are involved, the partner needs to provide the product description, quality test report (third-party or self-test report), and function test report (if any).
Integration test(Mandatory)	1)Manual test case	Generate integration cases based on the architecture. • If hardware products are involved, select three to six core business scenarios of the solution to test the connectivity of business flows and data flows. • If the integration case template does not cover all cloud service integration cases, contact the TE to design cases.
Security test(Mandatory)	1)Manual test case 2)Binary virus scan case	generates 16 manual interview security test cases, 1 manual virus scanning case, and 1 automatic virus scanning case based on the case template. During the virus scanning test, you can use a third-party tool to scan (manual cases) or use the scanning function of the innostage workbench to scan (automatic cases).

Test Type	Case Type	Test Requirements
Reliability test(Optional)	1)Manual test case	If reliability tests are required, partners can design test cases by themselves or contact Huawei solution TE to support reliability test case design. • Provide a reliability self-test report based on the HUAWEI CLOUD environment, covering reliability indicators or features. • Design test cases based on the reliability indicator sheet in the <Feature List Template>. Each feature must correspond to at least one test case to verify the indicator or feature.
Performance test(Optional)	1)Performance automation test cases	Generate one performance automation test cases based on the test case template,partners can create several performance automation cases as required. • The partner provides performance specifications based on the core scenarios in the OBP project initiation materials. • Performance test case templates in core scenarios of the solution are as follows: Example 1: (User operation follow page response latency) Two 8-core 16 GB servers are deployed in the InnoStage Workbench test. The redirection interface is 50 concurrent requests. The pressure test takes 5 minutes. The MTTR is less than 2000 ms. Example 2: (Number of concurrent users created by the platform follow) Two 4-core 8 GB servers are deployed in the InnoStage Workbench test. User interfaces are created at 100 concurrent users. The pressure test lasts for 10 minutes. The success rate is higher than 99.8%. • If hardware products are involved, select three to four hardware service scenarios and perform continuous concurrent tests for 0.5 to 2 hours to reflect the hardware product performance indicators. For example, the camera hardware product displays the resolution of camera lens camera stream and the number of concurrent video access channels.

Introduction To User Roles

A user can have multiple roles in a workspace and different roles in different workspaces. Spaces are isolated from each other. Different roles can be responsible for different affairs. For partner lead certification, the following roles are required:

- Administrator: space administrator, who can manage members in the space, for example, add members and set member roles, and review the test report.
- Architect: register, design, and review solutions, create test requirements, and handle test problems in the workspace.
- Test engineers: design and execute test cases, provision test resources, handle test problems, generate test reports and review test report.
- Guest: when inviting a user to a space, the user can be set as a guest role. Users with the guest role can only view the user in the space, but cannot perform any change operation.

Preparations Before Certification

All partners to participate in the certification need to log in to the InnoStage Workbench first.

Click [InnoStage Workbench](#) The login page is displayed. You can select an IAM account or a Huawei account.

Figure 1-1 HUAWEI CLOUD Login

IAM User Login

y

.....

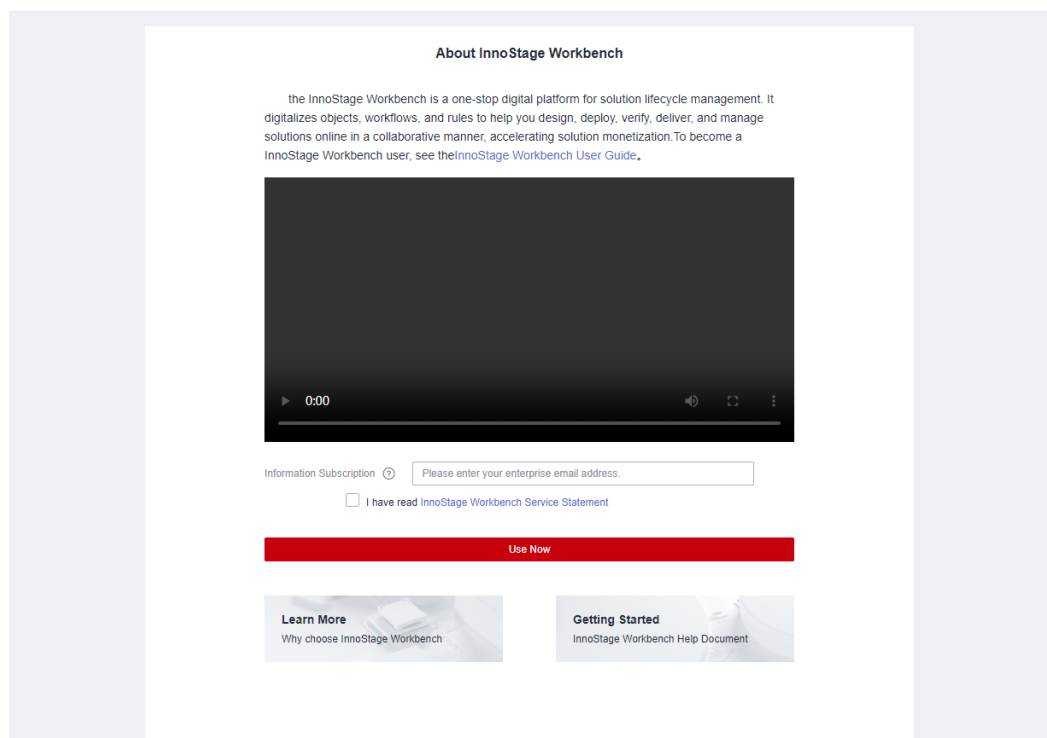
Log In

Forgot Password ☐ Remember me

Use Another Account: HUAWEI ID | Federated User

If you log in for the first time, the service statement signing page is displayed. Read the statement and check [I have read InnoStage Workbench service statement], the email address is optional.

Figure 1-2 Service Statement



Click [Use Now]

1.2 Certification Test Operation Guide

1.2.1 Jointly Initiating a Project In The Partner Center

Partner needs to create a solution and initiate a joint project in the partner center. After project initiation, a workspace is automatically generated in the InnoStage Workbench. Partner account, Huawei PSA and two test engineers are automatically added to the workspace.

NOTICE

If the partner program does not complete joint project initiation in the partner center, you need to manually create a workspace in the InnoStage Workbench and add space members. Go to [Create Workspaces And Add Space Members](#) to read the guide.

1. Create a solution

The partner creates a solution and enters basic information in the Partner Center. After the creation is complete. The solution information, such as the solution name and function list, will be imported to the solution workbench. For details, see [Partner Center-Creating a Solution](#).

2. Jointly Initiating a Project

The partner submits the project initiation application in the Partner Center. Huawei reviewer reviews the project initiation. For details, see [Partner Center-Jointly Initiating a Project](#)

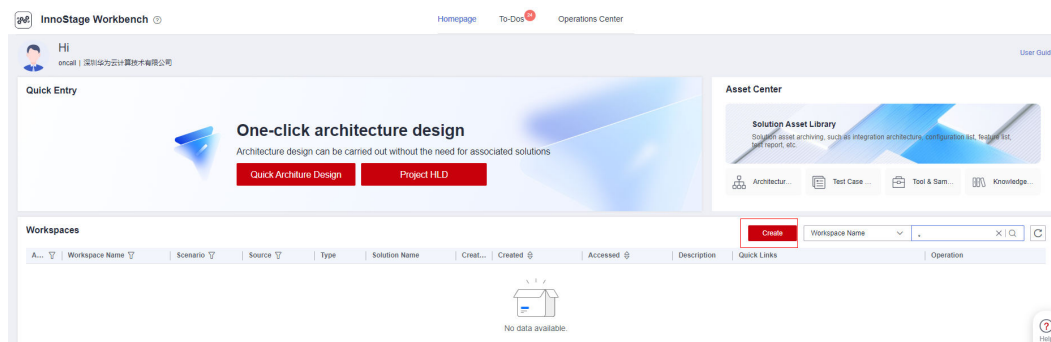
3. After the joint project initiation is complete, a workspace is automatically generated on the InnoStage Workbench. The project partner initiator, Huawei PSA, and Huawei test engineer are automatically added to the workspace and a solution draft is generated. The partner can click [Apply for Joint Design and Verification] in the Partner Center. The solution editing page is displayed. See [Requesting Joint Design and Verification](#) for details.

Create Workspaces And Add Space Members

If the partner has completed joint project initiation in the partner center, skip this section.

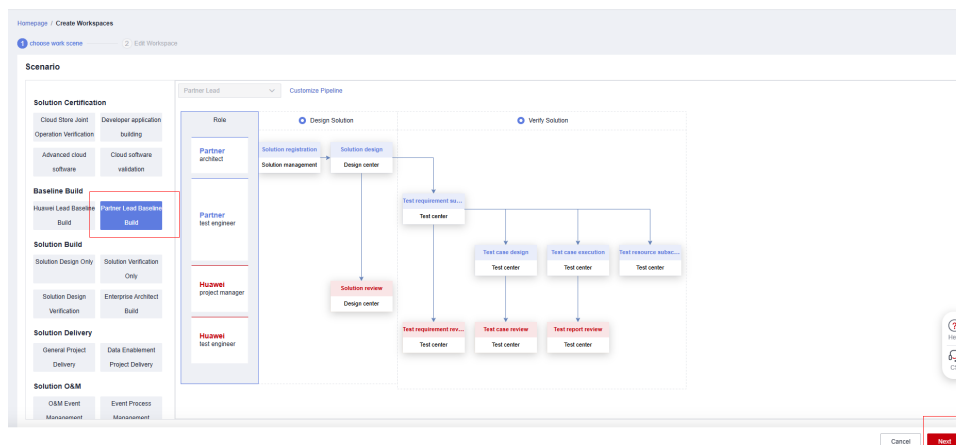
1. InnoStage Workbench console -> Homepage ->click [Create].

Figure 1-3 New Space



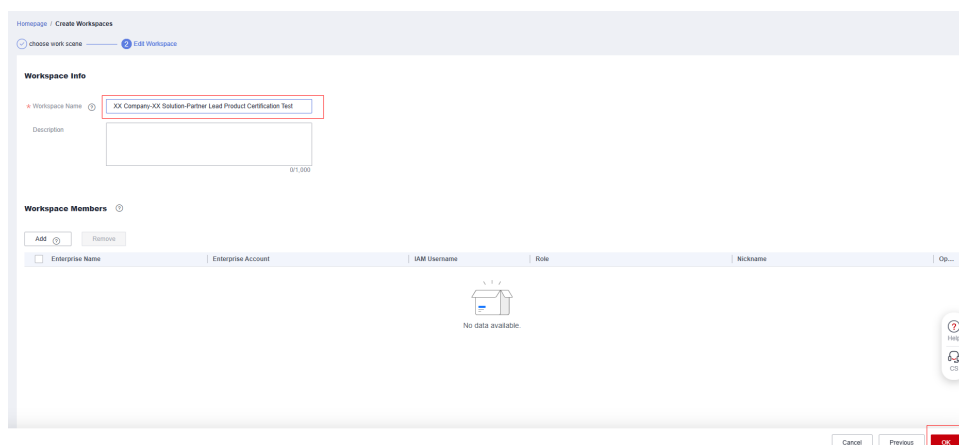
2. Select [Partner Lead Baseline Build]. The overall process of Partner Lead Baseline Build is automatically displayed on the right. Click [Next].

Figure 1-4 Creating Workspaces



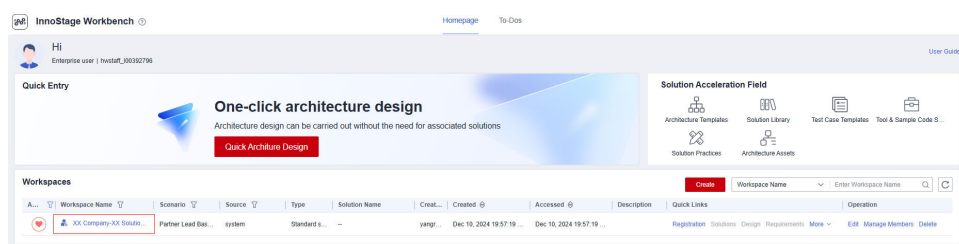
3. On the edit space information page, edit your space name in the format XX Company-XX Solution-Partner Lead Product Certification Test. Replace XX Company with your company name and XX Solution with your solution name. Space Description is optional. Click [OK].

Figure 1-5 Creating Workspaces



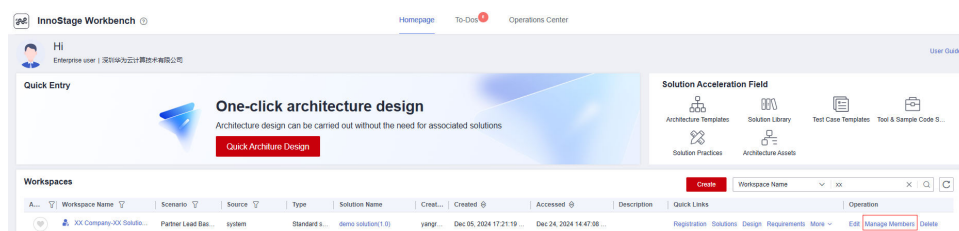
4. Return to the home page of the InnoStage Workbench. You can view the created space in the workspace list.

Figure 1-6 Homepage



5. After the space is created, add space members. Click the [Manage Members] button of the workspace.

Figure 1-7 Homepage



NOTE

Only members added to the workspace can participate in certification. The partner needs to add Huawei members to the space.

6. Click the [Add] -> Click [Invite Members].

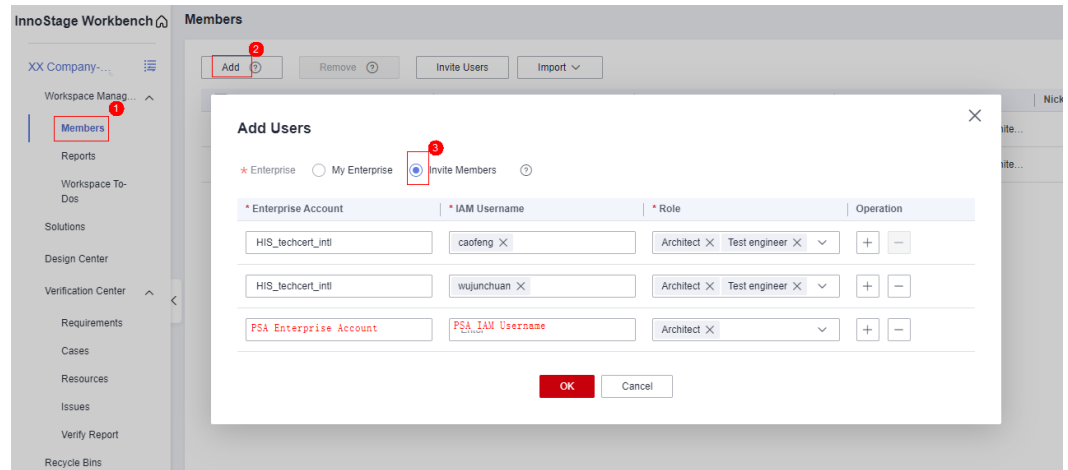
– Add two fixed Huawei test engineers and a PSA (Required).

Enterprise Account: HIS_techcert_intl IAM Username: wujunchuan
Role: Architect, Test engineer.

Enterprise Account: HIS_techcert_intl IAM Username: caofeng Role: Architect, Test engineer.

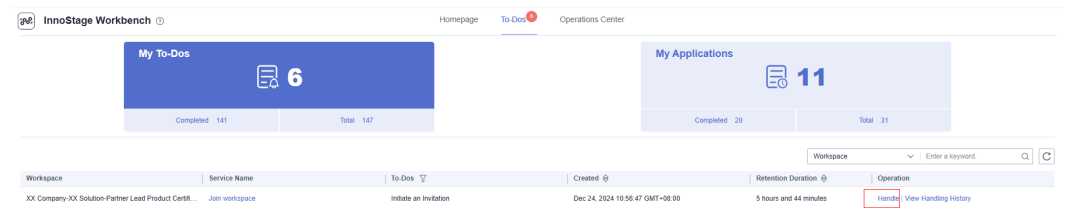
Contact the ecosystem manager to obtain the psa account Role: Architect.

Figure 1-8 Invite Huawei members



The invited person will receive the invitation to-do task. Click [Handle] and agree to join the workspace.

Figure 1-9 to-do



- You can also directly add an enterprise member with the same enterprise account.(Optional)

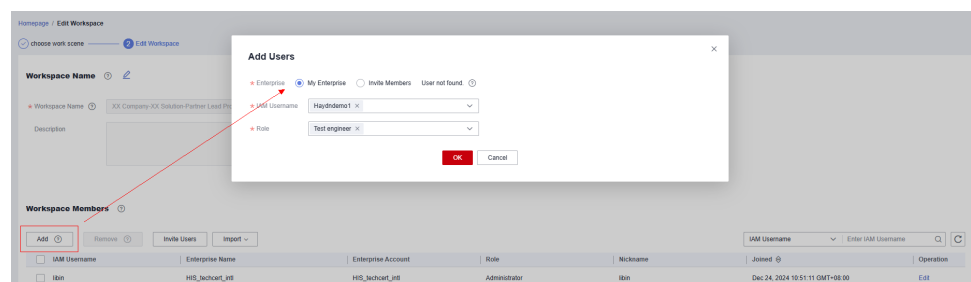
Click[My Enterprise]->Select the members to be added to the space.

When creating a solution and designing an architecture, you need to select the architect role.

When creating a requirement and executing a test case, you need to select the test engineer role.

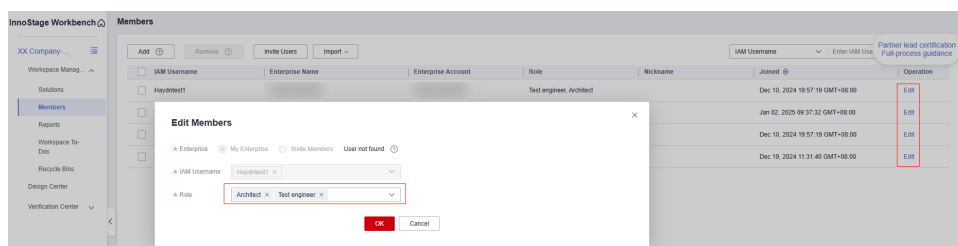
Click[OK]

Figure 1-10 Add enterprise members



- The space administrator can edit the role of a member in the workspace. On the member management page, click the [edit] button of a member to modify the role.

Figure 1-11 Edit Member

**NOTE**

Huawei test engineers(TE)are responsible for helping you complete the test. If you encounter any problem, you can contact Huawei test engineers by email.

wujunchuan:wujunchuan@huawei-partners.com

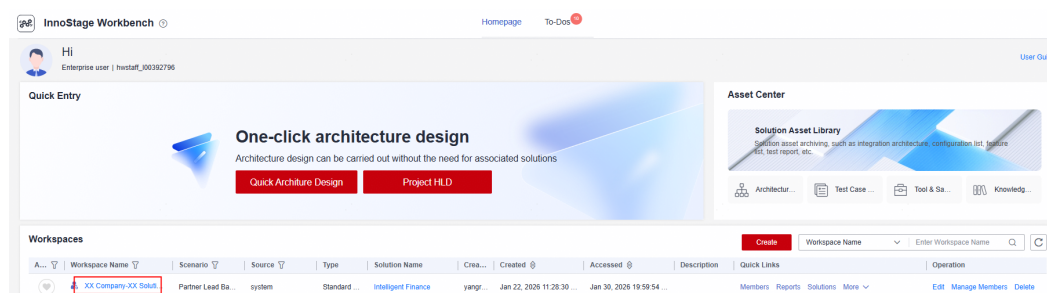
caofeng:caofeng24@h-partners.com

1.2.2 Create Solution

Partner Architects register solutions.

The architect clicks the workspace name on the home page to go to the solution management page.

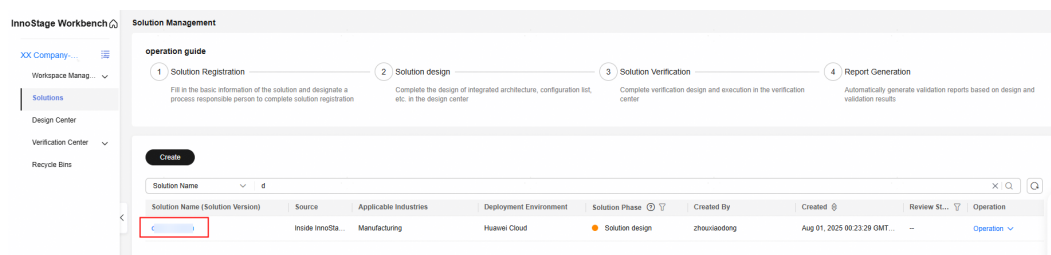
Figure 1-12 Homepage



Complete solution registration on the InnoStage Workbench.

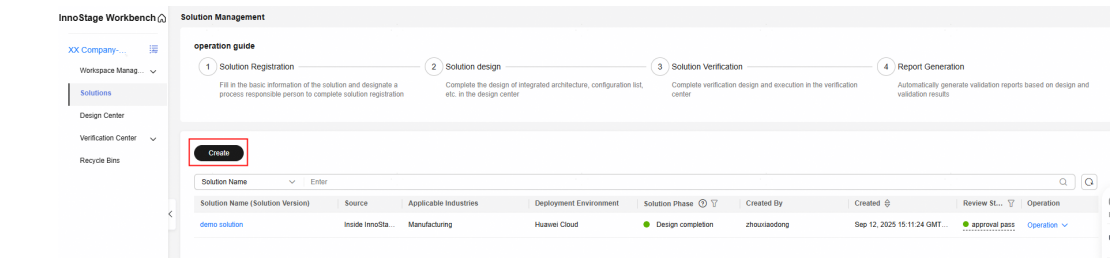
- If you completed the joint project initiation in the partner center, you can go to the solution draft editing page of the InnoStage Workbench from the partner center. For details, see [Certification Test Operation Guide](#). Alternatively, you can log in to the InnoStage Workbench, click the workspace name to enter the workspace, click the solution name.

Figure 1-13 Editing Solution



- If you create a workspace manually, you need to create a schema manually,log in to the InnoStage Workbench , click the workspace name to enter the workspace, choose [Solution] -> [Create].

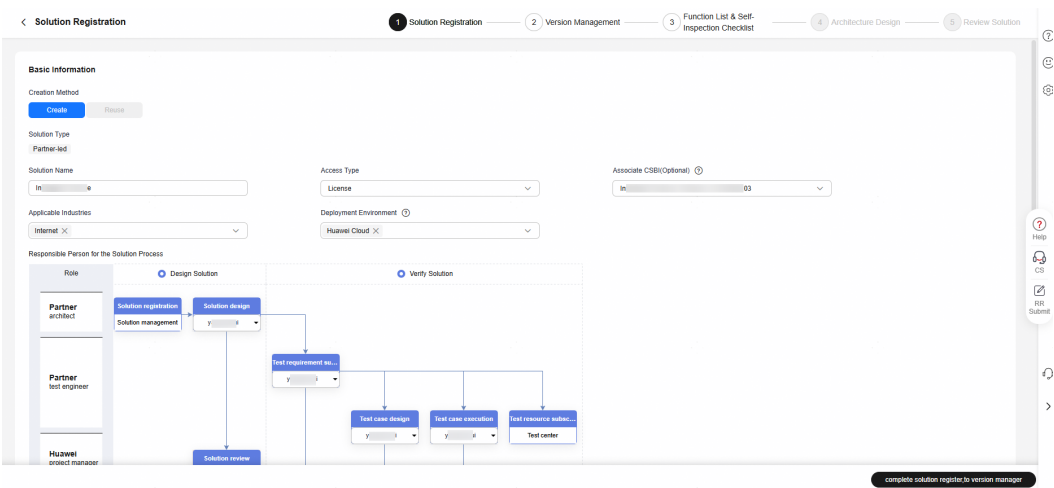
Figure 1-14 Creating Solution



Reuse Verified Solution-NoS(Create)

Step 1 Basic Information:

Figure 1-15 Solution Registration



Fill in the solution basic info.

Information item	Description
Solution Name	If the solution name has been automatically filled in, do not modify it. If the solution name is not automatically filled in, associate it with CSBI,the solution name will be automatically filled in based on CSBI. If the project initiation has not been completed,please enter the solution name,the solution name must be consistent with the solution name in the project initiation OBP material.

Information item	Description
Access Type	The value can be Hardware,API,Lisence,Saas.
Associate CSBI(Optional)	Associate the solution of the CSBI master data platform. The baseline solution must be initiated and associated here. If the project initiation has not been completed, you can also complete the association through the solution change function after the project initiation is completed.
Applicable Industry	Select the industry to which the product is applied. You can select multiple industries.
Deployment Environment	Set this parameter based on the actual deployment environment. The value can be HUAWEI CLOUD, HUAWEI CLOUD Stack (HCS), HUAWEI CLOUD Stack Online (HCSO), or Intelligent EdgeSite (IES)
Solution Description	Fill in the product solution description by referring to the sample text dimension.(The solution description is mandatory. Do not use the sample text directly.)

Select Node Handler.

Information item	Description	Sub-item
Solution design	The person responsible for designing the technical architecture and configuration list needs to be an architect role in the workspace to be selected.	Select a partner's architect
Solution review	Person responsible for reviewing the solution, technical architecture, and configuration list	Select the PSA and a TE that interconnects with the project.
Test requirement submission	Person responsible for editing and submitting test requirements	Select a partner's test engineer

Information item	Description	Sub-item
Test case design	Person responsible for designing test cases based on service requirements.	Select a partner's test engineer
Test case execution	Person responsible for executing test cases	Select a partner's test engineer
Test requirement review	Person responsible for reviewing requirements	Select the TE that interconnects with the project.
Test case review	Person responsible for reviewing whether test cases are qualified	Select the TE that interconnects with the project.
Test report review	Person responsible for reviewing whether the test report is qualified	Select Caofeng and wujunchaun.

NOTICE

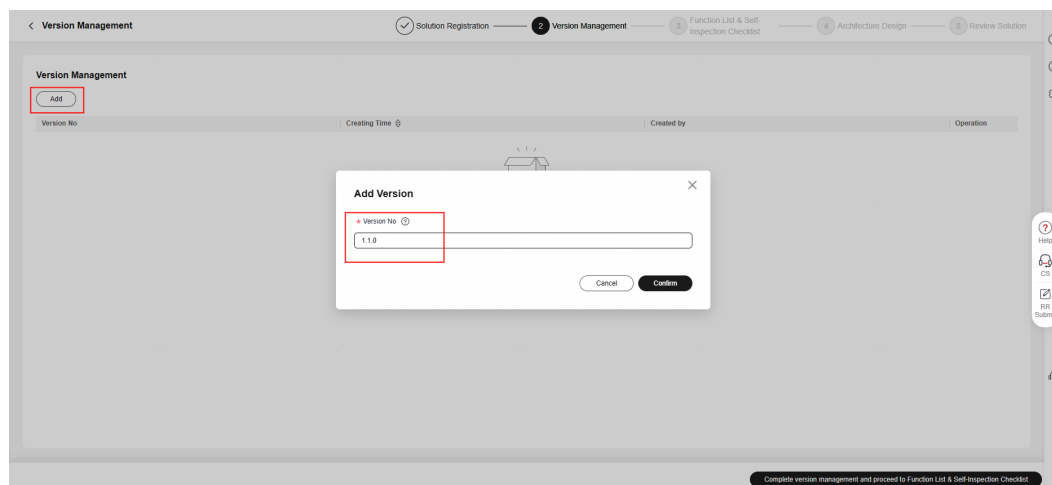
By default, the handler of each node is the specified user in the flowchart.

When finished, click [complete solution registe,to version manager].

Step 2 Version Manager:

Click [Add]->Enter the version number in the dialog box that is displayed.

Figure 1-16 Add Version



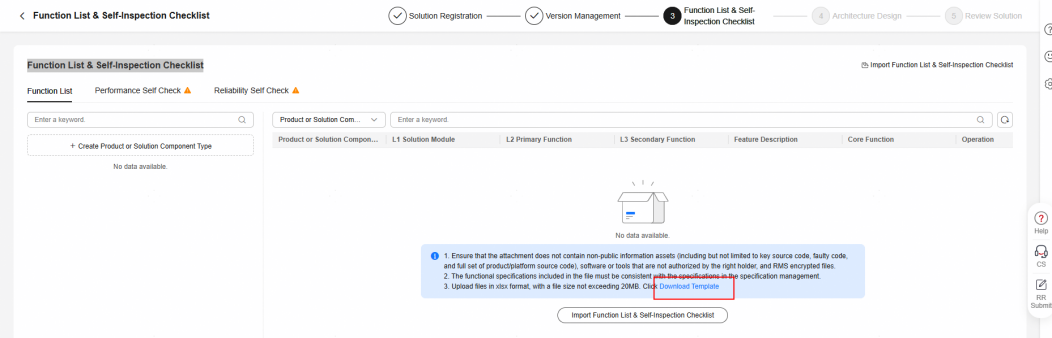
When finished, click [Complete version management and proceed to Function List & Self-Inspection Checklist].

Step 3 Function List & Self-Inspection Checklist:During subsequent solution verification, function test requirements and test cases are generated based on

the function list, performance test requirements and test cases are generated based on the performance indicator selfCheck, and reliability test requirements and test cases are generated based on the reliability index self-check.

- 1. Download the function list template.

Figure 1-17 Download template



- 2. Fill in the function list template.
 - Open the template and enter the solution name in the format of [XXX system product function list, version number: vx.x].

Figure 1-18 Modifying the solution name and version number

XXX system product function list/XXX solution feature list, version number: vx.x					
Product or Solution Component Type*	Product or Scenario Component Name*	Feature Category-L1*	Feature Category-L2*	Feature Category-L3*	Feature Description*

Figure 1-19 Example

Intelligent Finance system product function list, version number: v1.0					
Product or Solution Component Type*	Product or Scenario Component Name*	Feature Category-L1*	Feature Category-L2*	Feature Category-L3*	Feature Description*

- The information in column A does not need to be adjusted. The product or solution component column in column B has three types: software, hardware, and manual service. Fill in the content involved in the solution based on the site requirements. In normal cases, the software part is mandatory. For components that are not involved, delete the corresponding information.

Figure 1-20 Software, hardware, and manual service types

XXX system product function list/XXX solution feature list, version number: vx.x						
Product or Solution Component Type ^a	Product or Scenario Component Name ^a	Feature Category-L1 ^a	Feature Category-L2 ^a	Feature Category-L3 ^a	Feature Description ^a	Core functions ^a
Product or solution software (Fill in the associated products, advanced cloud products, and partner lead solution.)	XXX system (example)	Operation center	User management	Enterprise user management	Function and Feature Description 1	
				Individual User Management	Function and Feature Description 2	
			Personal Center	Login	Function and Feature Description 3	
				Log Out		
				Setting basic information		
				Security Settings		
			Operation report			
			Workbench	Work management		
Product or solution hardware (Fill in the associated products, advanced cloud products, and partner lead solution.)	XX hardware (example)	Hardware module	Feature 1	Function and Feature 1.1	Function and Feature Description 1	
			Feature 2	Features 2.1	Function and Feature Description 2	
			Feature 3	Functional Features 3.1	Function and Feature Description 3	
			Integrated delivery	Integrated delivery	System integration, delivery, deployment, commissioning, etc.	
Solution manual service (Fill in partner lead solution)	Manual service for the XX solution (example)	Manual service for the XX solution	O M service	O M service	Includes warranty, after-sales, and O&M services, such as repair, maintenance, upgrade, technical support, system operation monitoring, and data maintenance.	
			XX platform data service	XX platform data service	Analyzes and processes MCM-related data	

Figure 1-21 Example

Product or Solution Component Type ^a	Product or Scenario Component Name ^a	Feature Category-L1 ^a	Feature Category-L2 ^a	Feature Category-L3 ^a	Feature Description ^a
Product or solution software (Fill in the associated products, advanced cloud products, and partner lead solution.)	Trading system	Operation center	User management	Enterprise user management	Function and Feature Description 1
				Individual User Management	Function and Feature Description 2
			Personal Center	Login	Function and Feature Description 3
				Log Out	
				Setting basic information	
				Security Settings	
			Operation report		
			Workbench	Work management	

-
- Fill in the component feature division in columns D, E, and F. In the same column, cells with the same name are combined to facilitate identification on the Innostage workbench. For core functions in column G, partner lead venture is mandatory, corresponding to some sub-functions under level-2 functions, such as "Add" and "Delete". If there is no core function, copy the secondary function name to the core function.

Figure 1-22 Filling in columns C, D, E, and F

Product or Solution Component Type ^a	Product or Scenario Component Name ^a	Feature Category-L1 ^a	Feature Category-L2 ^a	Feature Category-L3 ^a	Feature Description ^a	Core functions ^a
Product or solution software (Fill in the associated products, advanced cloud products, and partner lead solution.)	XXX system (example)	Operation center	User management	Enterprise user management	Function and Feature Description 1	
				Individual User Management	Function and Feature Description 2	
			Personal Center	Login	Function and Feature Description 3	
				Log Out		
				Setting basic information		
				Security Settings		
			Operation report			
			Workbench	Work management		

Intelligent Finance system product function list, version number: v1.0							
Product or Solution Component Type*	Product or Scenario Component Name*	Feature Category-L1*	Feature Category-L2*	Feature Category-L3*	Feature Description*	Core functions*	
Product or solution software that in the associated products, advanced cloud products, and partner cloud solution.)	Trading system	Operation center	User management	Enterprise user management	Adding, deleting, modifying, and querying enterprise users	querying users	
						Adding user	
						Deleting user	
						Modifying user	
						Querying users	
					Individual User Management	Adding, deleting, modifying, and querying individual users	Adding user
							Deleting user
							Modifying user
					Personal Center	Log in	Log in to the system as a user
			Log Out	Log out of the system	Log out		
			Setting basic information	Set the user's nickname and gender	Set the user's nickname		
					Set the user's identifier		
			Security Settings	Set user rights and user groups	Set user rights		
					Set user groups		

- ### Figure 1-24 Self-check list

[illegible]

3. Import FunctionList&Sel-Inspection Checklist.click [Import FunctionList&Sel-Inspection Checklist]->Import template.

Function List & Self-Inspection Checklist

Solution Registration

Version Management

Function List & Self-Inspection Checklist

Architecture Design

Function List & Self-Inspection Checklist

Import Function List

Function List

Performance Self Check ▲

Reliability Self Check ▲

Enter a keyword.

+

Create Product or Solution Component Type

No data available.

Product or Solution Component Type

Enter a keyword.

Product or Solution Component Type

L1 Solution Module

L2 Primary Function

L3 Secondary Function

Feature Description

Core Function

No data available.

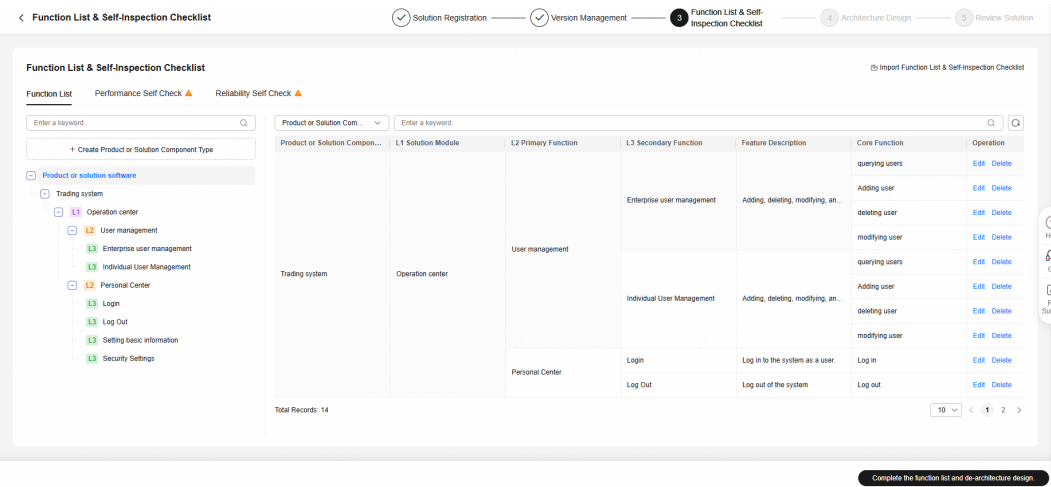
1. Ensure that the attachment does not contain non-public information assets (including but not limited to key source code, faulty code, and full set of product/platform source code), software or tools that are not authorized by the right holder, and RMS encrypted files.

2. The functional specifications included in the file must be consistent with the specifications in the specification management.

3. Upload files in xlsx format, with a file size not exceeding 20MB. Click [Download Template](#)

Import Function List & Self-Inspection Checklist

Figure 1-26 FunctionList Example



NOTE

Manual addition, deletion, and modification are also supported.

Figure 1-27 FunctionList

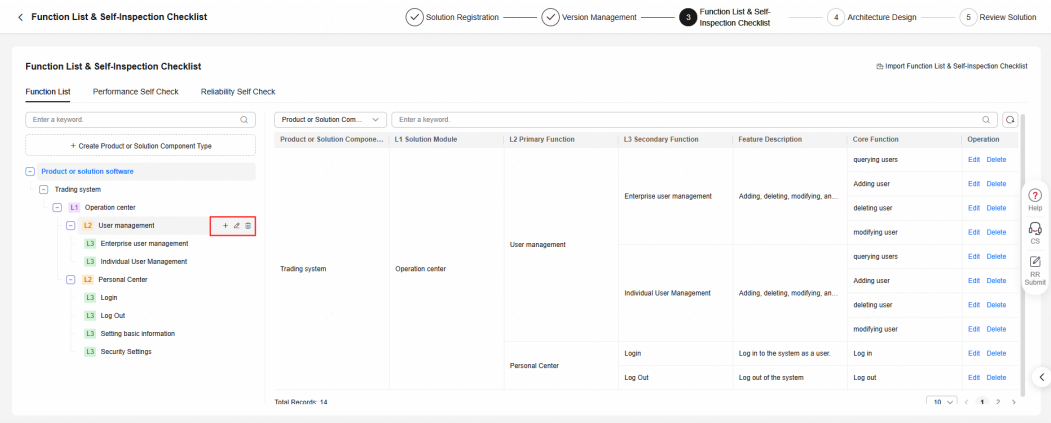
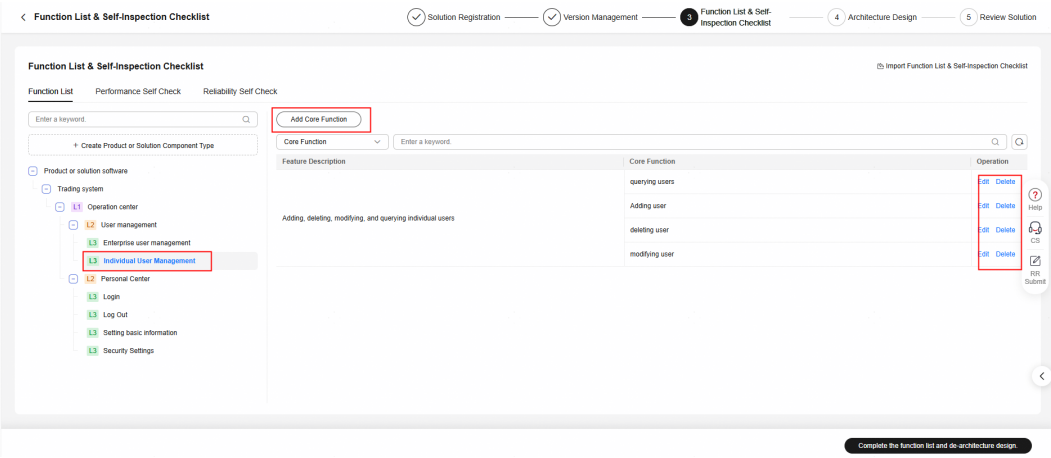


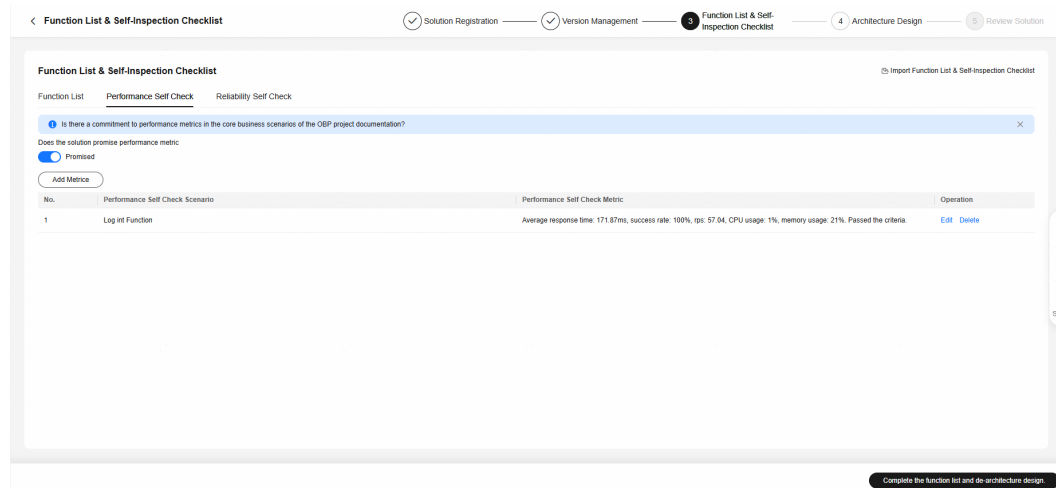
Figure 1-28 FunctionList



4. Sel-Inspection Checklist, If the self-check commitment switch is turned on, the system automatically generates performance test cases and reliability test

cases after the requirement is submitted in the verification phase. One test case is generated for each indicator.

Figure 1-29 Sel-Inspection Example



When finished, click [Complete the function list and de-architecture design].

NOTE

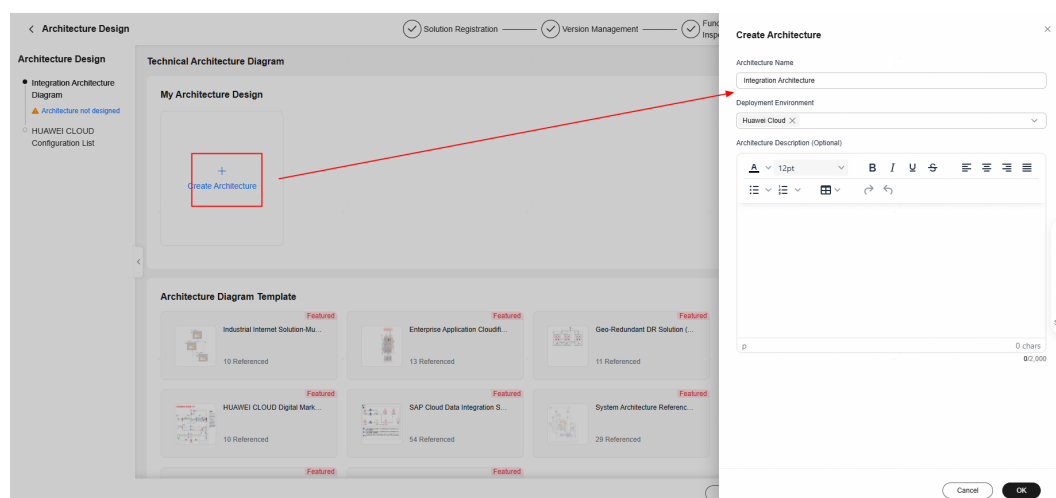
If your business does not need to test performance or reliability, close the Promised button.

Step 4 Architecture Design;

1. Integration Architecture Design.

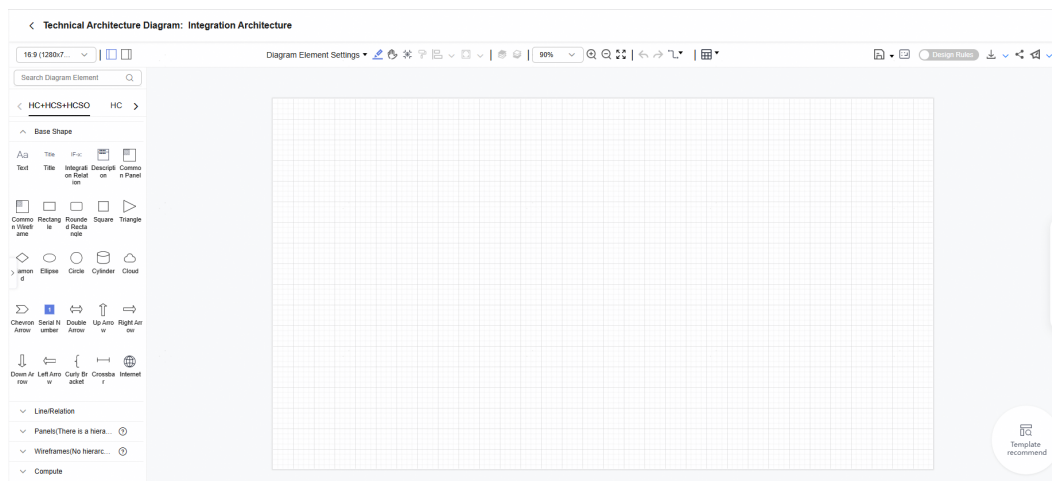
Click [Create Architecture] and enter the integration architecture name and deployment environment.

Figure 1-30 Create Architecture



Design the integration architecture in the designer. For details, see [Designing an Technical Architecture](#).

Figure 1-31 Architecture Design



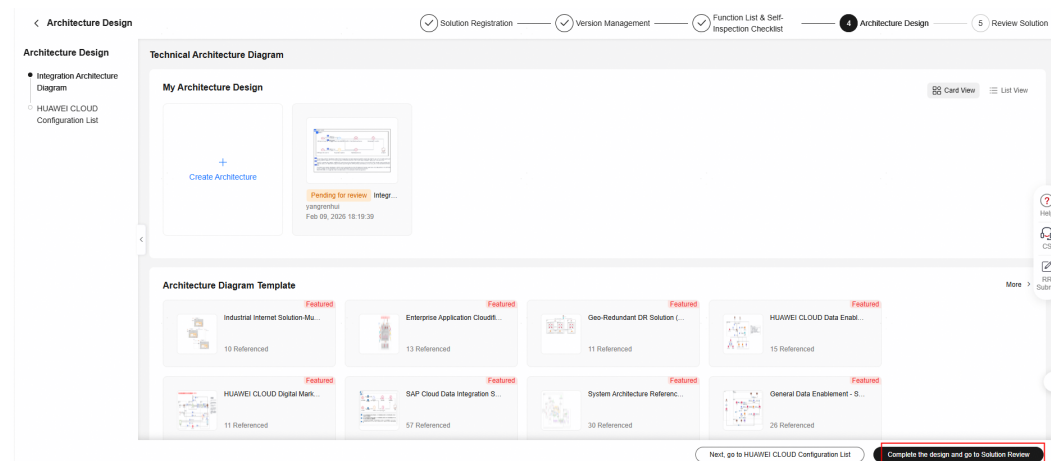
2. After the integration architecture design is complete, return to the Catalog page, select the configuration list, click [Create], and fill in the configuration list name and associated integration architecture in the dialog box that is displayed.

----End

Review Solution

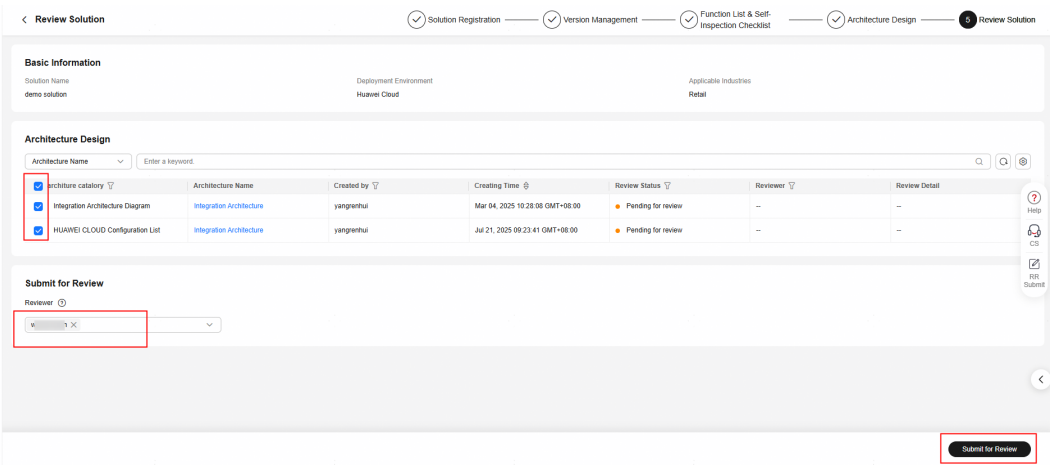
- Step 1 After completing the architecture and configuration list design, the designer clicks [Complete the design and go to Solution Review].

Figure 1-32 Design Center



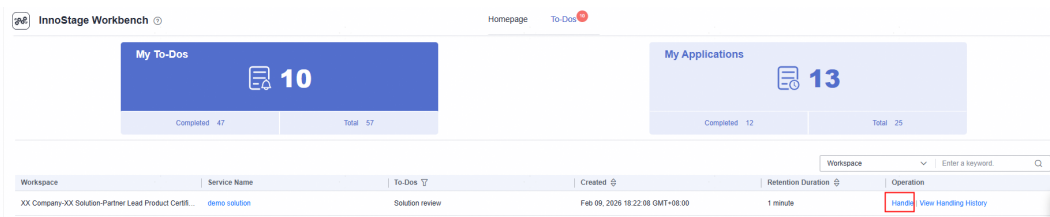
- Step 2 Select the architecture and configuration list to be reviewed, select the reviewer, and click [Submit for Review].

Figure 1-33 Review Solution



Step 3 The reviewer will generate a to-do task. Click the button of the to-do task to go to the review page.

Figure 1-34 To-Dos



Step 4 On the review page, click the [Review] button of the architecture or configuration list to review the architecture or configuration list. Select Through or Reject and click [OK.]

Figure 1-35 Review Solution

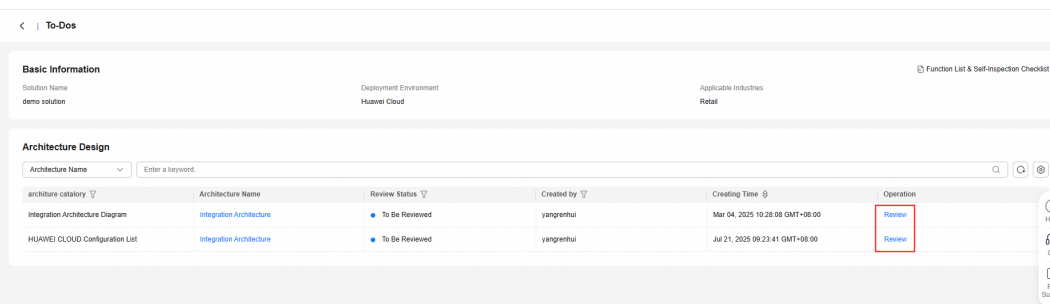
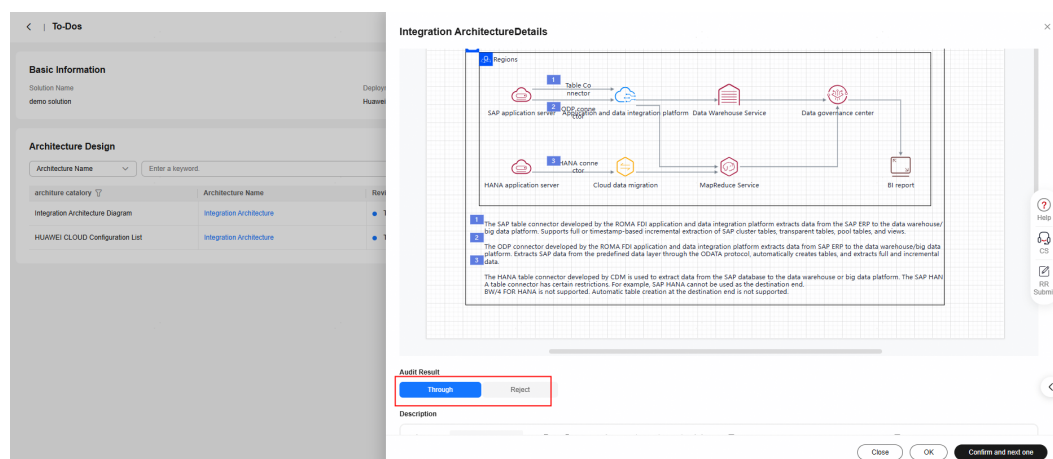


Figure 1-36 Review Solution



The rejected architecture or configuration list returns to the to-be-submitted phase. The designer modifies the rejected architecture or configuration list and submits it for review.

----End

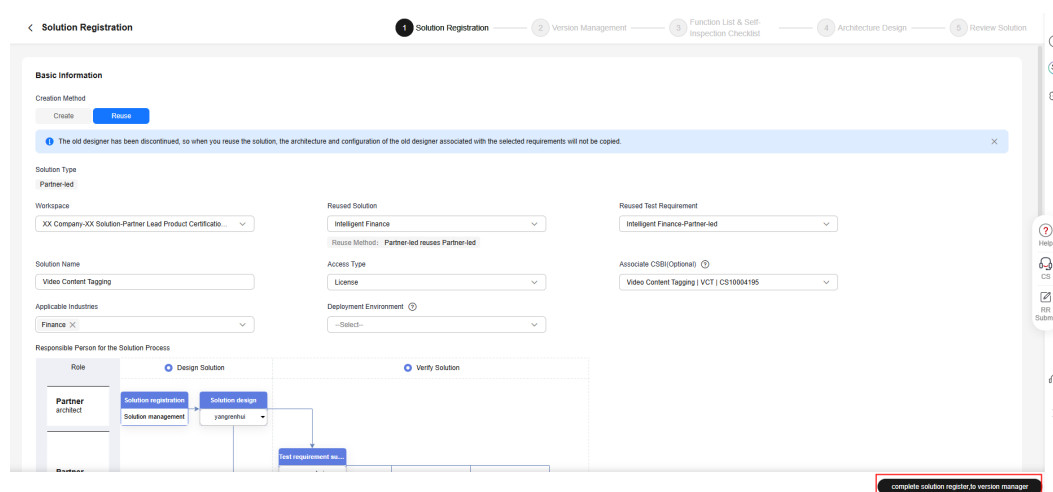
Reuse Verified Solution-Yes

NOTE

If you meet the requirements for report reuse, you can reuse historical test reports without repeated tests(only test reports of the AP-Singapore site can be reused). If the reuse conditions are not met, the reuse process is still performed. Test cases that need to be retested need be designed in the case design phase.

Step 1 If you have completed certification tests such as Joint Operation Verification or advanced cloud software on the Innostage Workbench, select Reuse and select the workspace,solution,test requirement to which the report to be reused belongs.

Figure 1-37 Reuse Verified Solution



Step 2 Fill in the solution basic info.

Information item	Description
Solution Name	If the solution name has been automatically filled in, do not modify it. If the solution name is not automatically filled in, associate it with CSBI, the solution name will be automatically filled in based on CSBI. If the project initiation has not been completed, please enter the solution name, the solution name must be consistent with the solution name in the project initiation OBP material.
Access Type	The value can be Hardware, API, Licence, SaaS.
Associate CSBI (Optional)	Associate the solution of the CSBI master data platform. The baseline solution must be initiated and associated here. If the project initiation has not been completed, you can also complete the association through the solution change function after the project initiation is completed.
Applicable Industry	Select the industry to which the product is applied. You can select multiple industries.
Deployment Environment	Set this parameter based on the actual deployment environment. The value can be HUAWEI CLOUD, HUAWEI CLOUD Stack (HCS), HUAWEI CLOUD Stack Online (HCSO), or Intelligent EdgeSite (IES)
Solution Description	Fill in the product solution description by referring to the sample text dimension. (The solution description is mandatory. Do not use the sample text directly.)

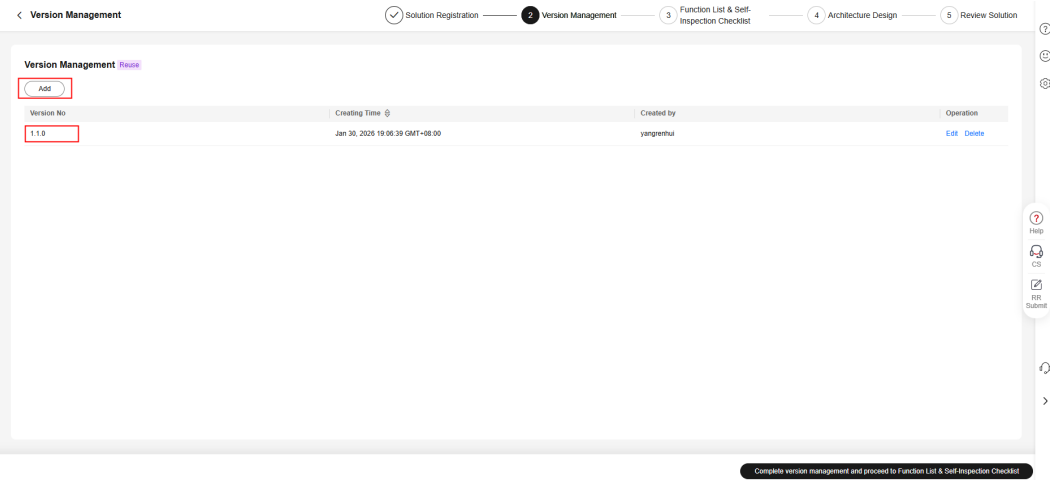
Select Node Handler.

Information item	Description	Sub-item
Solution design	The person responsible for designing the technical architecture and configuration list needs to be an architect role in the workspace to be selected.	Select a partner's architect
Solution review	Person responsible for reviewing the solution, technical architecture, and configuration list	Select the PSA and a TE that interconnects with the project.
Test requirement submission	Person responsible for editing and submitting test requirements	Select a partner's test engineer
Test case design	Person responsible for designing test cases based on service requirements.	Select a partner's test engineer
Test case execution	Person responsible for executing test cases	Select a partner's test engineer
Test requirement review	Person responsible for reviewing requirements	Select the TE that interconnects with the project.
Test case review	Person responsible for reviewing whether test cases are qualified	Select the TE that interconnects with the project.
Test report review	Person responsible for reviewing whether the test report is qualified	Select Caofeng and wujunchaun.

click[complete solution register,to version manager].

Step 3 The solution version automatically inherits the version of the reused solution. You can manually add versions.

Figure 1-38 Version Management

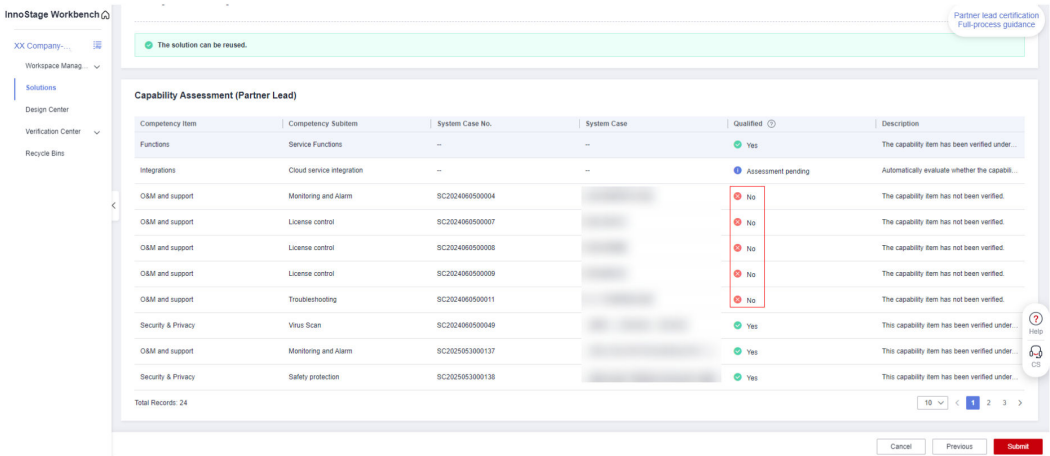


When finished, click[Complete versio management and proceed to Function List & Self-Inspection Checklist].

pection Checklist

In the "Capability Assessment" table, the column Qualified is displayed. The test case marked with Yes indicates that the test case has been executed and passed for the reused test requirement. In this case, you do not need to perform the test again. The test cases marked No are the test cases that need to be retested.

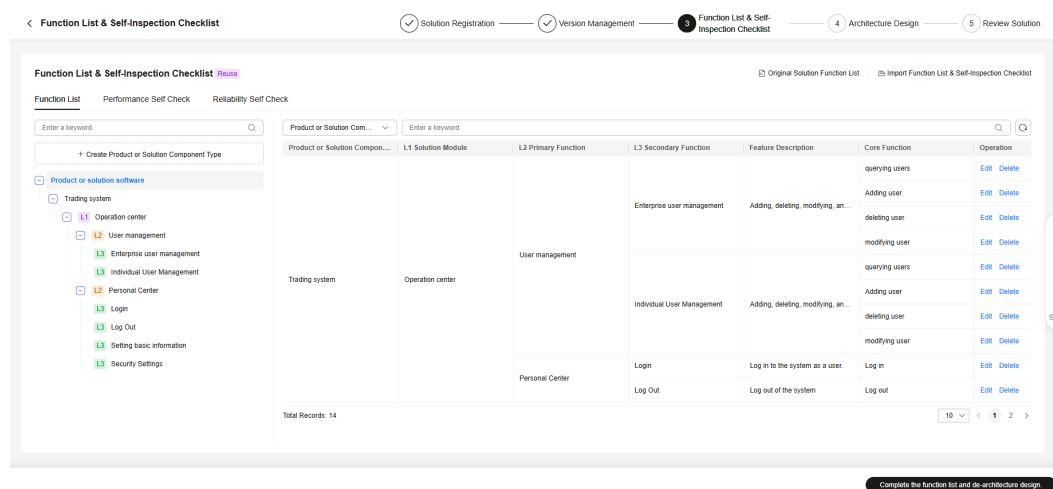
Figure 1-39 Reuse Verified Solution



NOTE

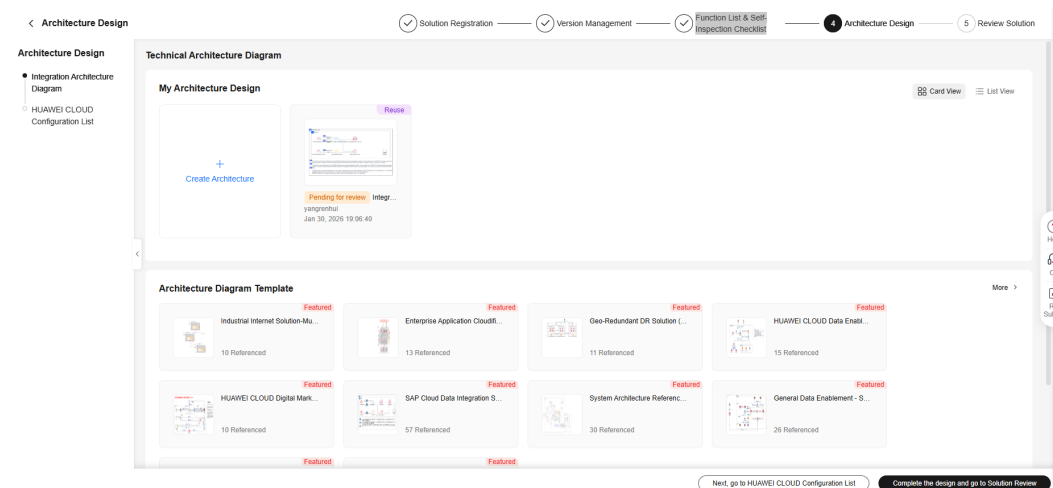
The criterion for determining whether the solution can be reused is as follows: Compare the solution architecture and function list to be reused. If the architecture is consistent and the change rate of the function list is lower than 10%, the solution can be reused.

Step 4 The new solution automatically inherits the function list of the reused solution. If the new solution requires new function modules, add new function items to the original function list. For details, seeFunction List.

Figure 1-40 Function List & Self-Inspection Checklist

When finished, click[Complete versio management and proceed to Function List & Self-Inspection Checklist].

- Step 5** The new solution automatically inherits the integration architecture and configuration list of the reused solution. If the new solution needs to modify the architecture or configuration list, modify the architecture or configuration list based on the existing architecture and configuration list. For details, see [Solution design](#).

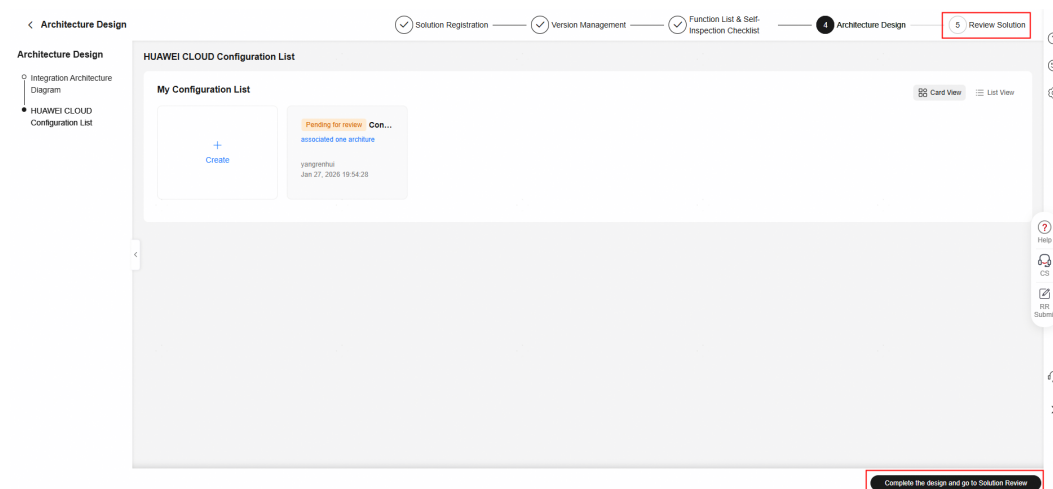
Figure 1-41 Architecture Design

When finished, click[Review Solution].

- Step 6** Submit for review.

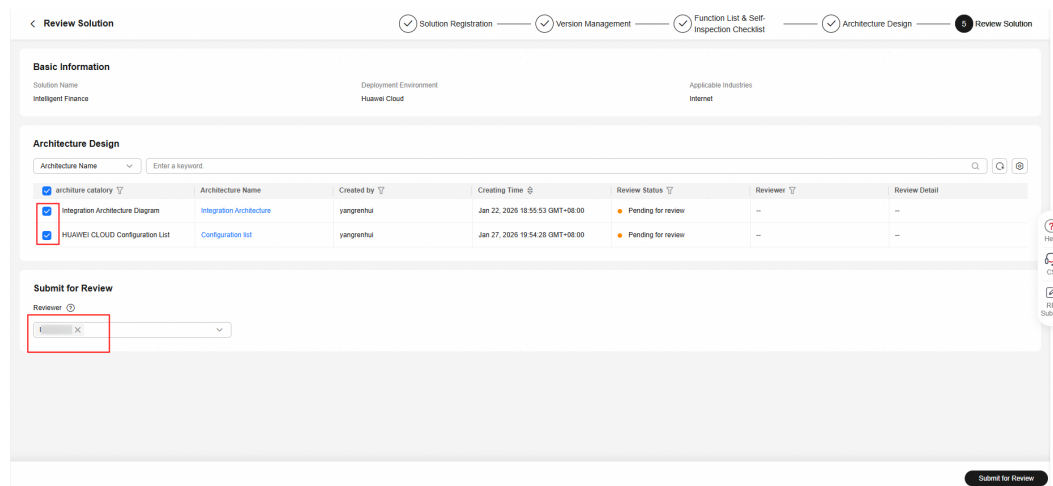
After the solution design is complete, click [Complete the design and go to Solution Review].

Figure 1-42 Review Solution



Step 7 Select the architecture to be submitted, use the default handler as the reviewer. (Huawei test engineers are required), click [Submit for Review] .

Figure 1-43 review the solution



Step 8 After the architecture is submitted, Huawei PSA and test engineers generate a to-do task. After the to-do task is approved by them, the solution phase is design completion.

Figure 1-44 to-do

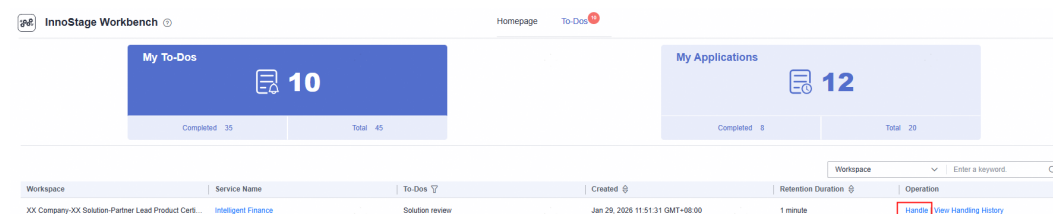
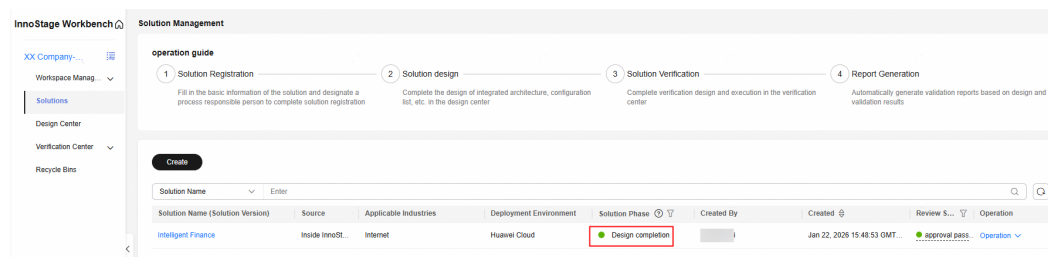


Figure 1-45 Solution Management



----End

1.2.3 Solution design

In the architecture design phase, partner architects complete the integration architecture design and resource list configuration.

NOTICE

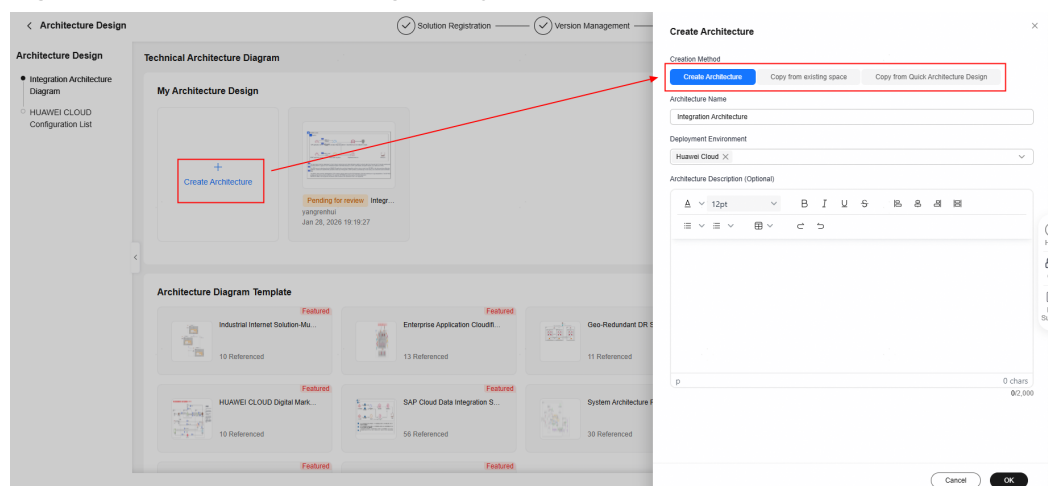
The architecture diagram must be consistent with the architecture in the OBP material.

- **Creating A Technical Architecture**

Step 1 On the Architecture Design page, click [Create Architecture].

In the displayed dialog box, new architectures can be created and existing architectures can be copied (Creating a new architecture is used as an example.) enter the architecture name, select a deployment environment, and click [OK].

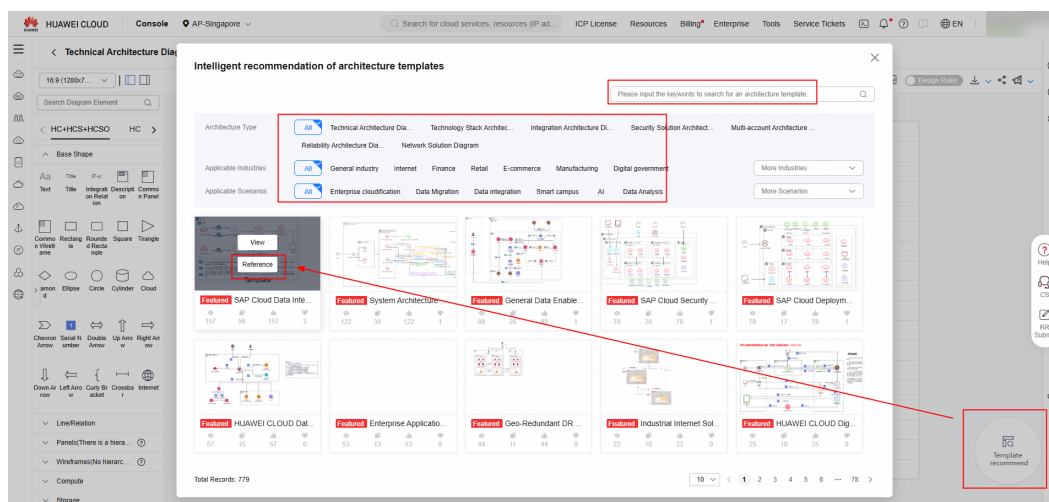
Figure 1-46 Architecture Design Entry



Step 2 Design architecture

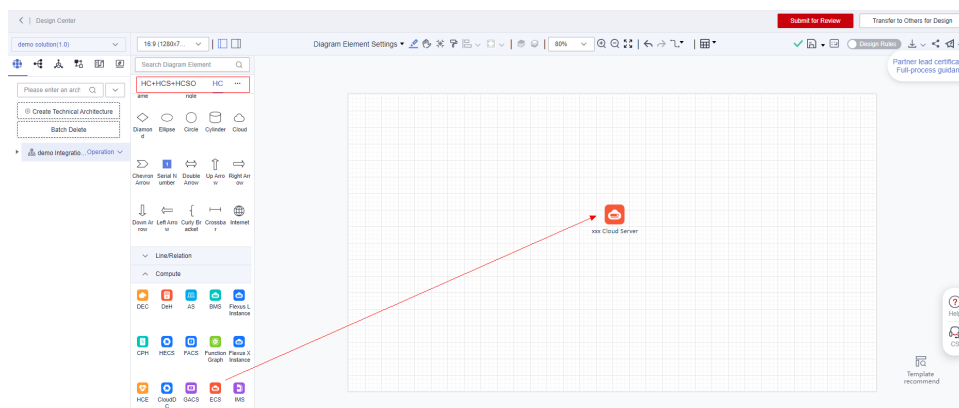
- **Template recommend:** Click [Template Recommendation]. A dialog box is displayed. In the dialog box, you can search for or filter architecture templates. After finding the schema template, click [Reference Template] to load the template to the canvas.

Figure 1-47 Design Architecture



- **Drag diagram elements:** select a diagram element in the diagram element library, and then drag the diagram element to the canvas (The deployment environment can be switched on the element library).

Figure 1-48 Drag Diagram Elements



- **Diagram element association:** move the cursor to a diagram element (without clicking it). Connection anchor points are displayed around the diagram element. Select an anchor point, hold down the left mouse button, and drag it to another diagram element anchor point to complete the connection.

Figure 1-49 Diagram Element Association

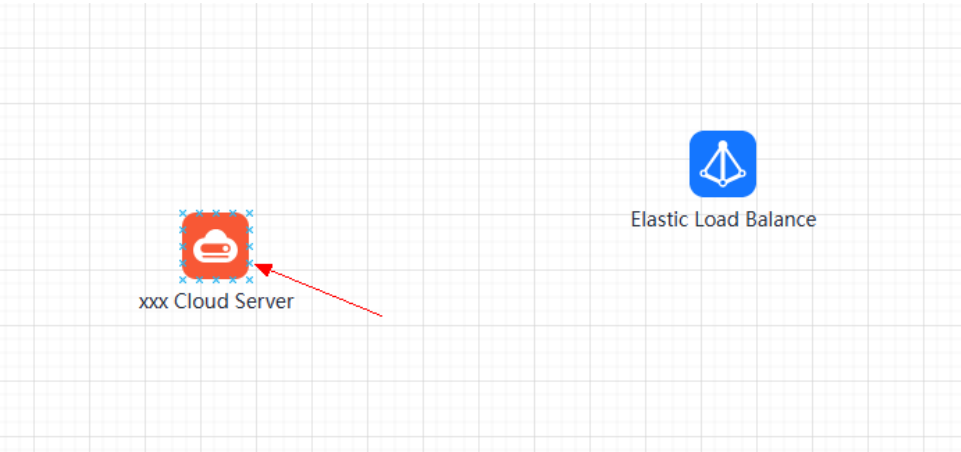
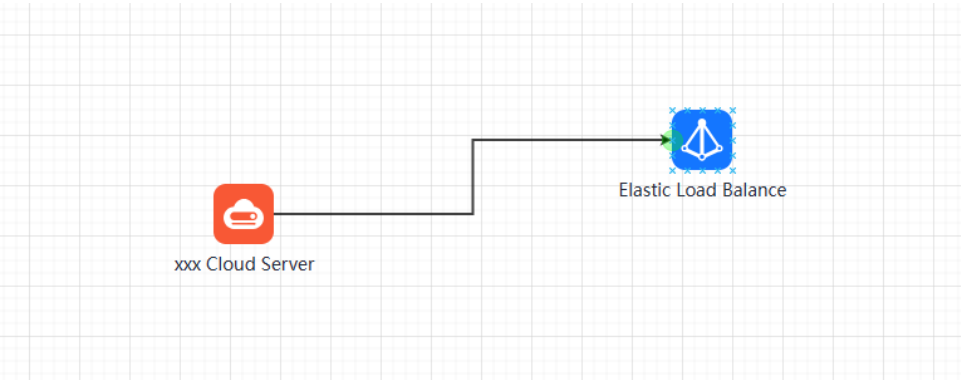
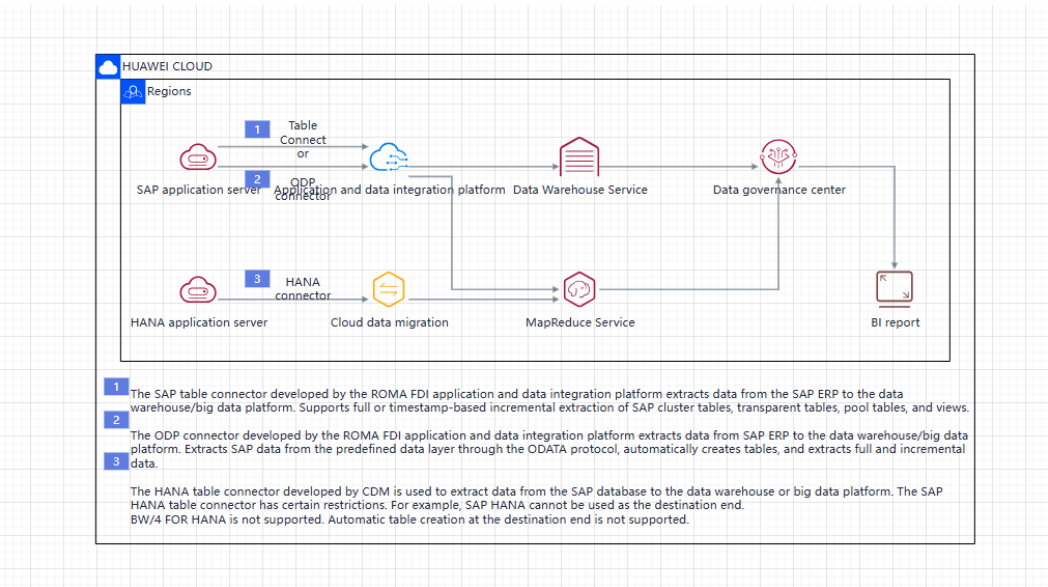


Figure 1-50 Design Center



----End

Figure 1-51 A Final Example Architecture Diagram

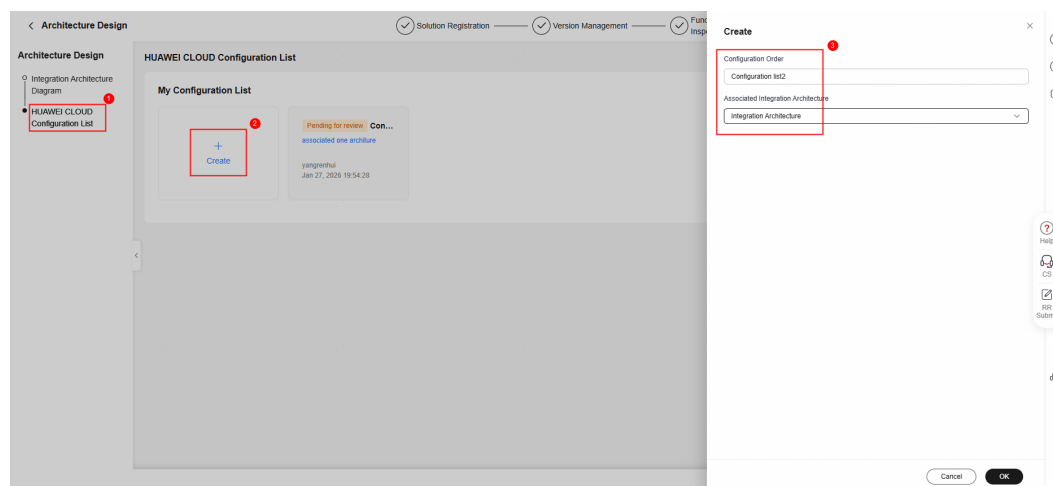


● Design The Configuration List

During subsequent verification tests, the system will automatically identify cloud services in the configuration list and generate required integration cases.

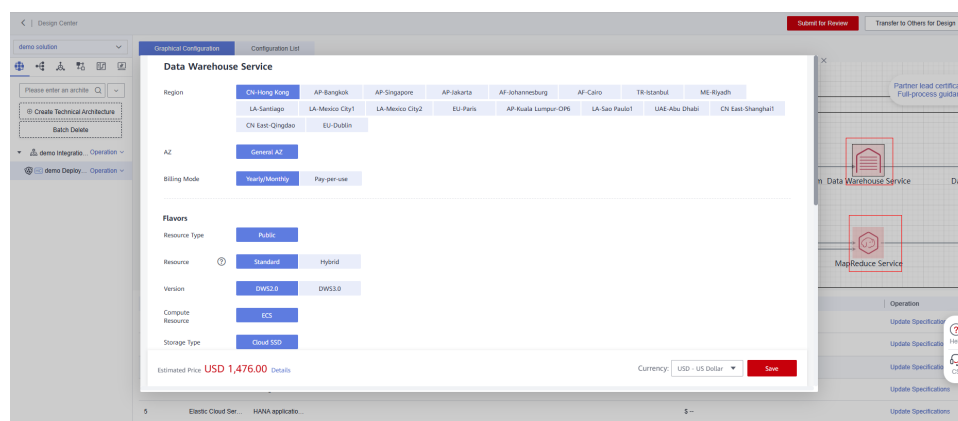
- Step 1** After the integration architecture design is complete, return to the architecture design page. Select the configuration list and click [New]. In the dialog box that is displayed, enter the configuration list name and select the associated integration architecture.

Figure 1-52 Design Center



- Step 2** Click a diagram element in the deployment architecture canvas, the Price Calculator dialog box is displayed. Select the specifications and click [Save].

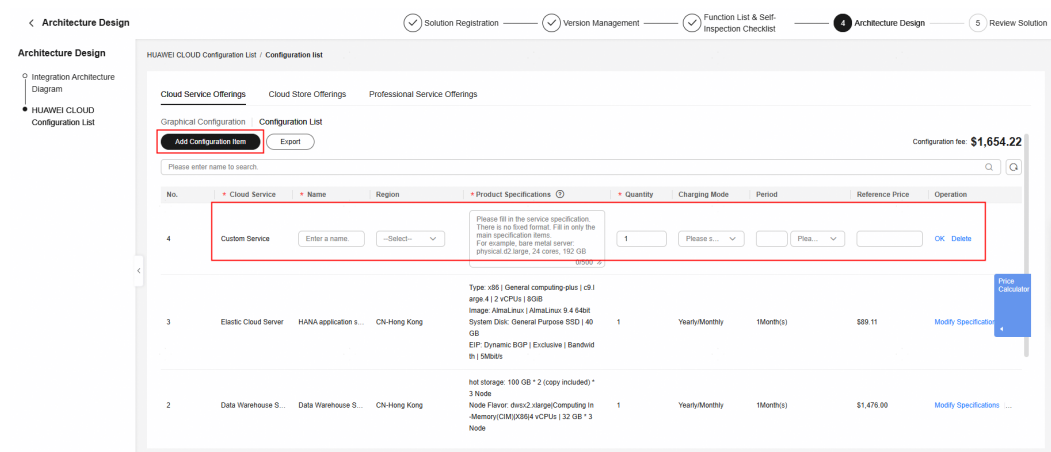
Figure 1-53 Deployment Architecture



- Step 3** Click the [Configuration list] to view the saved configuration specifications.

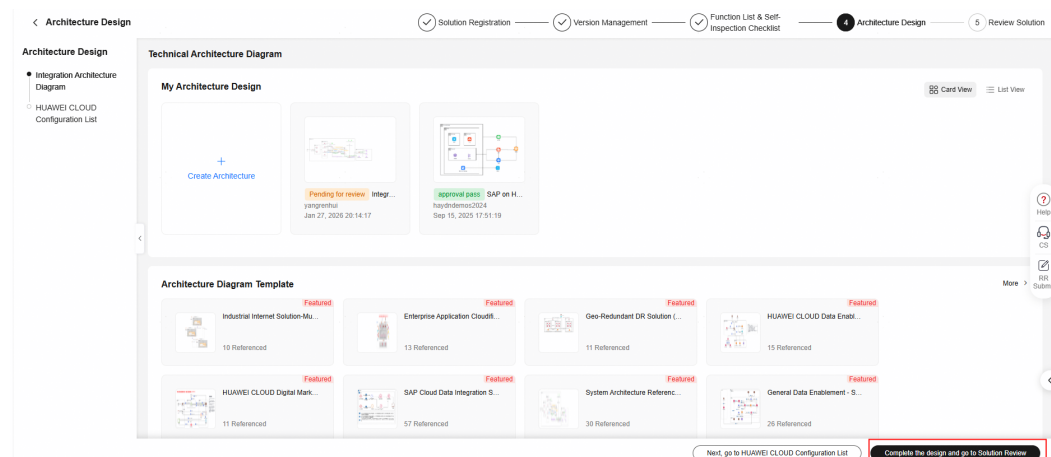
If the service does not support the price calculator, click [Add Configuration Item], select a custom service and manually enter the configuration.

Figure 1-54 Configuration List



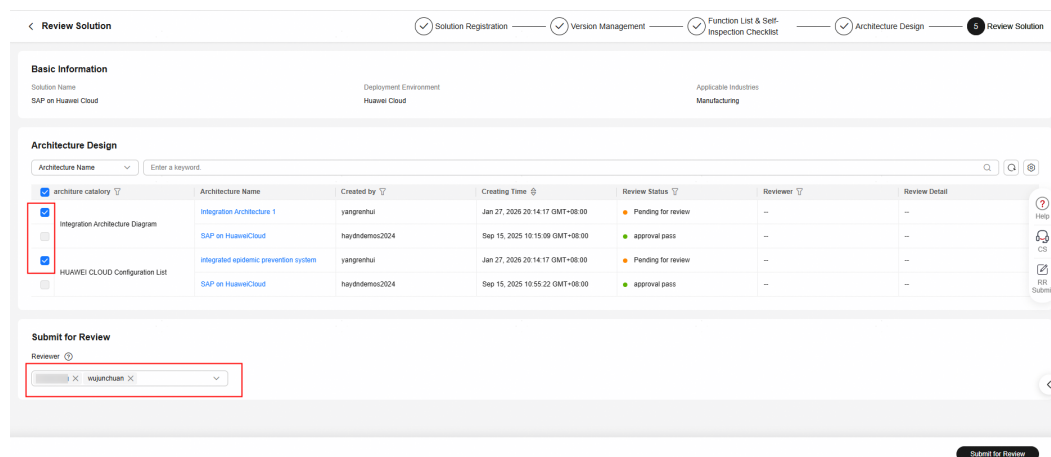
Step 4 After the design is complete, click [Complete the design and go to Solution Review].

Figure 1-55 Complete the design and go to Solution Review



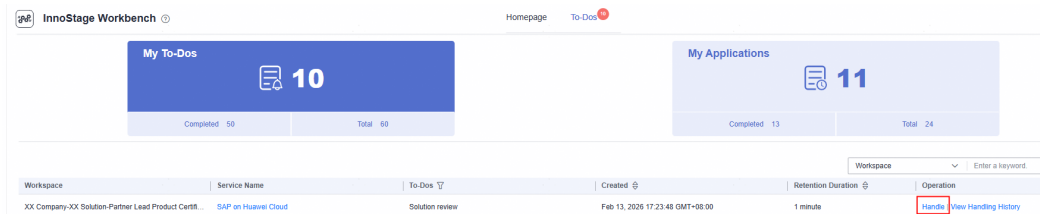
Step 5 Select the architecture and configuration list to be submitted for review, select the default approver, and click [Submit for Review].

Figure 1-56



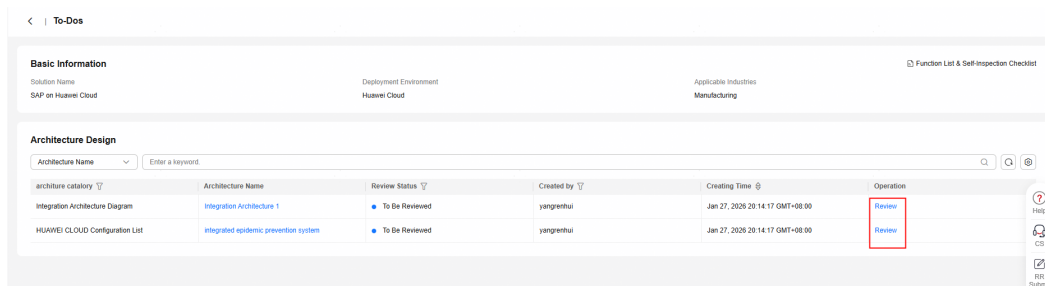
Step 6 The reviewer generates a to-do task. Click the [Handle] button to go to the review page.

Figure 1-57 to-do



Step 7 The reviewer clicks the [Review] button of the architecture and configuration list to review the architecture and configuration list. If the architecture is rejected, the architecture returns to the to-be-submitted phase and needs to be modified and submitted for review again.

Figure 1-58 Review



NOTE

There is no charge for generating Configuration list, but for configuring specifications and generating reference prices.

----End

1.2.4 Test Requirements Submission

The partner's test engineer submits the test requirement.

After the solution is approved, the partner's test engineer can access the workspace and click [Requirement Management.] Once the solution review is passed, a requirement will be automatically created. You can directly click [Enter Verification] on this requirement to complete the requirement details. Alternatively, you can click the [Create] button in the upper left corner to create a new requirement. For certification test requirements, please refer to [HUAWEI CLOUD Certification Test Contents And Requirements](#) .

NOTE

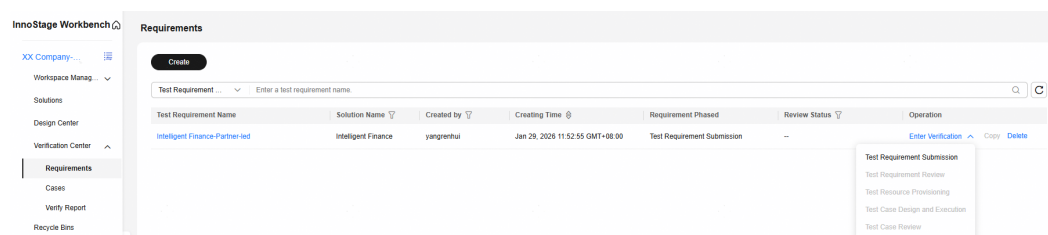
If the solution is reused, requirements and test cases will be copied. You only need to check whether requirement items and test cases need to be added based on the actual scenario. The operation process is the same as that of the non-reuse process.

test requirement submission

Step 1 Click [Enter Verification] and then [Test Requirement Submit] to access the test requirement page.

This section uses the example of editing an automatically created requirement.

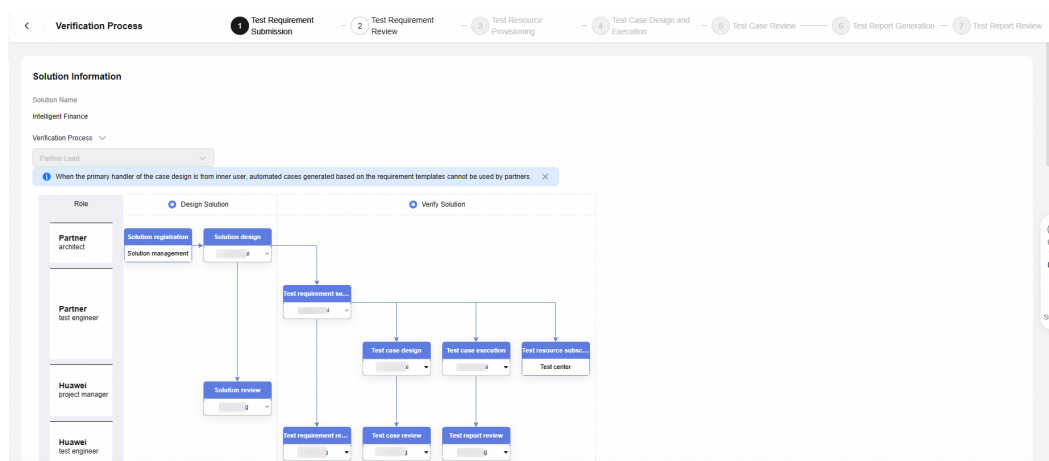
Figure 1-59 Requirements



Step 2 Check and fill in the requirement information.

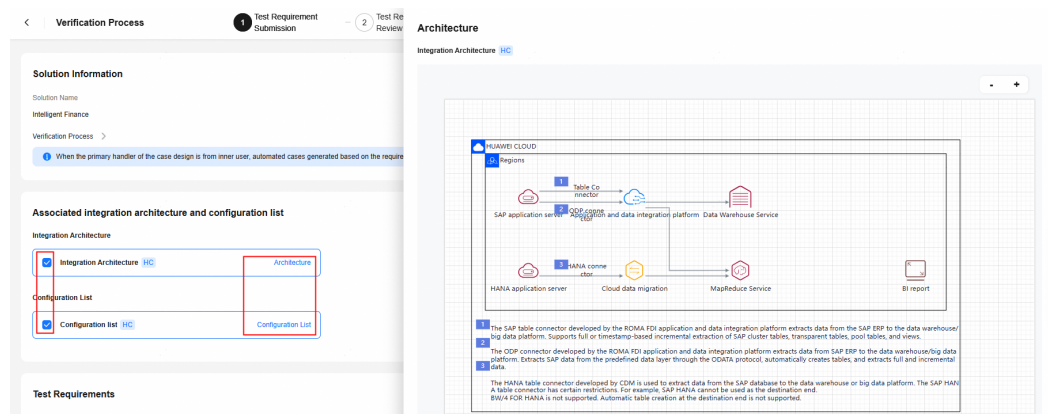
- Solution name: The solution name is automatically associated with the solution name created earlier and cannot be modified.
- Verification process type: The process based on the solution type. cannot be modified.
- Flowchart: You can change the owner of the process after "Test requirement creation." If the owner does not need to be changed, you do not need to modify the process.

Figure 1-60 Submit Test Requirement(solution info)



Step 3 Associate the integration architecture and configuration list.

- If there are multiple integration architectures, you can associate them at this step.
- Click [Architecture] or [Configuration List] to view details.

Figure 1-61 Submit Test Requirement(integration architecture and configuration list)**Step 4** Test requirement.

- Test requirement name: can be customized.
- Test requirement type: Security test, integration test, and function test are mandatory, while performance test and reliability test are optional. You can delete the test requirement types that are not involved, System corresponding test cases are generated based on the test requirement type.

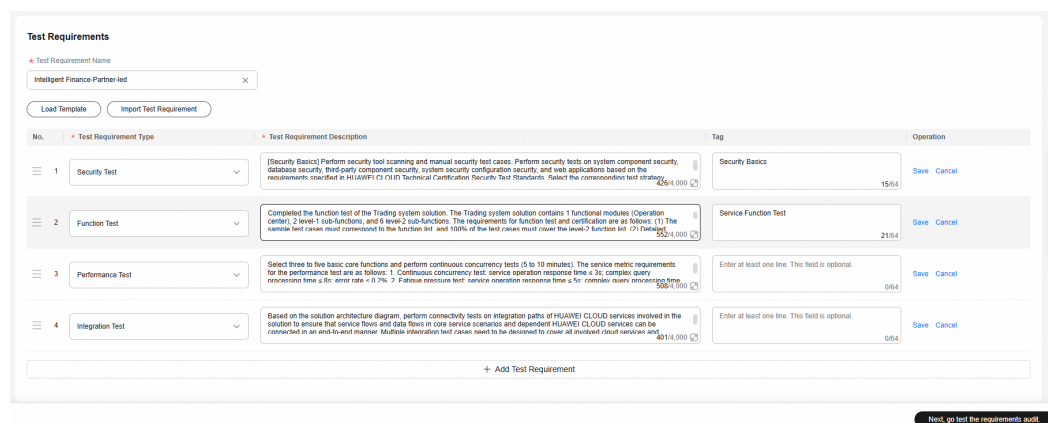
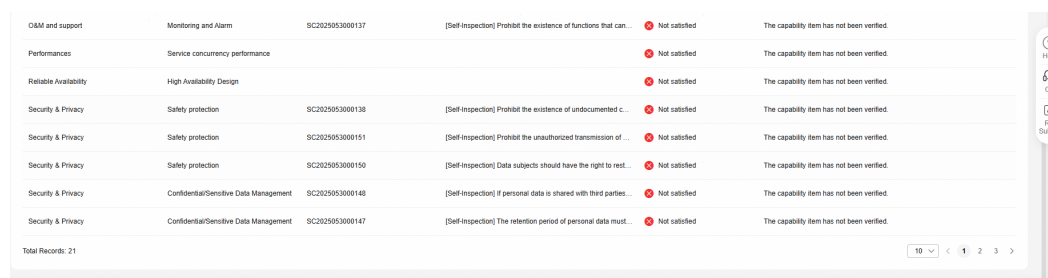
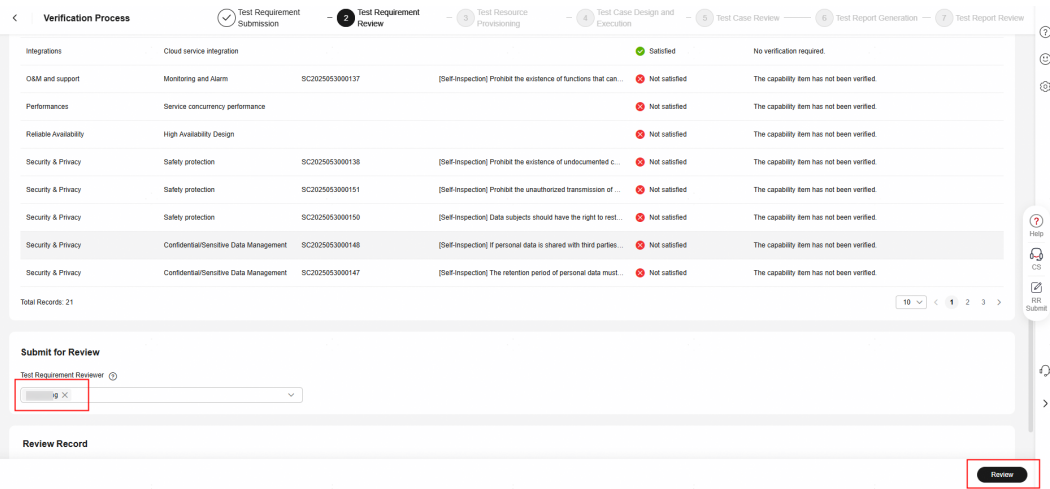
Figure 1-62 Submit Test Requirement**Step 5** Click [Next, go test the requirements audit.], Review Test Requirement to submit the test requirement for review.**Figure 1-63** Go Test the Requirements Audit

Figure 1-64 Review



----End

Reviewing test requirements

Huawei Cloud test engineers review the test requirements submitted by partners. Find the review to-do task and click [Handle]. The review page is displayed.

Figure 1-65 To-Do

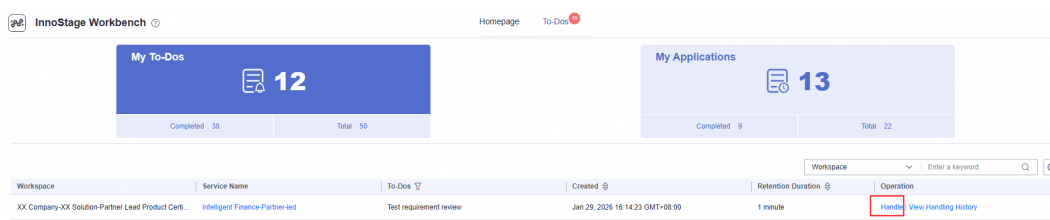
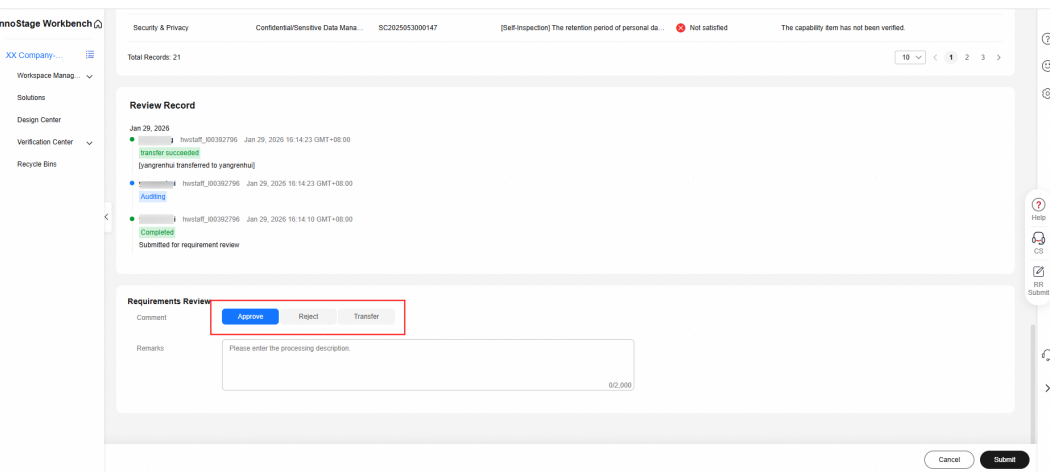


Figure 1-66 Review Test Requirements



NOTE

Test Resource Provisioning,Test Case Design and Test Case Execution are not in sequence.

1.2.5 Test Cases Design

The partner's test engineers design test cases.

NOTE

Security scanning cases can use third-party tools or the security scanning function provided by InnoStage Workbench.

The security automation function of InnoStage Workbench (includes web automated scanning and binary automated scanning) depends on the capabilities of the VSS cloud service on the China website. Therefore, the security scanning data is sent to the China website. We will perform the following operations to ensure your data security:

1. Encrypt your data during transmission.
2. Encrypt your sensitive data during scanning.
3. Destroy your data periodically after the scan is complete.

You can also use a third-party test tool. we provides the third-party test tool guide is provided later.

After the test requirement is submitted, the system automatically generates security test cases and performance test cases based on the test case template, and generates function test cases and integration test cases based on the function list and architecture.

NOTE

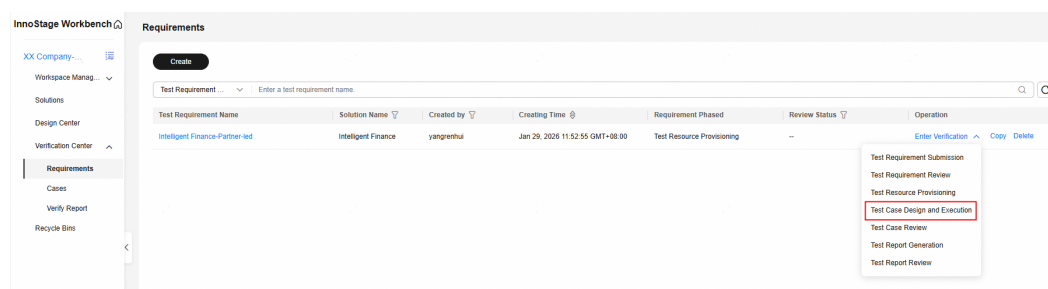
- If a requirement is reused, all the test cases of the reused requirement are inherited, and the inherited test cases do not need to be modified. If new test cases are added for new requirements, handle the new test cases by referring to this topic.
- If the function list is changed compared with the reused solution, function cases are loaded, you need to perform a virus scanning test again. For details, contact Huawei test engineers.

wujunchuan:wujunchuan@huawei-partners.com

caofeng:caofeng24@h-partners.com

Step 1 In the test requirement module, click the [Test Case Design and Execution] to enter the test case and design.

Figure 1-67 Test Case Design and Execution



Step 2 The "Case Management" page will be displayed. On this page, you can perform operations such as creating, modifying, executing, and deleting test cases.

NOTE

The system has generated test cases based on the solution information and requirement template. The test cases are designed based on your actual situation.

[Create]: You can create new test cases.

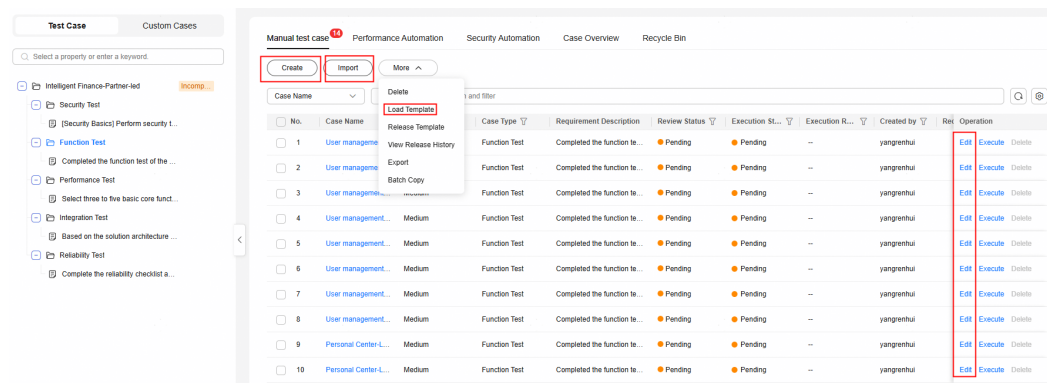
[Import]: You can fill in the Excel test case template and then import the test cases.

[Loading Templates]: You can load test cases in a test case template in batches.

[Edit]: You can edit and modify the test case content. Security test cases are A1 test cases provided by Huawei and cannot be edited or modified.

[Execute]: Click Execute to execute the test case and change the execution status of the test case.

Figure 1-68 Case Management

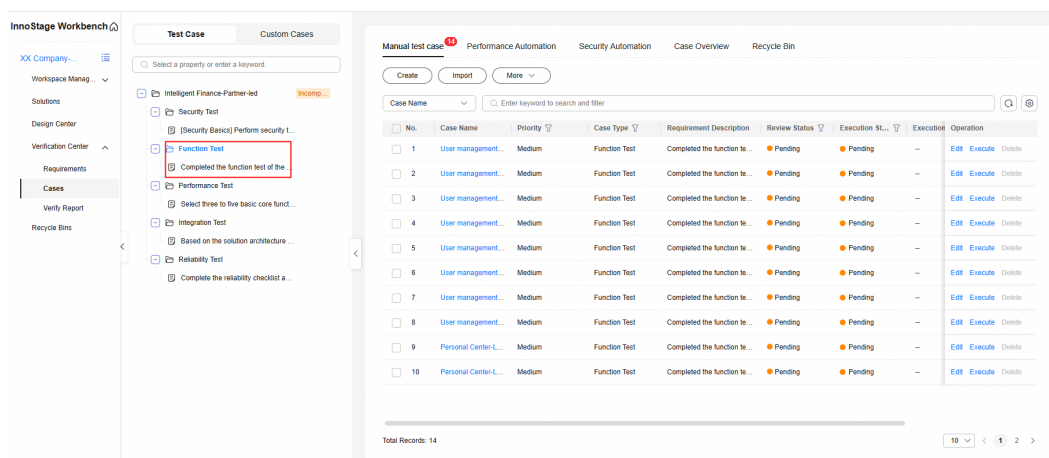


----End

Design Function Cases

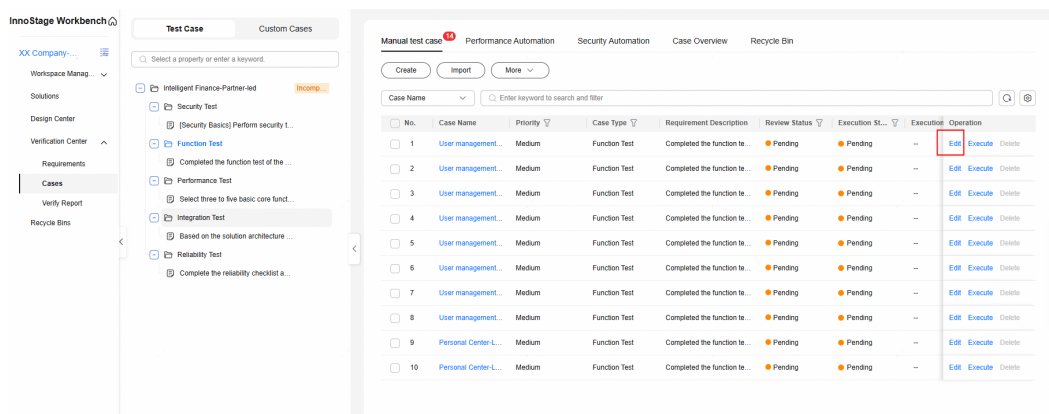
1. Click [Function Test] to view the names of function test cases automatically generated based on the function list uploaded during the solution creation phase.

Figure 1-69 Function Test



2. Currently, only the names of service function test cases are generated. You need to click the [Edit] button on the right of each service function to complete the prerequisites, procedure, and expected result of the test case.

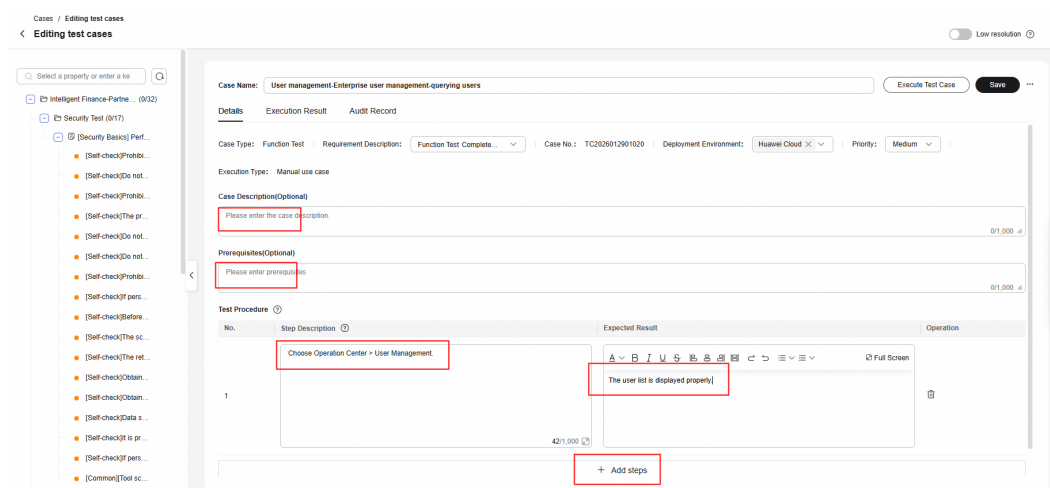
Figure 1-70 Edit Function Test Case



3. Edit function test case

- The page for editing test cases is displayed. On this page, the case description and prerequisites are optional.
- enter the first step of the test procedure in the input box under "Step Description"; then, in the input box below "Expected Result" on the right side of the operation steps, enter the expected result corresponding to the first step.
- If there are multiple operation steps, click the [Add] button below to customize the number of operation steps you need to add, and then complete the remaining operation steps and their corresponding expected results, forming an end-to-end scenario
- After editing, click [Save].

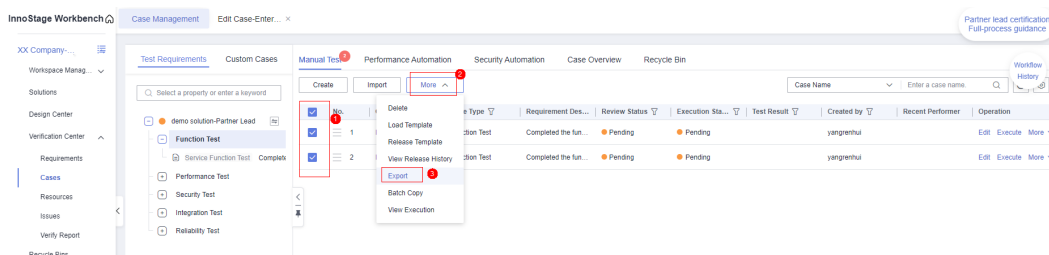
Figure 1-71



If there are a large number of function test cases, you can import test cases in batches to edit them in batches.

1. Select function cases, click [Export], Export the generated test case information..

Figure 1-72 Export Test Case



2. Enter the step description and expected result in the exported file.

Figure 1-73 Enter Exported File

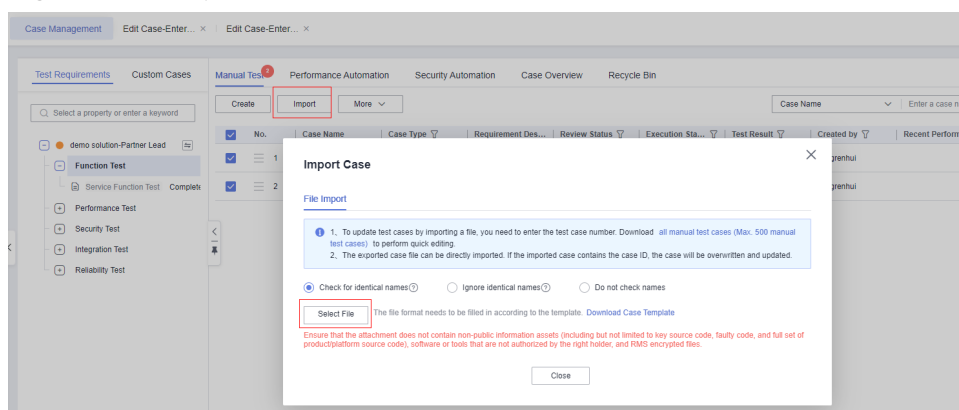
Test Case Priority	Pre-conditions	Latest Test Result	Latest Executor	Creation Time	Execution Status	Step 1 Description	Step 1 Expected Result	Step 2 Description	Step 2 Expected Result	Step 3 Description	Step 3 Expected Result	Step 4 Description
Medium	You have login			2025-07-22 17:17	Pending	Click User Management All interfaces are correct and the role is set successfully.						
Medium				2025-07-22 15:15	Pending	Click User Management Succeeded in adding the list view account.						

NOTICE

- Enter the test case information based on the remarks in the test case template.
- Cells without contents cannot contain spaces or newline characters.
- After filling in the test case information, delete the three lines in red. If the three lines are not deleted, a message will be displayed indicating that the three lines fail to be verified during the import. However, the test cases will still be imported.

3. On the Case Management page, click [Import] and [select file] to import the case in batches. The system updates test case steps in batches.

Figure 1-74 Import Case

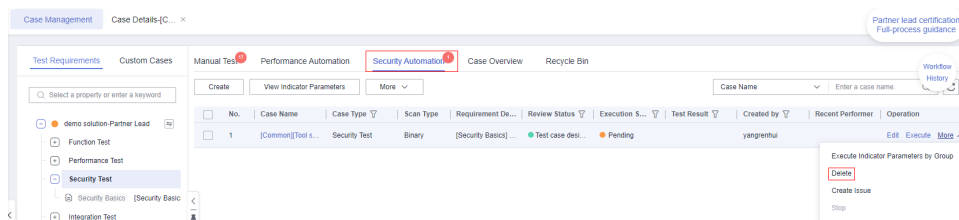


Design security cases

Security manual test cases do not need to be edited.

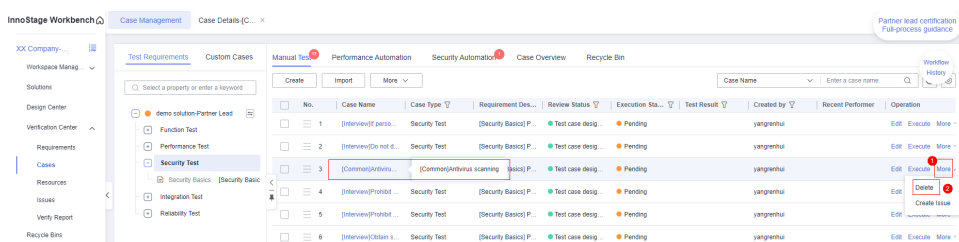
- If you use third-party tool to scan binary viruses, retain the manual scanning case and delete the binary scanning cases in security automation.

Figure 1-75 Case Management



- If you use the security scanning function provided by InnoStage Workbench to scan the binary viruses (vulnerabilities and viruses can be scanned at a time), retain the binary scanning case in security automation and delete the manual scanning case.

Figure 1-76 Case Management



Design reliability test cases.(Optional)

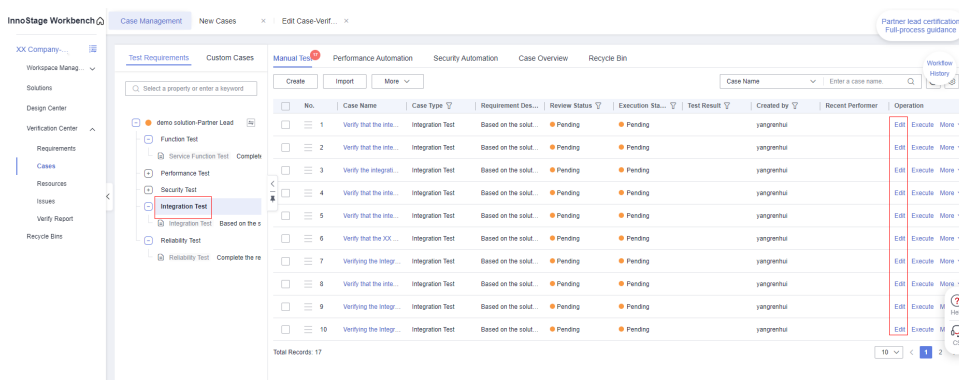
If there are reliability indicators in the function list, the system generates reliability test cases. In this case, you need to design reliability test cases based on the reliability indicators in the function list. For details, see [Design Function Cases](#).

Design Integration Cases

The system has automatically generated integration cases. You need to edit the case and replace "xx" in the case with the actual service information.

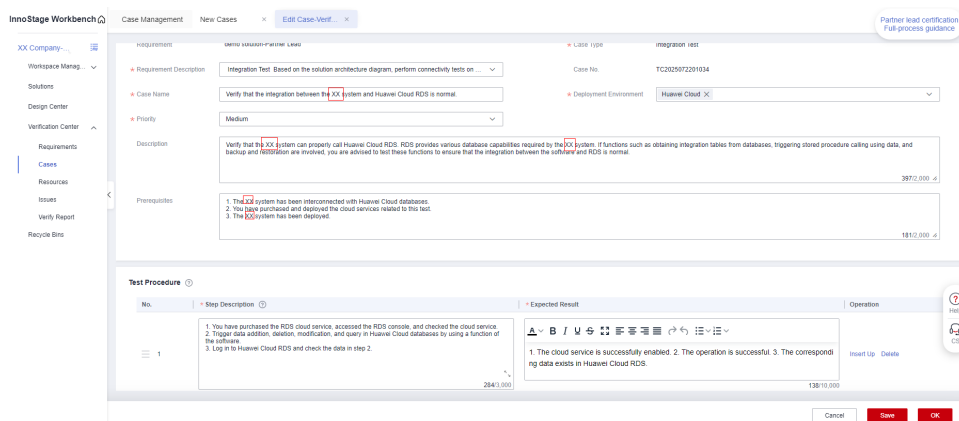
1. Select the integration test requirement and click the [Edit] button of the integration test cases.

Figure 1-77 Test Case Management



2. Replace "xx" in the case with the actual service information.

Figure 1-78 Edit Test Case

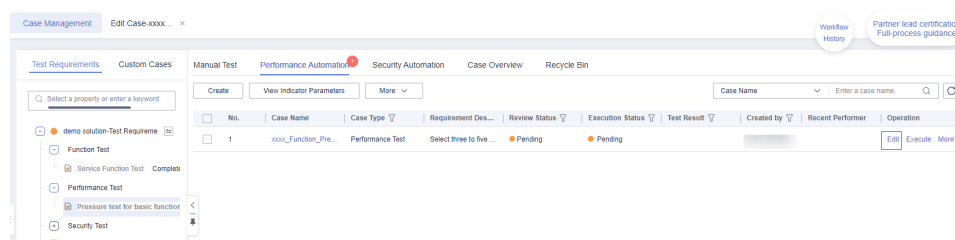


Design Performance Cases(Optional)

performance case is loaded from the case template when requirement is created. You can create more performance automation cases based on actual requirements.

1. Choose [Performance Automation]->Click [Edit] on the right of the performance automation case.

Figure 1-79 Test case management



2. Go to the test case information page. Generally, you only need to modify the following basic information and retain the default values for other information:

- Case name: the default value is xx function point pressure test, as shown in the following figure. You need to change the placeholder xx to the name of the interface to be tested.
- Description: as shown in the following figure, the default value is "xx users concurrently perform xx functions for 5 minutes". You need to change the first placeholder xx to the number of concurrent interface pressure tests. Change the second placeholder xx to the name of the interface to be tested.

Figure 1-80 Editing test cases

NOTE

You need to select a concurrency value that matches the cloud service specifications based on the specifications of the cloud service resources purchased in this test.

NOTE

- If you use a third-party pressure test tool, delete automatic performance test cases and create manual performance test cases. If you have any questions, contact Huawei test engineers.

After all test cases are designed, click [Submit Case Design] . After the design is submitted, a to-do task is generated for the test case reviewer.If you do not select any test case, all test cases are submitted.

Figure 1-81 Submit Case Design

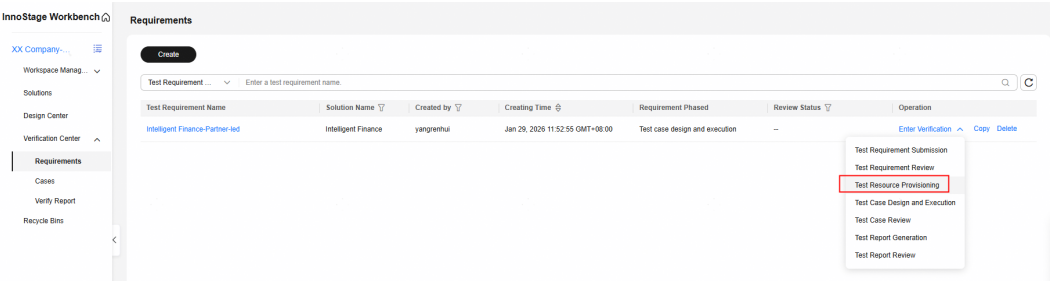
1.2.6 Provision Test Resources

Provision resources does not purchase and deploy resources on the Innostage workbench. Instead, users purchase resources and record them on the Innostage workbench. The records will be displayed in the test report later.

The partner's test engineer provision test resources.

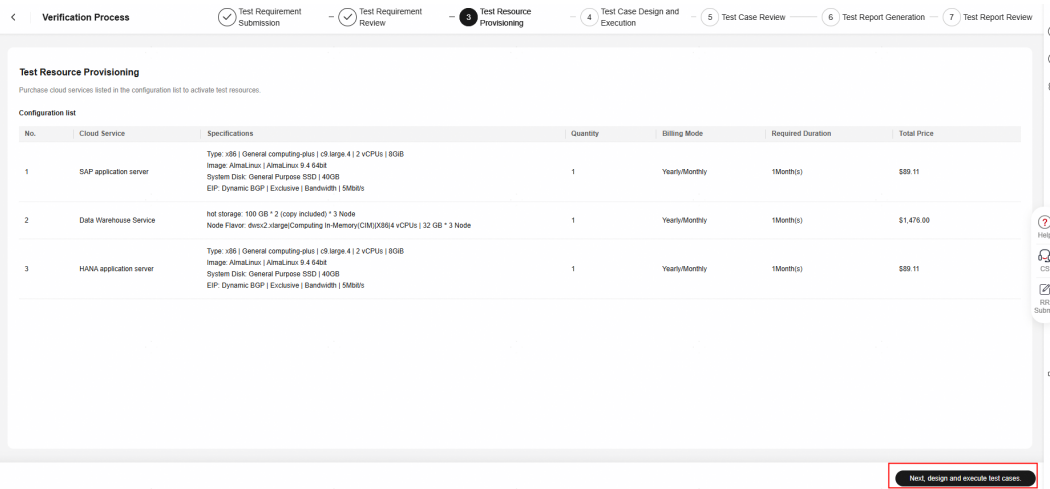
- Step 1** The resource provisioning handler click the [Enter verification] button corresponding to the test requirement and select [Test Resource Provisioning].

Figure 1-82 Resource Management



Step 2 Check that the configuration list is correct and click[Next,design and execution test case].

Figure 1-83 Resource Management



----End

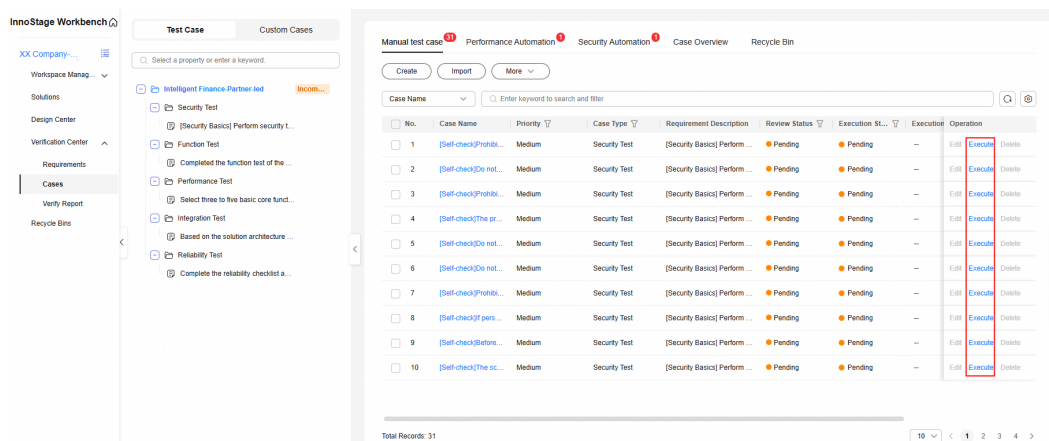
1.2.7 Test Case Execution

All test cases are required to pass the execution.
The partner's test engineer Execute test cases.

Manual case execution

- 1. The specified partner test case executor click the [Execute] button of the manual case.

Figure 1-84 Case Management

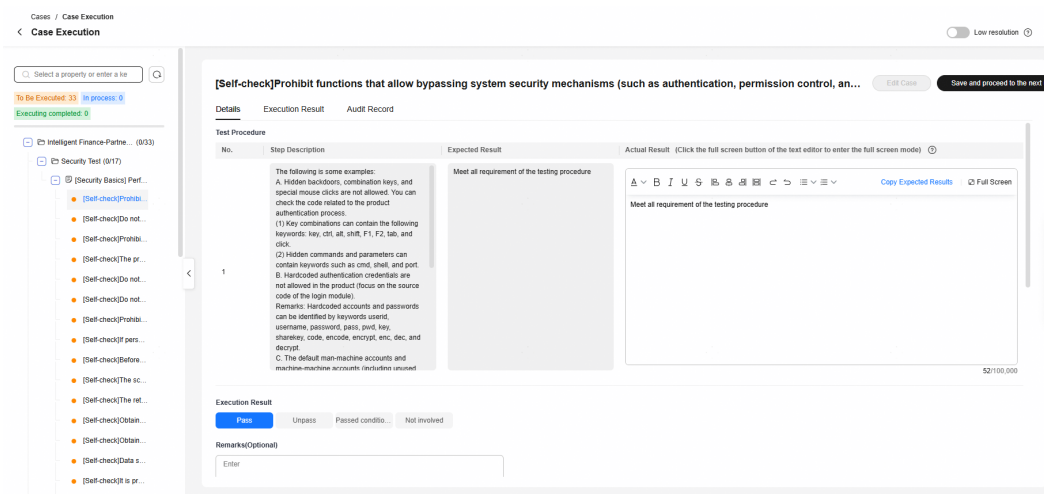


2. Complete the test case operations according to the test case steps, fill in the actual result, and determine whether the test case is passed based on the expected result.

Table 1-2 Test case execution information

Information item	Description
Actual Results	The text description is usually a description of the screenshot. Screenshots are not required for "self-check" cases and cases where the execution result is "N/A". You can directly paste screenshots into the text box of "Actual result". Please provide screenshots according to the case steps. The screenshot must be a full screen screenshot, including the function menu and system time in the lower right corner. If there is sensitive information, the sensitive information can be desensitized. (If the screenshot is saved to another document and copied to the actual result, it may be incompatible.)
Case Status	● Pending:the execution has not started. ● Executing:the execution is in progress. The execution is not complete. ● Completed:the execution is complete.
Execution result	● Failed:the actual structure does not meet the expected result. ● Pass:the actual structure meets the expectation. ● Pass conditionally:actual results do not fully match expected results, which can be ignored after confirmation with Huawei test engineers. ● N/A:the software does not have the functions described in the test case.
Attachments	File that describes the execution result.(optional)

Figure 1-85 Case Execution

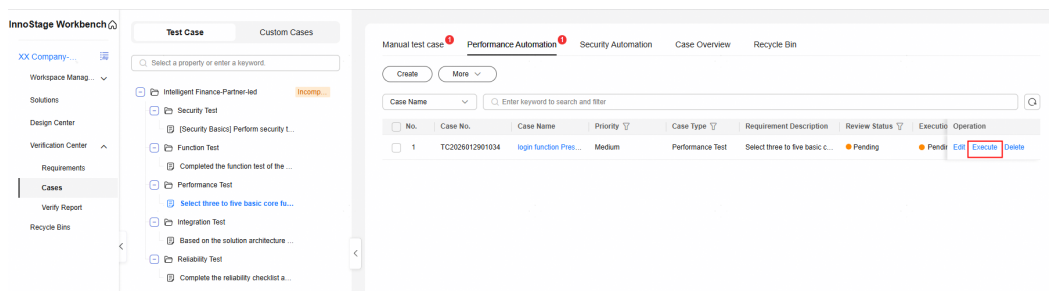


3. Click [Confirm Go to Next] or [OK].

Performance automation case execution

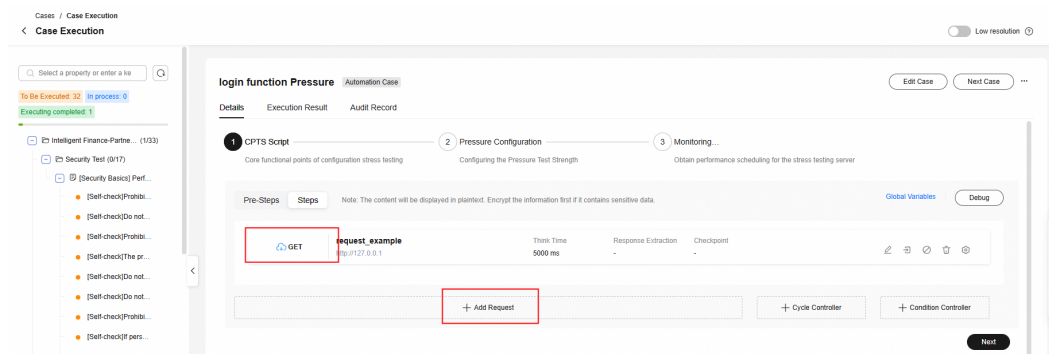
1. The test case executor accesses the test case management page and clicks the [execution] button of the performance test case.

Figure 1-86 Test Case Management



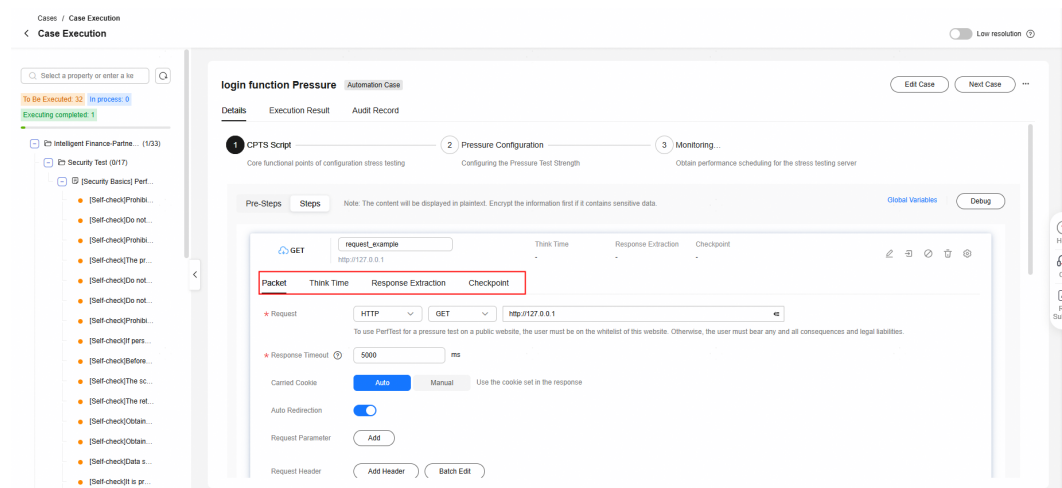
2. Go to the CPTS script page, allows users to edit preset requests and add new requests.

Figure 1-87 Performance Automation Case



- Packet: data sent between applications. For details, see the [operation guide](#).

- Think Time: specifies the waiting time between operations. This parameter is not required in authentication tests. For details, see the [operation guide](#).
- Response extraction: The output of the previous packet is extracted as the input of the next packet. For details, see the [operation guide](#).
- Checkpoint: Checkpoints are used to check whether the content returned by the server is correct based on customized verification information. For details, see the [operation guide](#).

Figure 1-88 Case script

3. After the CPTS script is complete, you can click [Debug] to quickly detect syntax or configuration errors and ensure that the model is available in the task. Click [Next] when you are finished.

NOTE

Prerequisites

- The resource group is in the running state.
- Ports 32001 and 32003 on the debugging node of the resource group are enabled in the security group.
- The execution node of the resource group and applications under the pressure test are connected through the network.

Debugging a Test Case

After you create or edit a test case, you can debug it to detect syntax or configuration errors before testing.

1. Click [Debug] in the upper right corner of the page.
2. Select the target test resource group as the executor and click [Start].
3. Click [View log] to view the test case debugging details.

If an error was reported in the debugging result, edit the case based on the log information and debug it again.

4. On the Debug log tab page, you can view the debugging history.

4. Configure the Pressure Configuration.

Configure the duration of the script based on the requirements in the requirement description

- Pressure test for basic function points: 5 to 10 minutes

- Pressure test in hybrid scenarios: 0.5 to 2 hours
- Comprehensive service fatigue test: 4 to 6 hours

after the configuration is complete, click [Save]. For details, see the [operation guide](#)

Figure 1-89 Test Case Management

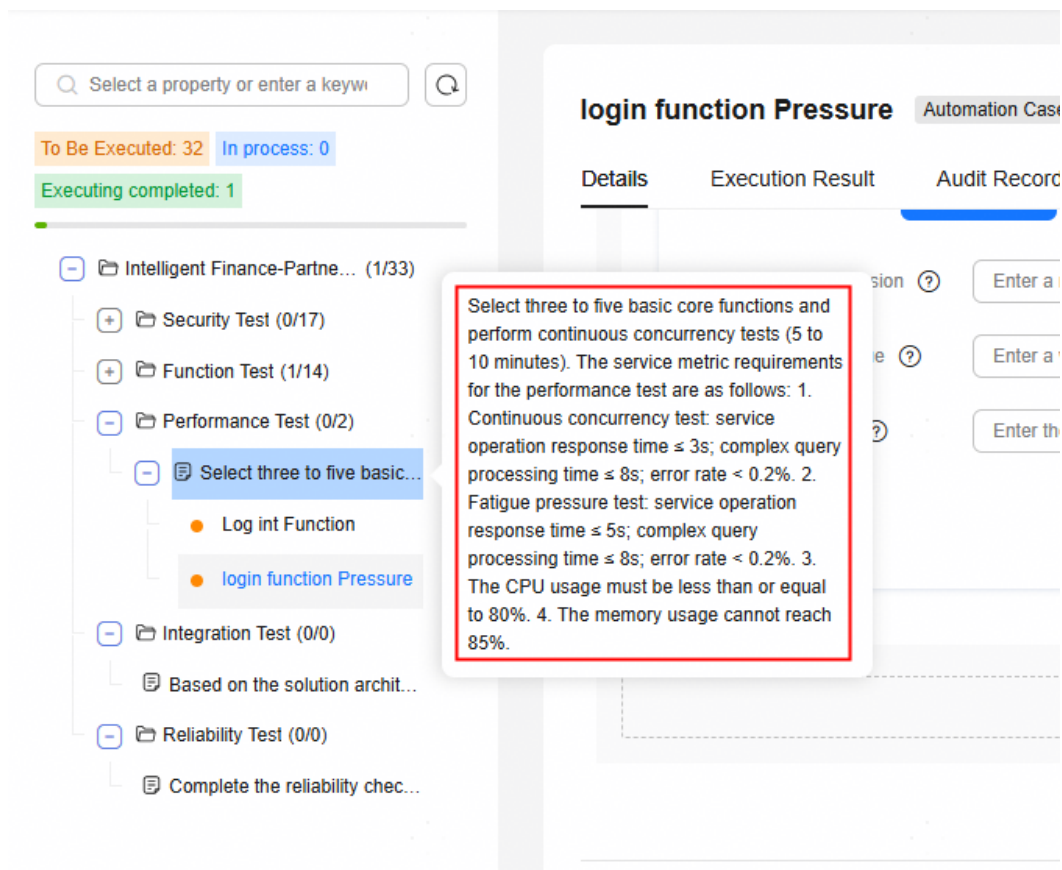
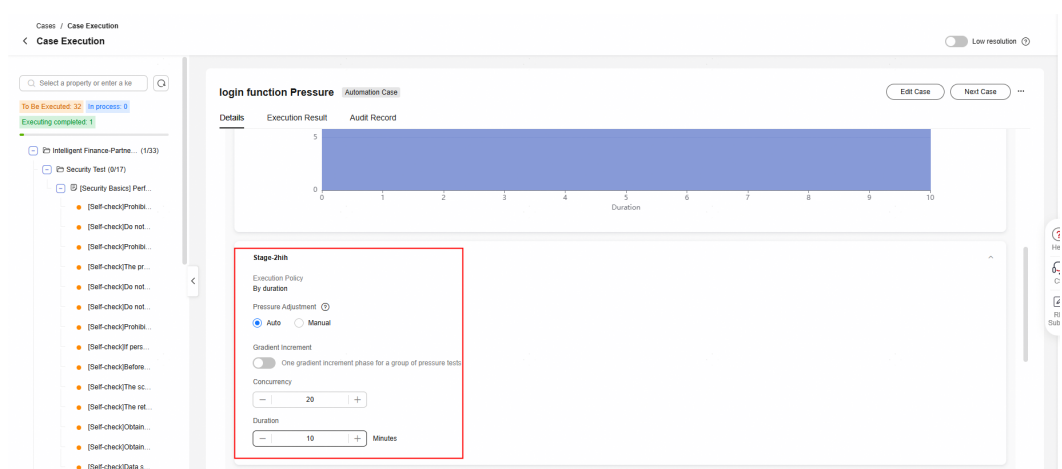


Figure 1-90 Pressure Configuration



Click [Next] when you are finished.

7. Monitoring configuration to capture the CPU and memory performance scheduling of the target server during the stress test.

Figure 1-91 Editing Test Cases

The screenshot shows the 'Edit Case' dialog in the InnoStage Workbench. The 'Basic Information' tab is active, displaying the following details:

- Requirement:** demo solution(1.0)-Test Requirements
- Case Type:** Performance Test
- Case No.:** TC2025022001029
- Deployment Environment:** Huawei Cloud
- Requirement Description:** Performance Test Select three to five basic core functions and perform continuous concurrent...
- Case Name:** xxx_Function_Pressur
- Priority:** Medium
- Description:** xx users concurrently perform xx function for 5 minutes.
- Prerequisites:** The CES Agent has been installed on the ECS where the service is deployed.

The 'Test Procedure' section shows a table of mapped CPTS cases:

CPTS Cases	Status	Latest Executive Report	Expected Result	Execution Result	Consume VUM	Operation
xxx_Function_Pressur	Pending execution	RT (ms) <= 3000 Success Rate (%) >= 99.8				Execution History

Below the table, there is a 'Manual Test Procedure' toggle switch.

NOTE

- If you need to add performance automation test cases, click the [Performance Automation] Test Case tab and click [Create], and design test cases by referring to If you do performance te....

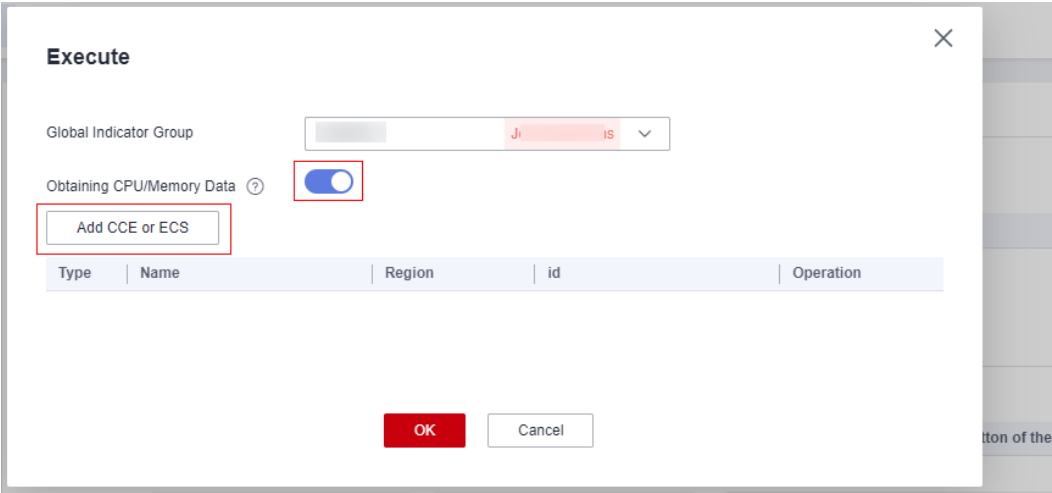
Figure 1-92

The screenshot shows the 'Performance Automation' tab in the InnoStage Workbench. The 'Create' button is highlighted. Below it, there is a table of test cases:

No.	Case Name	Case Type	Requirement Des...	Review Status	Execution Status	Test Result	Created by	Recent Performer	Operation
1	xxx_Function_Pressur	Performance Test	Select three to five ...	Pending	Pending		yangrenhui		Edit Execute More

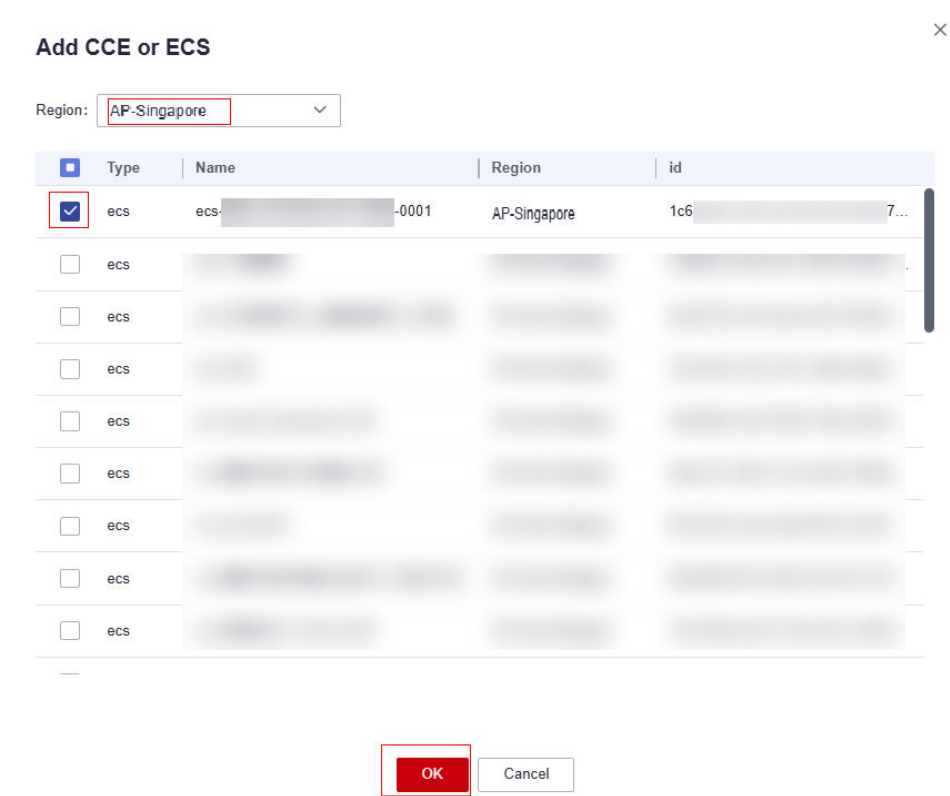
5. In the displayed dialog box, Obtains the CPU and memory performance scheduling of the monitored target server during the pressure test.
 - Select [global indicator group]: The execution result determines whether a test case is passed based on this indicator group.
 - enable [Obtaining CPU/Memory Data]: the CPU and memory usage of the object under pressure test can be obtained.
 - and click [Add CCE or ECS]: select the machine to be tested.

Figure 1-93 Performance Test Case Execution



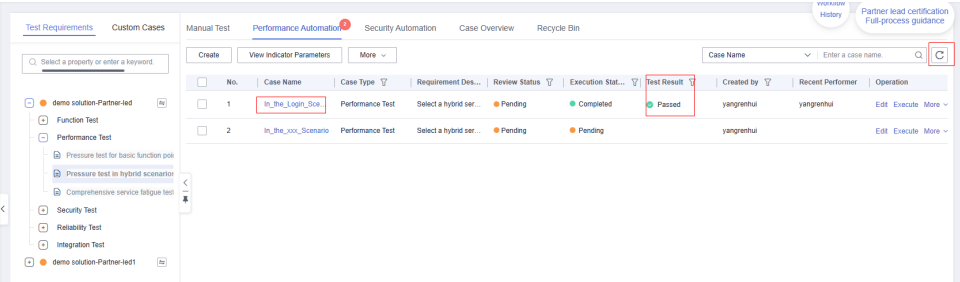
6. Select the region where the CCE or ECS is deployed,add the CCE or ECS to be tested.Click [OK] to start the pressure test.

Figure 1-94 Add The CCE or ECS



7. After the pressure test is complete, refresh the test case list to check whether the test case is executed successfully.

Figure 1-95 Case management



NOTE

The system determines whether the test case is successful based on the automatically loaded indicator parameters.

PerformanceWebsiteHostBinary

+ Add Indicator Parameter

Enter keywords.

Function_prJoint operations
scenario_pressure_test, an...

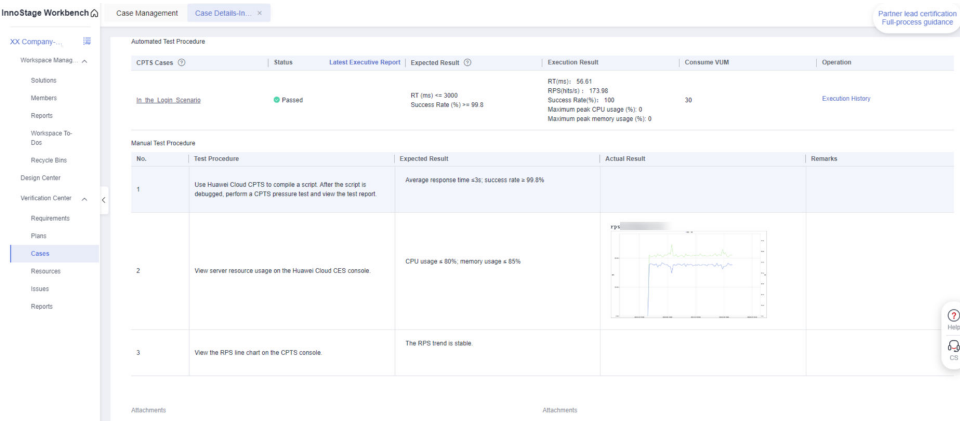
Add

No.	Indicator Name	Indicator Value	Operat...
1	Success Rate (%)	>= 99.8	Delete
2	RT (ms)	<= 3,000	Delete

OKCancel

8.
- click the case name to go to the case basic information page and view the case result.

Figure 1-96 Basic Information



9.
- Click the [Execution result] -> [Report preview] to view the pressure test report.

Figure 1-97 Execution Result

Case Management Case Details in ...

Partner lead certification
Full-process guidance

Basic Information Execution Results

Presets Metric Modified Unmodified

Executing by	Start Time	End Time	Presets counter	Actual Indicator	Manual Test Process	Metric Check Result	Case Execution Re...	VUM	Executing Report	Remarks
yangrenhui	Feb 28, 2025 17:03...	Feb 28, 2025 17:06...	RT (ms) <= 3000 Success Rate (%) >= 99	RT (ms): 56.61 RPS (R/s): 173.98 Success Rate (%): Maximum peak CPU... Maximum peak me...	Yes	Passed	Passed	30	Report Preview View Logs	
yangrenhui	Feb 28, 2025 17:03...	Feb 28, 2025 17:06...	RT (ms) <= 3000 Success Rate (%) >= 99	RT (ms): 56.61 RPS (R/s): 173.98 Success Rate (%): Maximum peak CPU... Maximum peak me...	No	Passed		30	Report Preview View Logs	

Figure 1-98 Report Preview

Report Preview

Task Start Time: Feb 28, 2025 17:03:19 GMT+08:00 Duration: 3Minutes1seconds Total VUM consumption: 30

Executing By: yangrenhui

Total Indicators

Maximum Concurrent10

RPS173.98

Normal returnReturned Number 31490
Success Rate 100%

Abnormal Return0

Response TimeAverage 56.61ms
Max 673ms
Minimum 46ms

Failed to verify 0
Resolving failed 0
Response timed out 0

Other Errors 0
Connection rejected 0

Response Code1XX 0 3XX 0
2XX 31490 4XX 0
5XX 0

Traffic Peak 5486.04KB/S
Maximum Upstream 9.52KB/S
Max Downstream 5476.52KB/S

Test Indicators

Case Name	Maximum Con...	Requests	RPS	Success Rate	Average Delay	TP90	TP95	TP99	Operation
In_the_ox_Scenario	10	31490	173.98	100%	56.61ms	61	64	89	View Logs

Security scanning case execution

- if you use the security scanning function provided by InnoStage Workbench to scan binary,complete the binary scanning case in security automation,vulnerabilities and viruses can be scanned at a time.
 - Select the Security Automation case type,and click the [Execute] button of the Binary Scanning test case.

Figure 1-99 Case Management

InnoStage Workbench

Test Case Custom Cases

Select a property or enter a keyword.

Intelligent Finance Partner-led Incom...

Security Test

[Security Basics] Perform security L...

Function Test

Completed the function test of the ...

Performance Test

Select three to five basic core funct...

Integration Test

Based on the solution architecture ...

Reliability Test

Complete the reliability checklist a...

Manual test case Performance Automation Security Automation Case Overview Recycle Bin

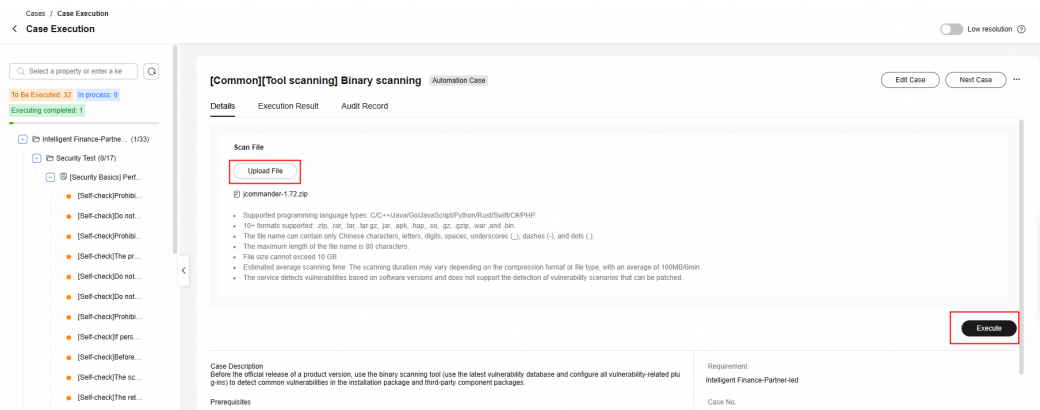
Create More

Case Name Enter keyword to search and filter

No.	Case No.	Case Name	Priority	Case Type	Sca...	Requirement Descri...	Review S...	Executio...	Operation
1	TC202601290...	[Common]Tool...	High	Security Test	Binary	[Security Basics] Perf...	Pending	Pending	Edit Execute Delete

- Click [Upload File] to upload the binary package file to be scanned,and click [Execute].

Figure 1-100 Upload File And Execute



NOTE

Copy all complete binary files (such as the deployment package and installation package) of the solution. For details about the file type, see https://support.huaweicloud.com/vss_faq/vss_01_0083_01.html. Packaged and uploaded as the scanning object. (If the file size exceeds the limit, split it into multiple packages and scan it in multiple cases.)

- c. After the scanning is complete, the test case status is displayed as Completed. You can click the test case name to view the test case execution result.

Figure 1-101 Case Management

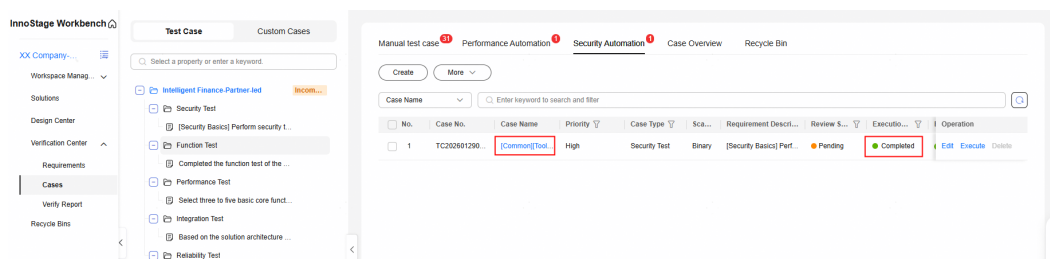
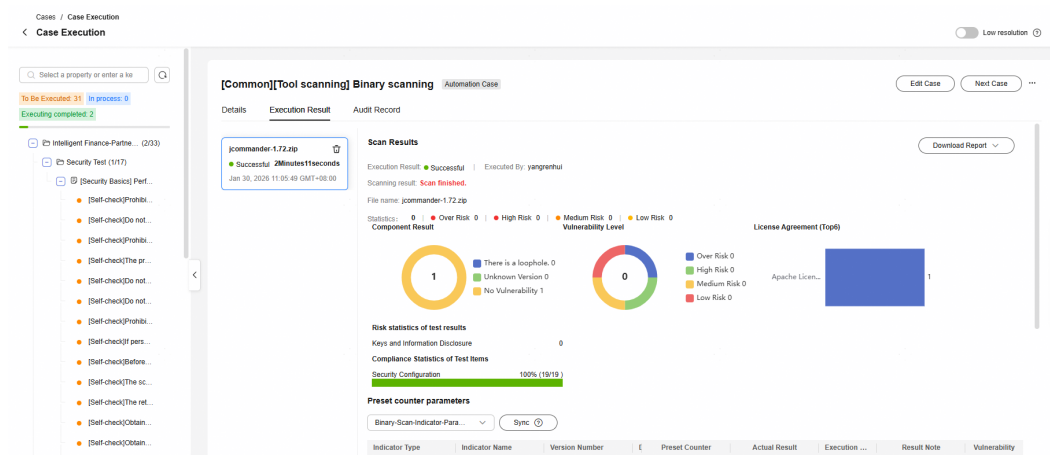


Figure 1-102 Execution Result



NOTE

If the Scanning result is fails, view the result details list, fix the vulnerabilities or clear the virus, and upload and scan the file again.

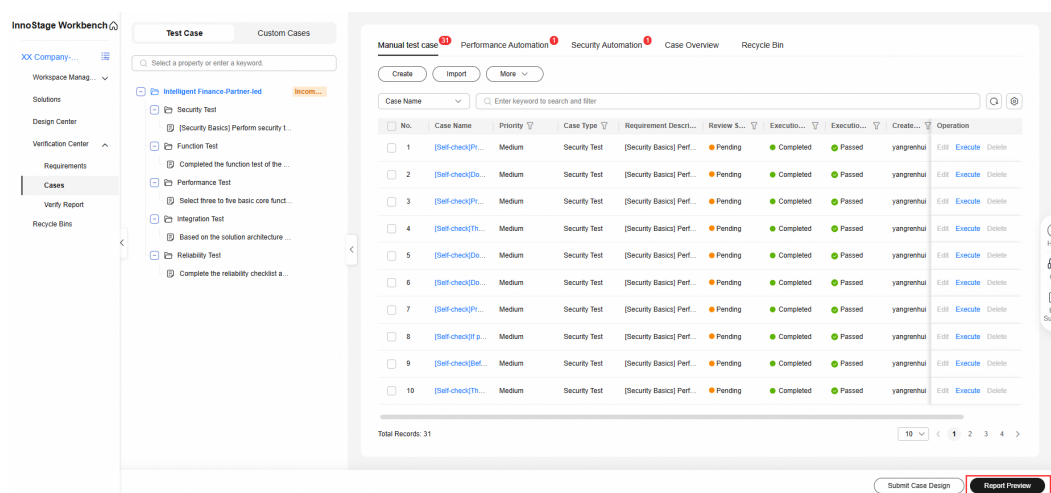
- If you use the third-party tool to scan binary
 - For non-image package scanning.For details, see [Binary Virus Scanning\(non-image\)](#)
 - For Linux image scanning.For details, see [Linux Image Viruses Scanning](#)
 - For Windows image scanning.For details, see [Windows Image Viruses Scanning](#)

1.2.8 Generate And Submit The Test Report.

After all test cases are executed, the executor generates a test report and submits the report to Huawei test engineers for review.

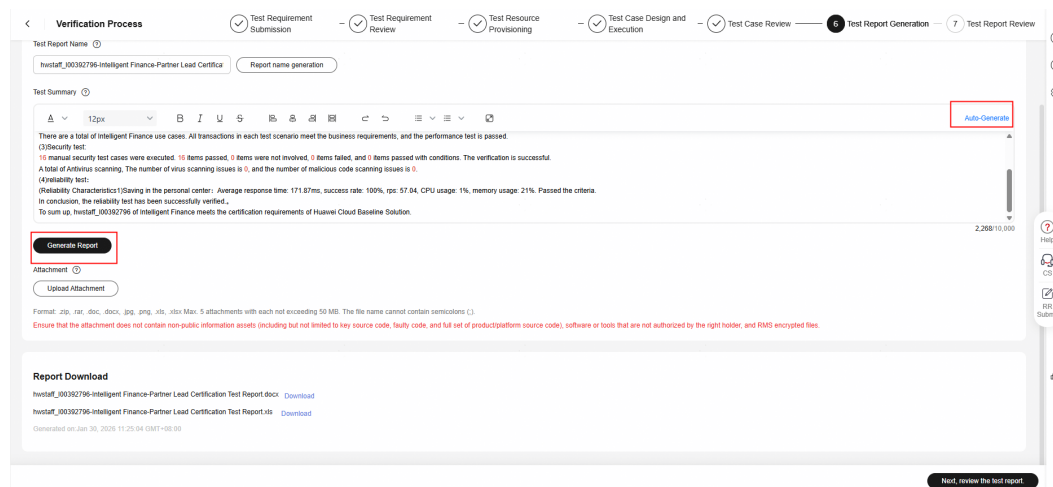
Step 1 the executor clicks the [report preview] button. The report preview page is displayed.

Figure 1-103 Case Management



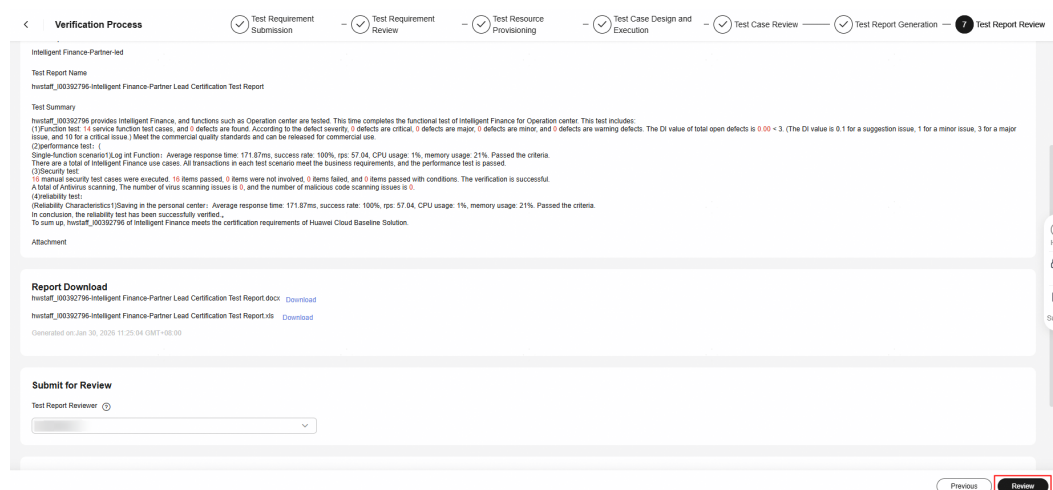
Step 2 On the report preview page, click [Auto-Generate] to generate a test summary. Click [Generate Report] to automatically generate a test report.When finished, click[Next,review the test report].

Figure 1-104 Report Preview



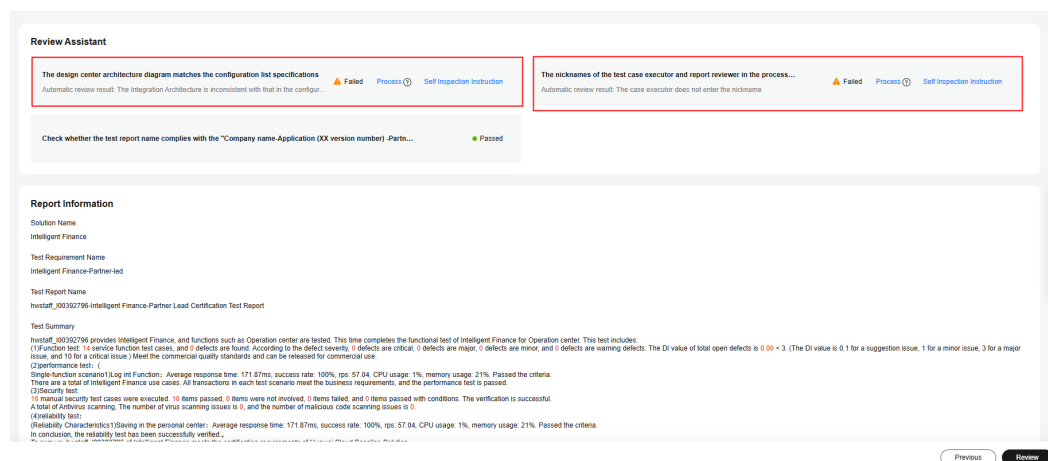
Step 3 Report reviewers are caofeng and wujunchuan. and then click Submit.

Figure 1-105 Report Preview



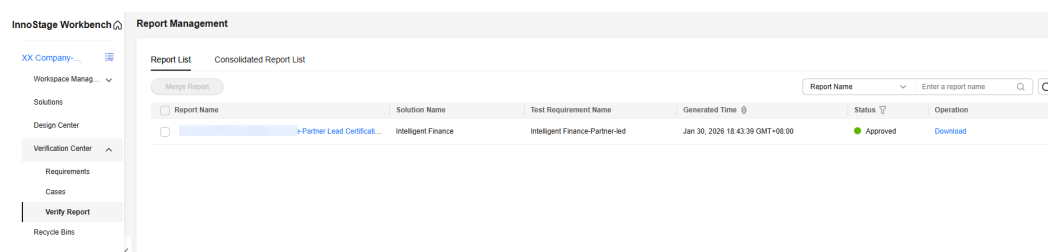
Step 4 If the system displays a message indicating that the review result is rejected, check whether you can ignore it. If yes, click Self-Check Description to fill in the detailed reason description. If the problem cannot be ignored, solve the problem and submit the application again.

Figure 1-106 Report Preview



Step 5 After the report is submitted, the reviewer generates a to-do task. After the report is approved, the status of the report is "Approved", and the partner lead qualification is completed.

Figure 1-107 Report Management



----End

1.2.9 Third-Party Tools

Binary Vulnerability Scanning (Linux Image)

Trivy is required for mirror image package scanning. The following uses the MySQL container image as an example.

- **Environment setup**

Installing Docker(The host machine uses CentOS 7.9)

Uninstall Docker of the old version (if any).

Run the following command:`sudo yum remove docker docker-client docker-client-latest docker-common docker-latest docker-latest-logrotate docker-logrotate docker-engine`


```
[root@ecs-test-libin ~]# sudo yum remove docker docker-client docker-client-latest
docker-common docker-latest docker-latest-logrotate docker-logrotate docker-engine
Loaded plugins: fastestmirror
No Match for argument: docker
No Match for argument: docker-client
No Match for argument: docker-client-latest
No Match for argument: docker-common
No Match for argument: docker-latest
No Match for argument: docker-latest-logrotate
No Match for argument: docker-logrotate
No Match for argument: docker-engine
No Packages marked for removal
[root@ecs-test-libin ~]#
```

(The server does not have Docker of the earlier version, and a message is displayed indicating that no image is available.)

Installing necessary dependency packages.

Run the following command: `sudo yum install -y yum-utils device-mapper-persistent-data lvm2`

```
[root@ecs-test-libin ~]# sudo yum install -y yum-utils device-mapper-persistent-data lvm2
Loaded plugins: fastestmirror
Determining fastest mirrors
base                                                    | 3.6 kB  00:00:00
epel                                                    | 4.7 kB  00:00:00
extras                                                  | 2.9 kB  00:00:00
updates                                                 | 2.9 kB  00:00:00
(1/7): epel/x86_64/updateinfo                          | 1.0 MB  00:00:00
(2/7): base/7/x86_64/primary_db                       | 6.1 MB  00:00:00
(3/7): base/7/x86_64/group_gz                         | 153 kB  00:00:00
(4/7): epel/x86_64/group_gz                           | 100 kB  00:00:00
(5/7): epel/x86_64/primary_db                         | 7.0 MB  00:00:00
(6/7): extras/7/x86_64/primary_db                    | 253 kB  00:00:00
(7/7): updates/7/x86_64/primary_db                   | 26 MB  00:00:08
Resolving Dependencies
```

Setting the Docker Image Source(HUAWEI CLOUD image source is used as an example.)

Run the following command: `sudo yum-config-manager --add-repo https://mirrors.aliyun.com/docker-ce/linux/centos/docker-ce.repo`

```
[root@ecs-test-libin ~]# sudo yum-config-manager --add-repo https://mirrors.aliyun.com/docker-ce/linux/centos/docker-ce.repo
Loaded plugins: fastestmirror
adding repo from: https://mirrors.aliyun.com/docker-ce/linux/centos/docker-ce.repo
grabbing file https://mirrors.aliyun.com/docker-ce/linux/centos/docker-ce.repo to /etc/yum.repos.d/docker-ce.repo
repo saved to /etc/yum.repos.d/docker-ce.repo
[root@ecs-test-libin ~]#
```

Updating the YUM Software Package Index

Run the following command: `sudo yum makecache fast`

```
[root@ecs-test-libin ~]# sudo yum makecache fast
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
base
docker-ce-stable
epel
extras
updates
(1/2): docker-ce-stable/7/x86_64/updateinfo
(2/2): docker-ce-stable/7/x86_64/primary_db
Metadata Cache Created
[root@ecs-test-libin ~]#
```

Installing Docker

Installing Docker CE of the Latest Version (Community Edition)

Run the following command: `sudo yum install docker-ce docker-ce-cli containerd.io`

```
[root@ecs-test-libin ~]# sudo yum install docker-ce docker-ce-cli containerd.io
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
No package docker-ce available.
No package docker-ce-cli available.
No package containerd.io available.
Error: Nothing to do
[root@ecs-test-libin ~]# sudo yum-config-manager --add-repo https://mirrors.aliyun.com/docker-ce/linux/centos/docker-ce.repo
Loaded plugins: fastestmirror
adding repo from: https://mirrors.aliyun.com/docker-ce/linux/centos/docker-ce.repo
grabbing file https://mirrors.aliyun.com/docker-ce/linux/centos/docker-ce.repo to /etc/yum.repos.d/docker-ce.repo
repo saved to /etc/yum.repos.d/docker-ce.repo
[root@ecs-test-libin ~]# sudo yum makecache fast
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
base
docker-ce-stable
```

Start and enable Docker

Run the following command:

`sudo systemctl start docker`

`sudo systemctl start docker`

Figure 1-108

```
[root@ecs-test-libin ~]# sudo systemctl start docker
[root@ecs-test-libin ~]# sudo systemctl enable docker
Created symlink from /etc/systemd/system/multi-user.target.wants/docker.service to /usr/lib/systemd/system/docker.service.
[root@ecs-test-libin ~]#
```

Test Docker

Run the following command:`sudo docker run hello-world`

```
[root@ecs-test-libin ~]# sudo docker run hello-world
Unable to find image 'hello-world:latest' locally
latest: Pulling from library/hello-world
c1ec31eb5944: Pull complete
Digest: sha256:53641cd209a4fecfc68e21a99871ce8c6920b2e7502df0a20671c6fccc73a7c6
Status: Downloaded newer image for hello-world:latest

Hello from Docker!
This message shows that your installation appears to be working correctly.

To generate this message, Docker took the following steps:
 1. The Docker client contacted the Docker daemon.
 2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
    (amd64)
 3. The Docker daemon created a new container from that image which runs the
    executable that produces the output you are currently reading.
 4. The Docker daemon streamed that output to the Docker client, which sent it
    to your terminal.

To try something more ambitious, you can run an Ubuntu container with:
$ docker run -it ubuntu bash

Share images, automate workflows, and more with a free Docker ID:
https://hub.docker.com/

For more examples and ideas, visit:
https://docs.docker.com/get-started/
```

- **Scanning process**
 - **Trivy Scanning MySQL Container Images.**
 - i. Updating the Trivy offline library
Run the following command:`docker pull quay.io/sighup/trivy-offline:latest`

```
[root@ecs-test-libin ~]# docker pull quay.io/sighup/trivy-offline:latest
latest: Pulling from sighup/trivy-offline
26528ae74efr: Pull complete
3dd9ae104f9d: Pull complete
296636aa14dd: Pull complete
331e16d7effr: Pull complete
1act597a165d: Pull complete
Digest: sha256:10f5fb8a1d68e5b6ed146d282cc54810686c918a8e9ee37e79389fce4283fe91
Status: Downloaded newer image for quay.io/sighup/trivy-offline:latest
quay.io/sighup/trivy-offline:latest
[root@ecs-test-libin ~]# docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS          NAMES
34bd5472720b   mysql:5.7     "docker-entrypoint.s..." 6 hours ago   Up 6 hours    33060/tcp      libin-mysql-container
[root@ecs-test-libin ~]# docker run -it --rm -v /var/run/docker.sock:/var/run/docker.sock quay.io/sighup/trivy-offline libin-mysql-container
2024-04-08T08:46:02.645Z      INFO    Vulnerability scanning is enabled
2024-04-08T08:46:02.645Z      INFO    Secret scanning is enabled
2024-04-08T08:46:02.645Z      INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-04-08T08:46:02.645Z      INFO    Please see also https://aquasecurity.github.io/trivy/v0.46/docs/scanner/secret/#recommendation for faster secret detection
2024-04-08T08:46:05.225Z      ERROR   Image scan errors: scan errors: unable to initialize a scanner: unable to initialize a docker scanner: 4 errors occurred:
* unable to inspect the image (libin-mysql-container): Error response from daemon: No such image: libin-mysql-container:latest
* containerd socket not found: /run/containerd/containerd.sock
* unable to initialize Podman client: no podman socket found: stat podman/podman.sock: no such file or directory
* GET https://index.docker.io/v2/library/libin-mysql-container/manifests/latest: UNAUTHORIZED: authentication required; [map[Action:pull Class: Name:library/libin-mysql-container Type:repository]]
```

ii. Use Trivy to scan images and provide scan result screenshots.

NOTICE

The test case can be passed only when the number of high-risk and super-risk vulnerabilities is 0. Otherwise, the vulnerability needs to be fixed and then scanned again.

Run the following command:`docker run -it --rm -v /var/run/docker.sock:/var/run/docker.sock quay.io/sighup/trivy-offline mysql:5.7` (Scanning the MySQL:5.7 image offline is used as an example.)

critical vulnerability:CVE-2020-36242

high-risk

vulnerability:CVE-2023-0286,CVE-2022-40897,CVE-2023-27561

If the scanning result does not contain vulnerabilities at the HIGH or CRITICAL level, the test case passes. Otherwise, the test case fails,Security vulnerabilities whose severity level is HIGH and CRITICAL need to be fixed.

Screenshots of basic image vulnerabilities are required for each image. Screenshots of application vulnerabilities are required for each application.Screenshots. Refer to three pictures.

```
[root@ecs-test-libin ~]# docker run -it --rm -v /var/run/docker.sock:/var/run/docker.sock quay.io/sighup/trivy-offline mysql:5.7
2024-04-08T08:47:04.646Z      INFO    Vulnerability scanning is enabled
2024-04-08T08:47:04.646Z      INFO    Secret scanning is enabled
2024-04-08T08:47:04.646Z      INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-04-08T08:47:04.646Z      INFO    Please see also https://aquasecurity.github.io/trivy/v0.46/docs/scanner/secret/#recommendation for faster secret detection
2024-04-08T08:47:12.562Z      INFO    Detected OS: oracle
2024-04-08T08:47:12.562Z      INFO    Detecting Oracle Linux vulnerabilities...
2024-04-08T08:47:12.570Z      INFO    Number of language-specific files: 2
2024-04-08T08:47:12.570Z      INFO    Detecting goby binary vulnerabilities...
2024-04-08T08:47:12.570Z      INFO    Detecting python-pkg vulnerabilities...

mysql:5.7 (oracle 7.9)
Total: 6 (UNKNOWN: 0, LOW: 0, MEDIUM: 6, HIGH: 0, CRITICAL: 0)



| Library      | Vulnerability  | Severity | Status | Installed Version | Fixed Version           | Title                                                                                                                                                                     |
|--------------|----------------|----------|--------|-------------------|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| openssl      | CVE-2021-23840 | MEDIUM   | fixed  | 1:1.0.2k-26.el7_9 | 10:1.0.2k-22.el7_9_fips | openssl: integer overflow in CipherUpdate<br><a href="https://avd.aquasec.com/nvd/cve-2021-23840">https://avd.aquasec.com/nvd/cve-2021-23840</a>                          |
|              | CVE-2021-23841 |          |        |                   |                         | openssl: NULL pointer dereference in X509 issuer_and_serial_hash()<br><a href="https://avd.aquasec.com/nvd/cve-2021-23841">https://avd.aquasec.com/nvd/cve-2021-23841</a> |
|              | CVE-2021-3712  |          |        |                   |                         | openssl: Read buffer overruns processing ASN.1 strings<br><a href="https://avd.aquasec.com/nvd/cve-2021-3712">https://avd.aquasec.com/nvd/cve-2021-3712</a>               |
| openssl-libs | CVE-2021-23840 | MEDIUM   | fixed  | 1:1.0.2k-22.el7_9 | 10:1.0.2k-22.el7_9_fips | openssl: integer overflow in CipherUpdate<br><a href="https://avd.aquasec.com/nvd/cve-2021-23840">https://avd.aquasec.com/nvd/cve-2021-23840</a>                          |
|              | CVE-2021-23841 |          |        |                   |                         | openssl: NULL pointer dereference in X509 issuer_and_serial_hash()<br><a href="https://avd.aquasec.com/nvd/cve-2021-23841">https://avd.aquasec.com/nvd/cve-2021-23841</a> |
|              | CVE-2021-3712  |          |        |                   |                         | openssl: Read buffer overruns processing ASN.1 strings<br><a href="https://avd.aquasec.com/nvd/cve-2021-3712">https://avd.aquasec.com/nvd/cve-2021-3712</a>               |


2024-04-08T08:47:12.648Z      INFO    Table result includes only package filenames. Use '--format json' option to get the full path to the package file.
```

python (python-pkg)

Total: 12 (UNKNOWN: 0, LOW: 3, MEDIUM: 5, HIGH: 3, CRITICAL: 1)

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title		
cryptography (METADATA)	CVE-2020-36242	CRITICAL	fixed	3.2.1	3.3.2	python-cryptography: Large inputs for symmetric encryption can trigger integer overflow leading to... https://avd.aquasec.com/nvd/cve-2020-36242		
	CVE-2023-0286	HIGH			39.0.1	openssl: X.400 address type confusion in X.509 GeneralName https://avd.aquasec.com/nvd/cve-2023-0286		
	CVE-2023-50782	MEDIUM			42.0.0	python-cryptography: Bleichenbacher timing oracle attack against RSA decryption - incomplete fix for... https://avd.aquasec.com/nvd/cve-2023-50782		
	CVE-2023-23931				39.0.1	python-cryptography: memory corruption via immutable objects https://avd.aquasec.com/nvd/cve-2023-23931		
	CVE-2023-49083				41.0.6	python-cryptography: NULL-dereference when loading PKCS7 certificates https://avd.aquasec.com/nvd/cve-2023-49083		
	CVE-2024-0727	LOW			42.0.2	openssl: denial of service via null dereference https://avd.aquasec.com/nvd/cve-2024-0727		
	GHSA-5cpq-8wj7-hf2v				41.0.0	Vulnerable OpenSSL included in cryptography wheels https://github.com/advisories/GHSA-5cpq-8wj7-hf2v		
	GHSA-jm77-qphf-c4w8				41.0.3	pyca/cryptography's wheels include vulnerable OpenSSL https://github.com/advisories/GHSA-jm77-qphf-c4w8		
	GHSA-v8gr-m533-ghj9				41.0.4	Vulnerable OpenSSL included in cryptography wheels https://github.com/advisories/GHSA-v8gr-m533-ghj9		
paramiko (METADATA)	CVE-2023-48795	MEDIUM	fixed	2.11.0	3.4.0	ssh: Prefix truncation attack on Binary Packet Protocol (BPP) https://avd.aquasec.com/nvd/cve-2023-48795		
pip (METADATA)	CVE-2023-5752	HIGH		23.0.1	23.3	pip: Mercurial configuration injectable in repo revision when installing via pip https://avd.aquasec.com/nvd/cve-2023-5752		
setuptools (METADATA)	CVE-2022-40897			58.1.0	65.5.1	pypa-setuptools: Regular Expression Denial of Service (ReDoS) in package_index.py https://avd.aquasec.com/nvd/cve-2022-40897		

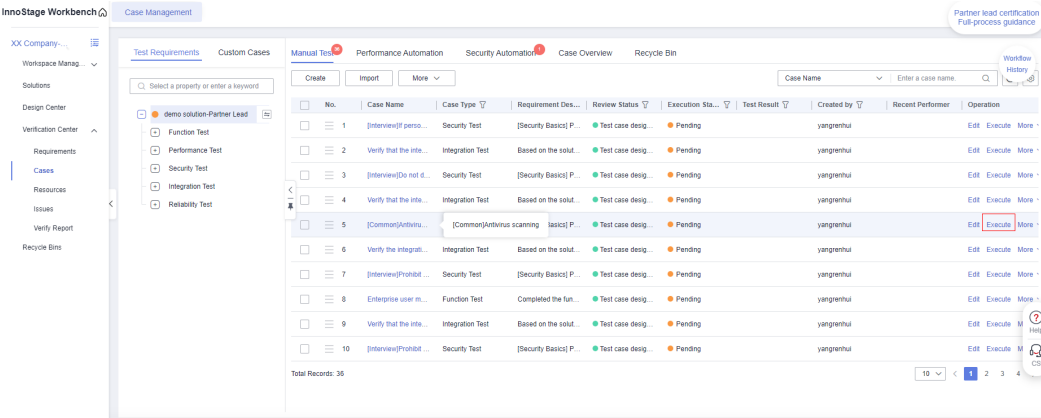
usr/local/bin/gosu (gobinary)

Total: 5 (UNKNOWN: 0, LOW: 1, MEDIUM: 2, HIGH: 2, CRITICAL: 0)

Library	Vulnerability	Severity	Status	Installed Version	Fixed Version	Title		
github.com/opencontainers/runc	CVE-2023-27561	HIGH	fixed	v1.1.0	1.1.5	runc: volume mount race condition (regression of CVE-2019-19921) https://avd.aquasec.com/nvd/cve-2023-27561		
	CVE-2024-21626	MEDIUM			1.1.12	runc: file descriptor leak https://avd.aquasec.com/nvd/cve-2024-21626		
	CVE-2022-29162				1.1.2	runc: incorrect handling of inheritable capabilities https://avd.aquasec.com/nvd/cve-2022-29162		
	CVE-2023-28642				1.1.5	runc: AppArmor can be bypassed when '/proc' inside the container is symlinked... https://avd.aquasec.com/nvd/cve-2023-28642		
	CVE-2023-25809	LOW				runc: Rootless runc makes '/sys/fs/cgroup' writable https://avd.aquasec.com/nvd/cve-2023-25809		

iii. After the scan is passed, go back to the innostage workbench and enter the case management page. Click the [Execution] button of the binary test case.

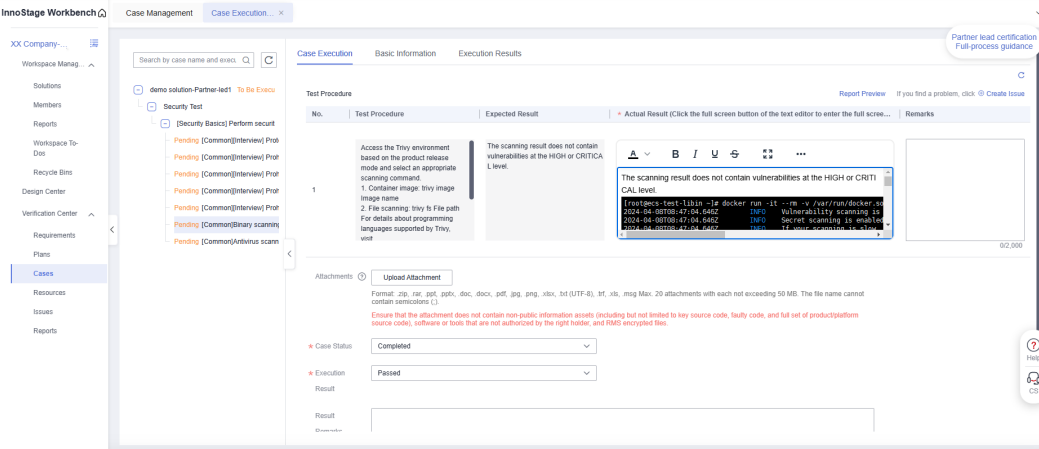
Figure 1-109 Case Management



Copy the expected result to the actual result, and paste the screenshot in step 2 to the actual result,
Case Status:Completed

Execution Result:Passed

Figure 1-110 Test Case Execution



Click[Confirm and go to Next] or click[OK].

- Binary Security Scanning of Dependent Libraries

Trivy automatically detects supported files and scans for vulnerabilities in application dependencies. Currently, only several binary packages are supported.

Table 1-3

language	Packet format
Java	JAR/WAR/PAR/EAR
Go	Binaries built by Go
Rust	Binaries built with cargo-auditable

If the file to be scanned is a compressed package, manually decompress the package.

The scanning procedure is as follows:

- i. Copy the files to be scanned to the current directory, create a container instance, and mount the host file system to the container.
- ii. Enter the container and specify the scanning path to perform scanning. For details about the file system modes supported by different languages, see <https://aquasecurity.github.io/trivy/v0.45/docs/coverage/language/>
- iii. Run the following command:

```
docker run --rm -it -v /var/run/docker.sock:/var/run/docker.sock -v $(pwd):/wrk --entrypoint /bin/sh quay.io/sighup/trivy-offlin  
trivy fs --skip-db-update --skip-java-db-update -o /wrk/  
report.txt /wrk/
```

The following table lists the scanning parameters of different forms.

Table 1-4

Formatting	Command parameter
Image	image
Rootfs	rootfs
Filesystem	fs
Repository	repo

– **Dependent Open Source Component Definition List Scanning**

Trivy can check for vulnerabilities in dependent components through the dependency library definition file.

i. **Prerequisites**

Obtain the third-party dependency definition file of the corresponding development language. The following table lists the supported development language dependency definition files. More supported languages are [<https://aquasecurity.github.io/trivy/v0.45/docs/coverage/language/>].

Table 1-5

language	Dependency definition file	Command Parameters
PHP	composer.lock	trivy fs
Go	go.mod	trivy fs
C#	packages.config	trivy fs
Java	pom.xml	trivy rootfs
Node.js	package-lock.json yarn.lock pnpm-lock.yaml	trivy fs
Node.js	package.json	trivy rootfs

For example, in the PHP project, the third-party dependency library is managed by the Composer, and the composer.lock file of the development project can be obtained.

ii. **Operation Procedure**

- 1) Copy the dependency definition file to the /tmp/trivy/ directory on the Docker host.

- 2) Run the following command to start the container: `docker run --rm -it -v /tmp/trivy:/wrk --entrypoint /bin/sh quay.io/sighup/trivy-offline`
- 3) Run the following command to perform the scanning: `trivy fs --skip-db-update --skip-java-db-update /wrk/`
- 4) Run the following command to save the result to the report.txt file:
`trivy fs --skip-db-update --skip-java-db-update -o /wrk/report.txt /wrk/`

You are advised Run the following command to export the results to the HTML file report.html:

```
trivy fs --skip-db-update --skip-java-db-update --format template --template "@/contrib/html.tpl" -o /wrk/report.html /wrk/
```

- **Reference Document**

- Language-specific Packages[<https://aquasecurity.github.io/trivy/v0.45/docs/coverage/language/>]
- Download the vulnerability database[<https://github.com/aquasecurity/trivy-db#download-the-vulnerability-database>]
- <https://github.com/sighupio/trivy-offline>[<https://github.com/sighupio/trivy-offline>]
- Trivy Documents[<https://aquasecurity.github.io/trivy/latest/docs/>]
- HUAWEI CLOUD Docker CE Mirror[<https://mirrors.huaweicloud.com/mirrorDetail/5ea14d84b58d16ef329c5c13>]
- Docker Ubuntu Installation Document [<https://docs.docker.com/engine/install/ubuntu/>]

Linux Image Viruses Scanning

Only the host image of Joint operation products needs to be scanned. Other types of products and non-images do not need to be scanned.

This section describes how to use Kaspersky to scan Linux images for viruses.

 CAUTION

1. Kaspersky offers a 30-day trial.
 2. To download the installation package, the database needs to access the Internet, and the ECS needs to be bound with an EIP.
-

Step 1 Download

Select the Kaspersky Endpoint Security installation package based on the OS type:

https://www.kaspersky.com.cn/small-to-medium-business-security/downloads/endpoint?utm_content=downloads

- Ubuntu:

✓ Kaspersky Endpoint Security for Linux

Version 12.0.0.6672 | Debian x64 | Distributive

SHA256:

CF124A7DCB0C70DD85503FA250737BC981FF56630A891710DBC579E2
39D153B2

Version 12

下载

- Centos,Fedora:

✓ Kaspersky Endpoint Security for Linux

Version 12.0.0.6672 | Red Hat Enterprise Linux x64 | Distributive

SHA256:

40D0E987711E924F92DA102D6060A28244586BD00D3E9584AE3138D81
115A09A

Version 12

下载

After the installation package is downloaded, Run the following command:sha256sum <Installation package file>

Check whether the result is consistent with the downloaded information. If yes, start the installation.

Figure 1-111

✓ Kaspersky Endpoint Security for Linux

Version 12.0.0.6672 | Debian x64 | Distributive

SHA256:

CF124A7DCB0C70DD85503FA250737BC981FF56630A891710DBC579E2
39D153B2

Version 12

下载

Step 2 Installed

For Red Hat:RPM format:run the following command:rpm -ivh <Installation package file>

Debian: Deb format:run the following command: dpkg -i <Installation package file>

Step 3 Initial Configuration

run the following command:/opt/kaspersky/kesl/bin/kesl-setup.pl script (marked in the red box in the following figure) when the following information is displayed.

```
[root@touchspring-raozhiqiang ~]# ll
total 97916
-rw-r--r-- 1 root root 4795 Dec 15 15:05 AutoStartOrStop.log
-rw-r--r-- 1 root root 100246188 Dec 1 14:43 kesl-12.0.0-6672.x86_64.rpm
-rwxr-xr-x 1 root root 210 Dec 1 15:08 testJar.sh
[root@touchspring-raozhiqiang ~]# sha256sum kesl-12.0.0-6672.x86_64.rpm
40d0e987711e924f92da102d6060a28244586bd00d3e9584ae3138d81115a09a kesl-12.0.0-6672.x86_64.rpm
[root@touchspring-raozhiqiang ~]# rpm -ivh kesl-12.0.0-6672.x86_64.rpm
Preparing...
Updating / installing...
 1:kesl-12.0.0-6672
The application 'Kaspersky Endpoint Security 12.0 for Linux' was successfully installed but must be configured before use.
Please run script '/opt/kaspersky/kesl/bin/kesl-setup.pl' for application configuration
[root@touchspring-raozhiqiang ~]# /opt/kaspersky/kesl/bin/kesl-setup.pl
```

The system prompts you to initialize the configuration.

1. If the parameters have default values, press "Enter" and wait until the environment initialization is complete.
2. If there is no default value, enter "y" and wait until the environment initialization is complete.

Analyze the file. If the file is not used by the image, delete the file. If the file is used by the image, check whether the file is falsely reported. The analysis file is displayed as a document.

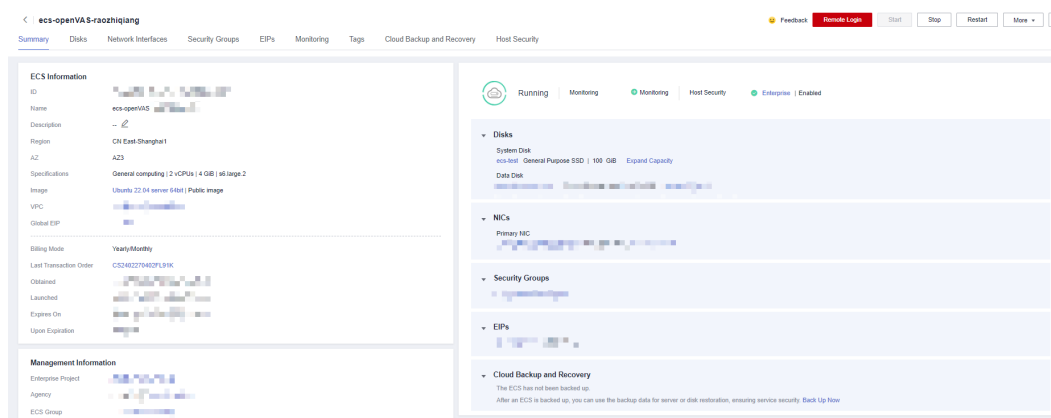
Step 5 Provide scan results

NOTICE

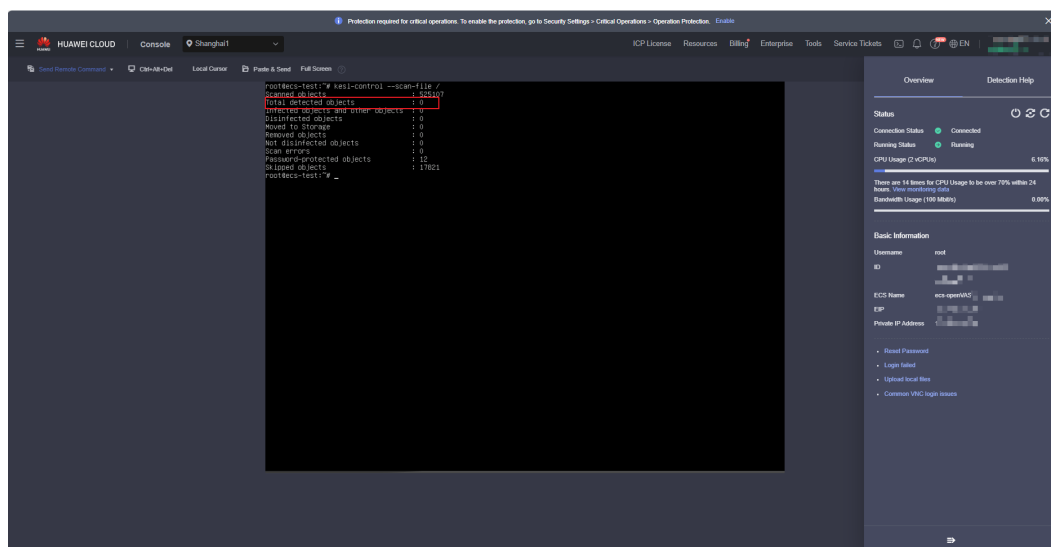
The execution is successful only when the virus value is 0. Otherwise, you need to remove viruses and scan them again.

The partner needs to provide the following materials by email (You do not need to mosaic the screenshot.). The server information in different snapshots must be the same.

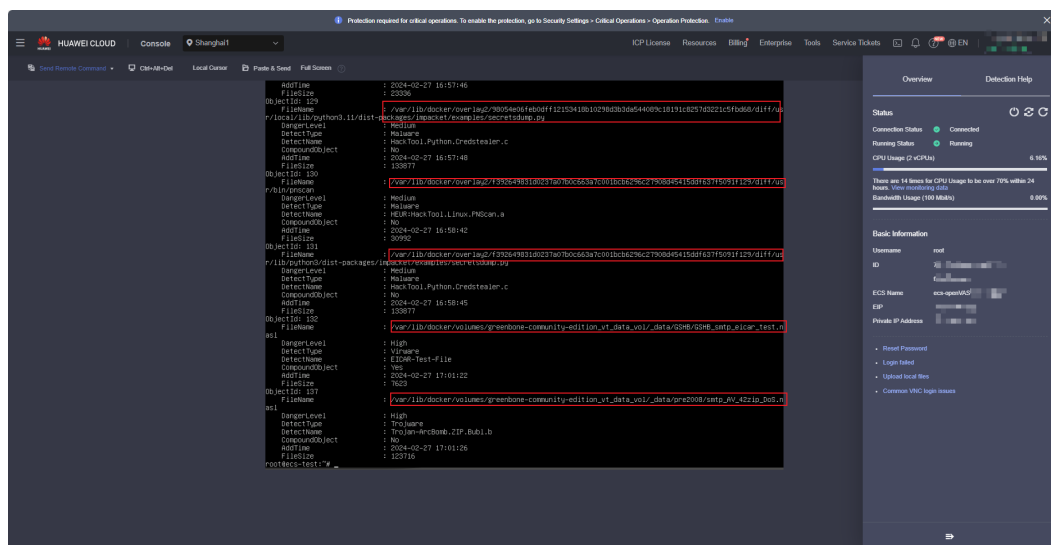
1. Screenshot of the scanning server



2. Screenshot of the final full-disk scanning result (screenshot of the remote login page of the ECS console)



3. Check the screenshot of the file in the isolation zone (after the risk is handled) (screenshot of the remote login page of the ECS console).

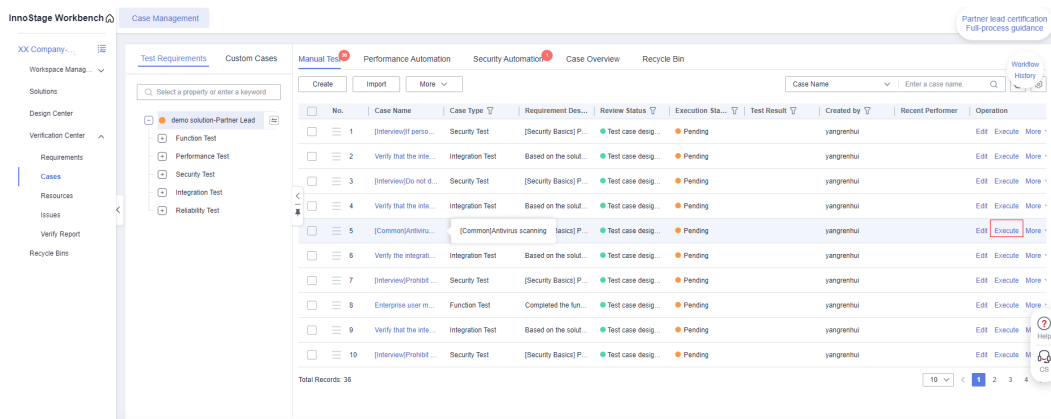


4. Description of the document corresponding to the false positive file (if any).

Step 6 Enter the execution result.

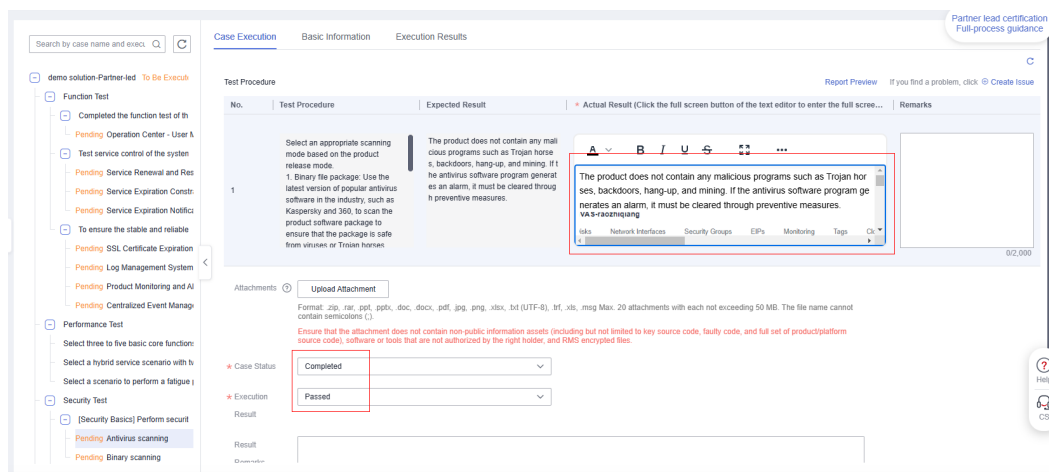
1. Return to InnoStage Workbench and click the execution button of the "Antivirus scanning" case. The execution page is displayed.

Figure 1-112 Test Case Management



2. If the test case is successfully executed, copy the content in the expected result to the actual result, paste the screenshot obtained in step 5 to the actual result, and click OK.

Figure 1-113 Test Case Execution



Step 7 Reference URL

Kaspersky Documentation: <https://support.kaspersky.com/help/KES4Linux/12.0.0/zh-Hans/93769.htm>

-----End

Windows Image Viruses Scannin

Download and install the official Kaspersky software in Windows to perform a full scan.

Step 1 Download (Kaspersky)

Kaspersky download address reference (with a 30-day trial period after download):

China site: <https://www.kaspersky.com.cn/small-to-medium-business-security/downloads/endpoint>

International site: <https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint>

Select Kaspersky Endpoint Security for Windows and select Kaspersky Endpoint Security for Windows Version 12.4.0.467 | Windows | Distributive | Lite encryption for the version.

Step 2 Installation Reference Website

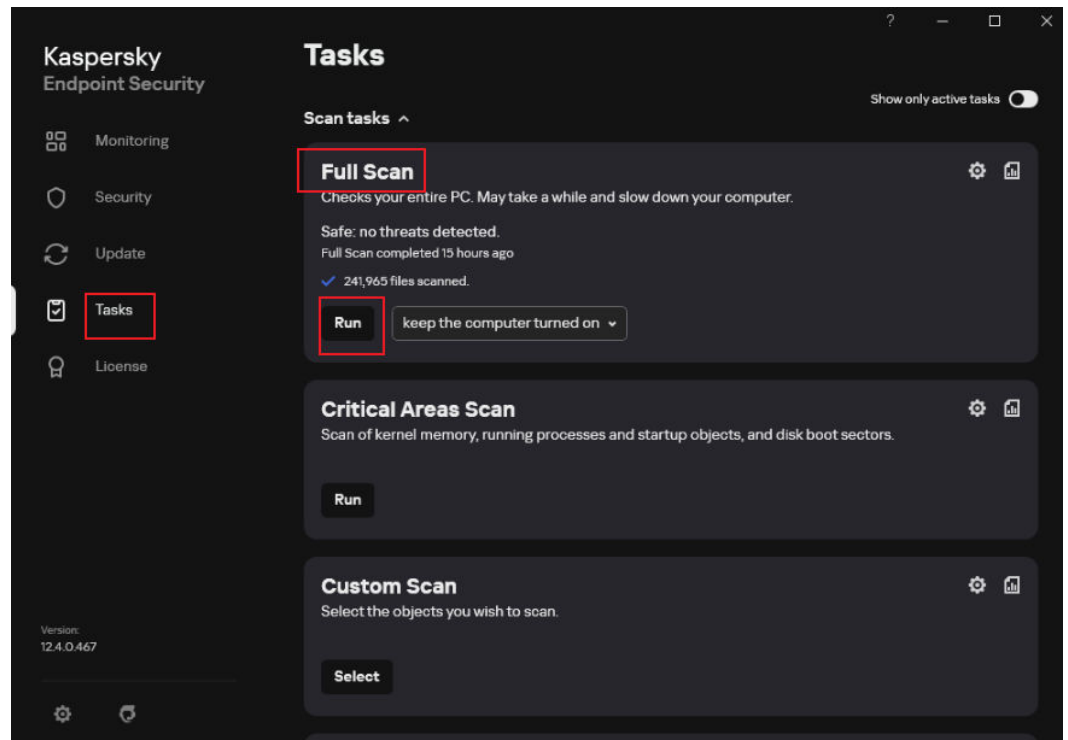
Install the Kaspersky reference document: <https://support.kaspersky.com/KESWin/12.4/zh-Hans/141289.htm>

Step 3 Operation Procedure

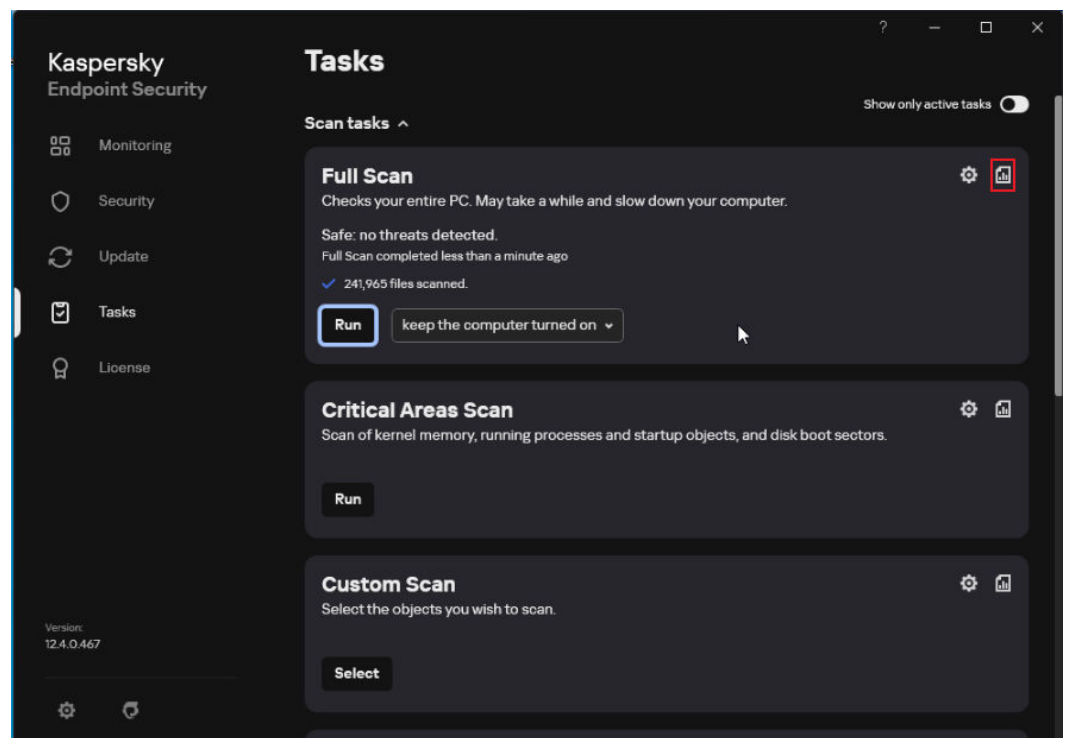
NOTICE

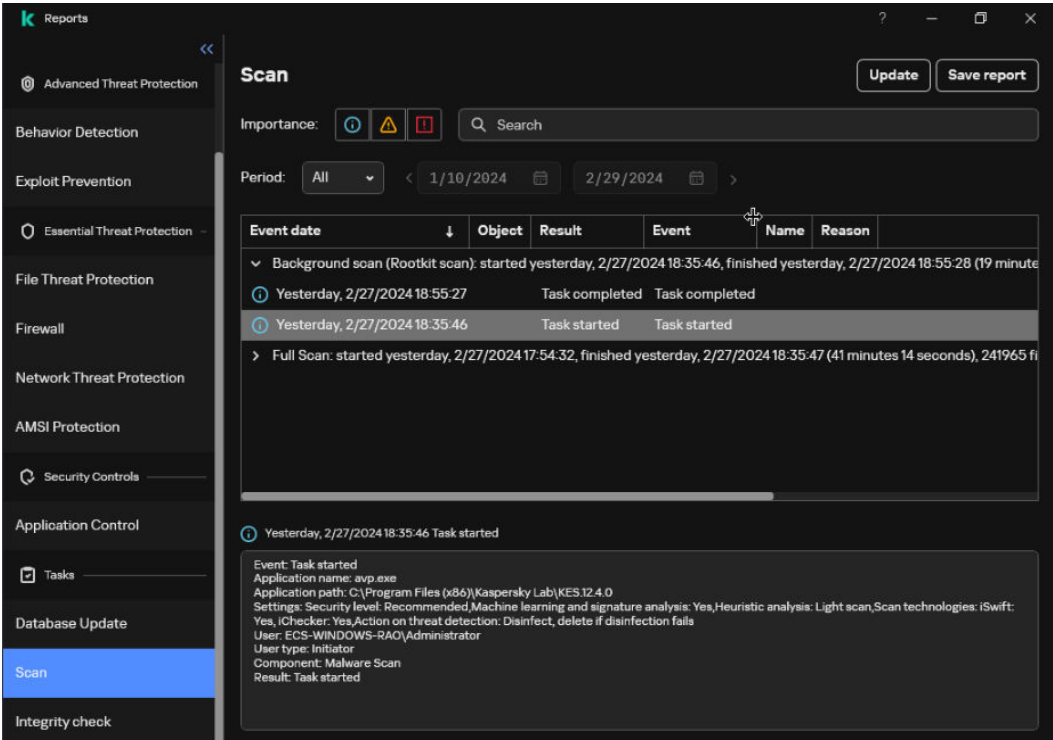
The execution is successful only when the virus value is 0. Otherwise, you need to remove viruses and scan them again.

1. Start Kaspersky, click Task, and click [Run] to start the full disk scanning. Wait until the scanning is complete.



2. Check whether the latest scanning result contains risky items.



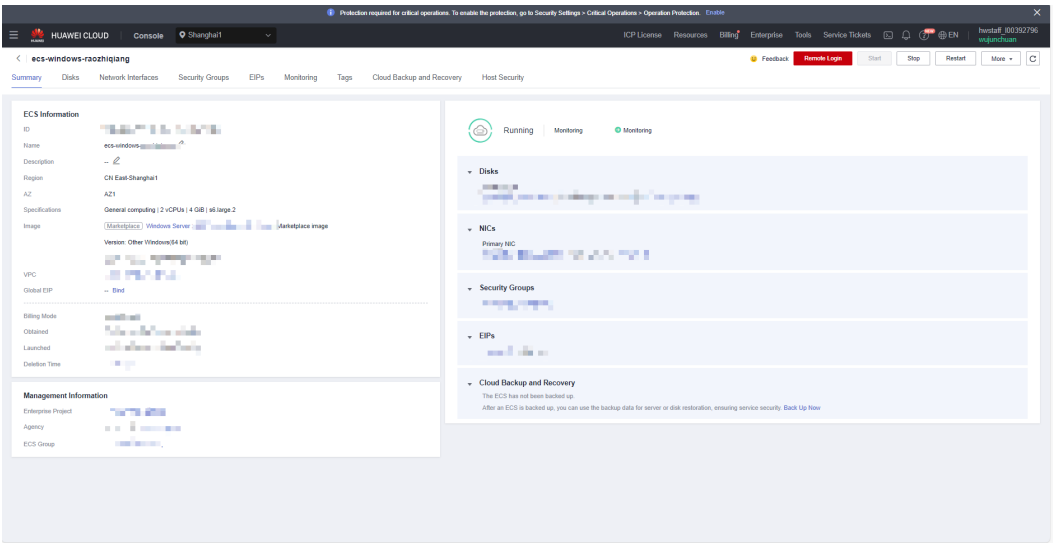


If no problem is found, only the task start and finished information is displayed in the list. If the scanning has risks, the risk items are displayed in the list. All the risk items need to be resolved and the scanning needs to be performed again.

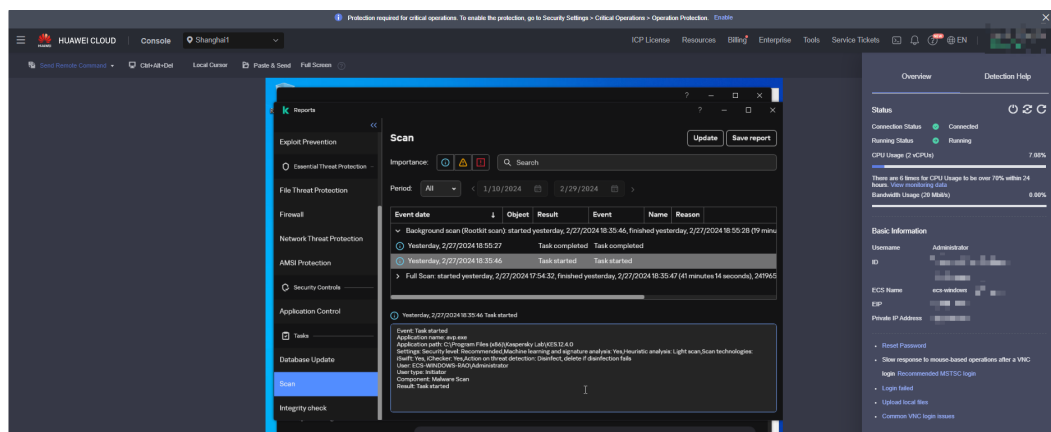
Step 4 Provide scan results

The partner needs to provide the following materials by email: (You do not need to mosaic the screenshot.). The server information in different snapshots must be the same.

1. Screenshot of the scanning server



2. Screenshot of the final full-disk scanning result (screenshot of the remote login page of the ECS console)



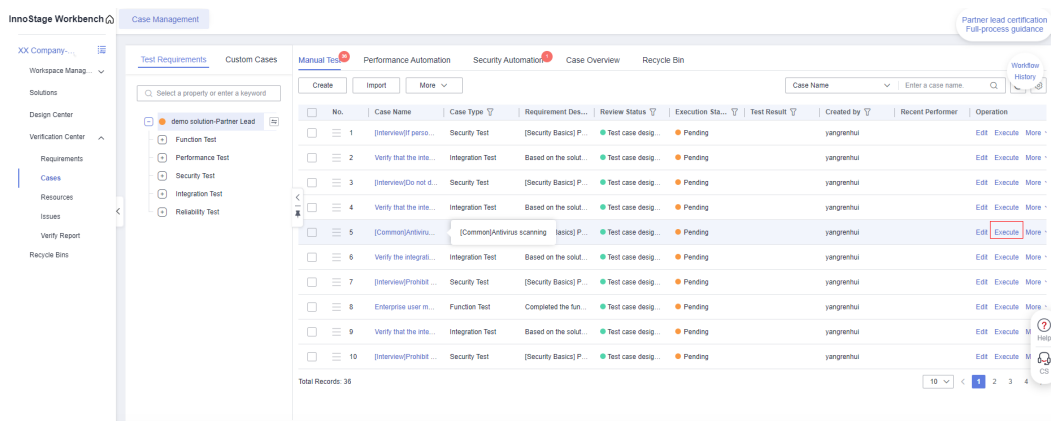
If the scanning has risks, the risk items are displayed in the list. All the risk items need to be resolved and the scanning needs to be performed again.

3. Description of the document corresponding to the false positive file (if any)

Step 5 Enter the execution result.

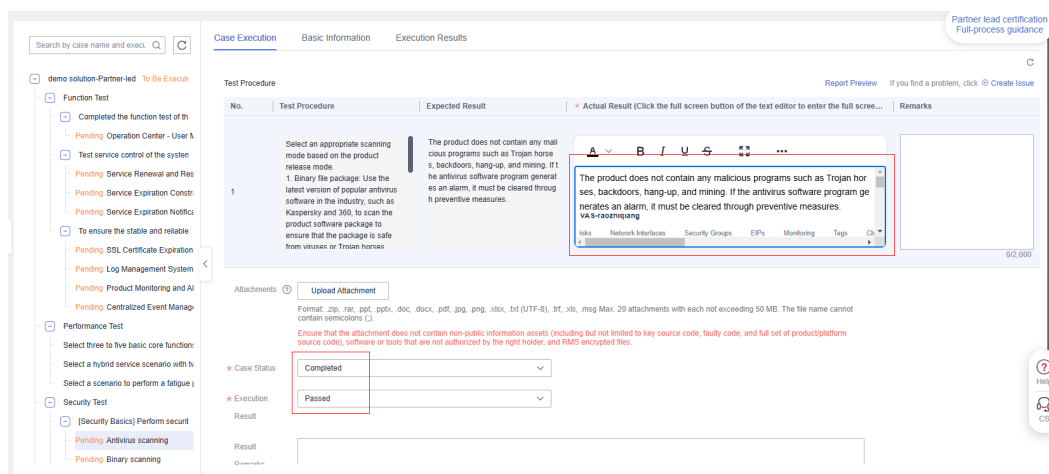
1. Return to InnoStage Workbench and click the execution button of the "Antivirus scanning" case. The execution page is displayed.

Figure 1-114 Test Case Management



2. If the test case is successfully executed, copy the content in the expected result to the actual result, paste the screenshot obtained in step 5 to the actual result, and click OK.

Figure 1-115 Test Case Execution



----End

Binary Virus Scanning(non-image)

Download and install the official **Kaspersky** software in Windows to perform a full scan.

Step 1 Download (Kaspersky)

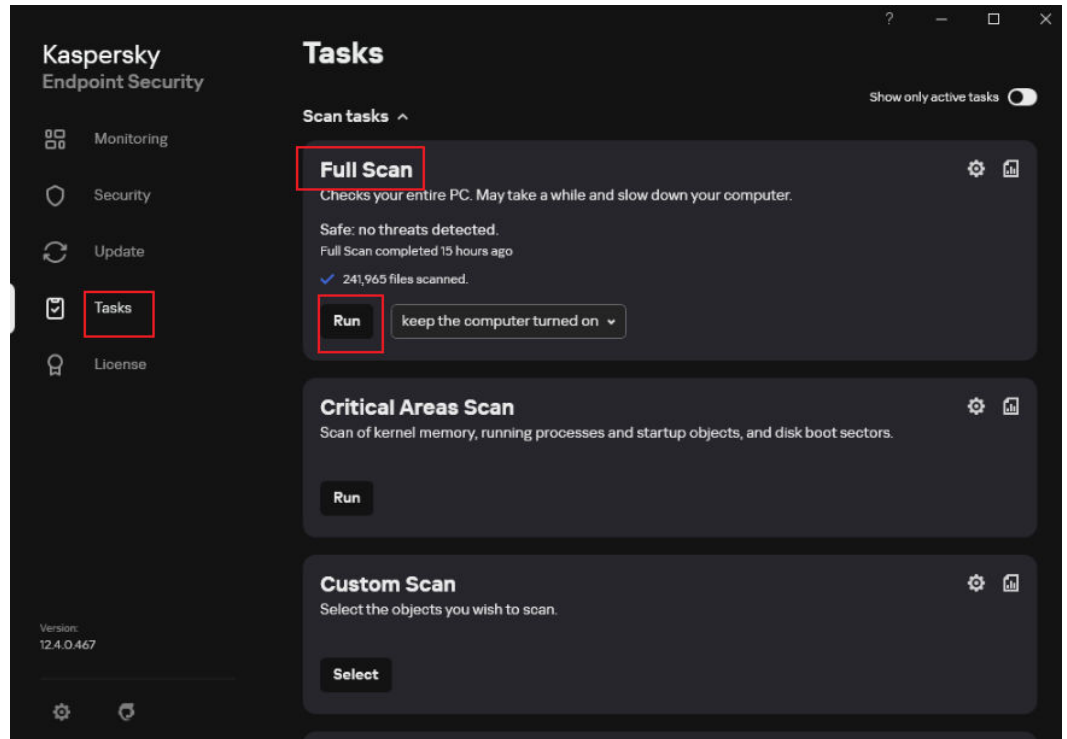
Kaspersky download address reference (with a 30-day trial period after download):<https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint>

Select Kaspersky Endpoint Security for Windows and select Kaspersky Endpoint Security for Windows Version 12.4.0.467 | Windows | Distributive | Lite encryption for the version.

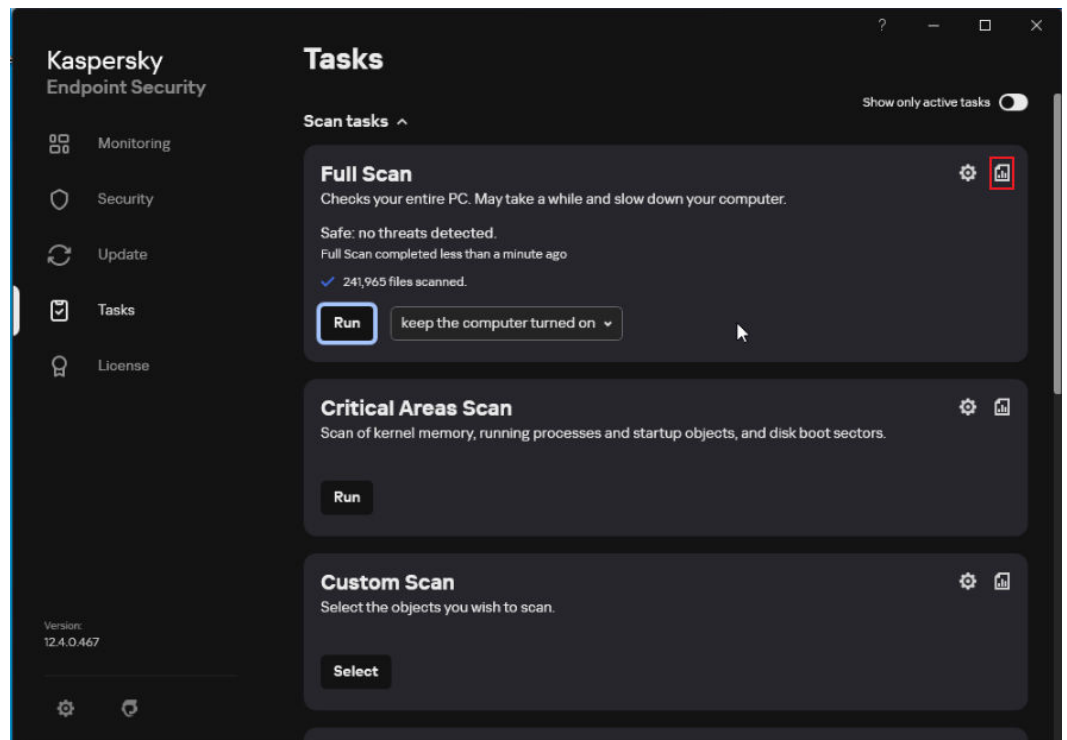
Step 2 Install the Kaspersky reference document:<https://support.kaspersky.com/KESWin/12.4/zh-Hans/141289.htm>

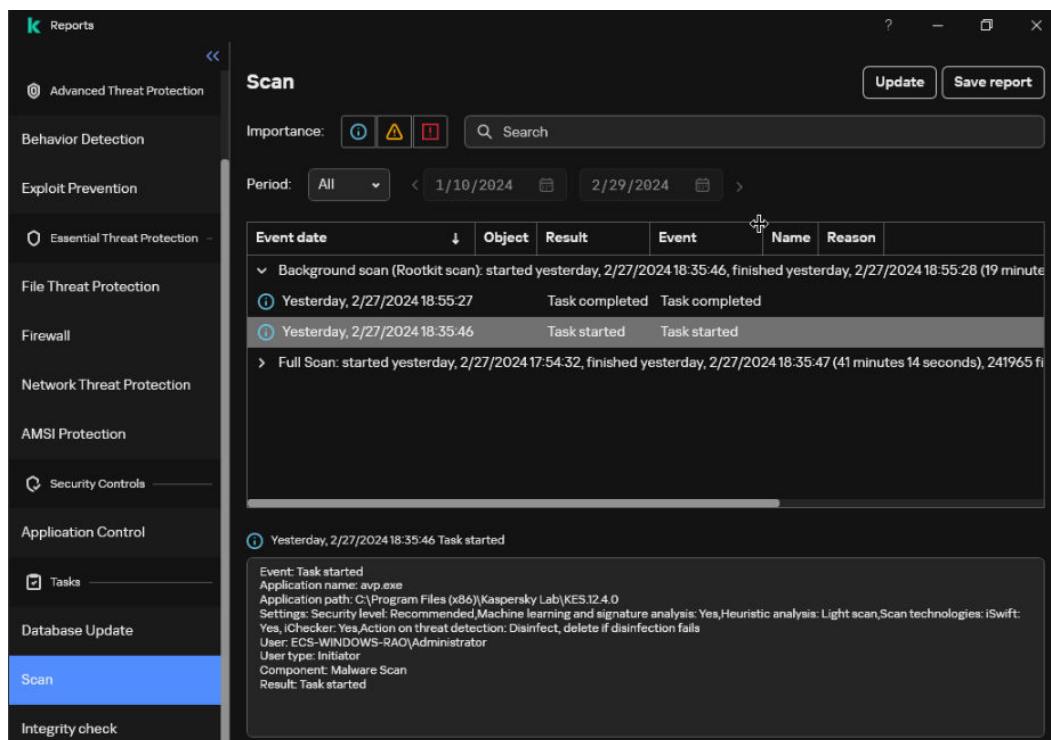
Step 3 Scan operation

1. Start Kaspersky, click Task, and click Run to start the full disk scanning. Wait until the scanning is complete.



2. Check whether the latest scanning result contains risky items.





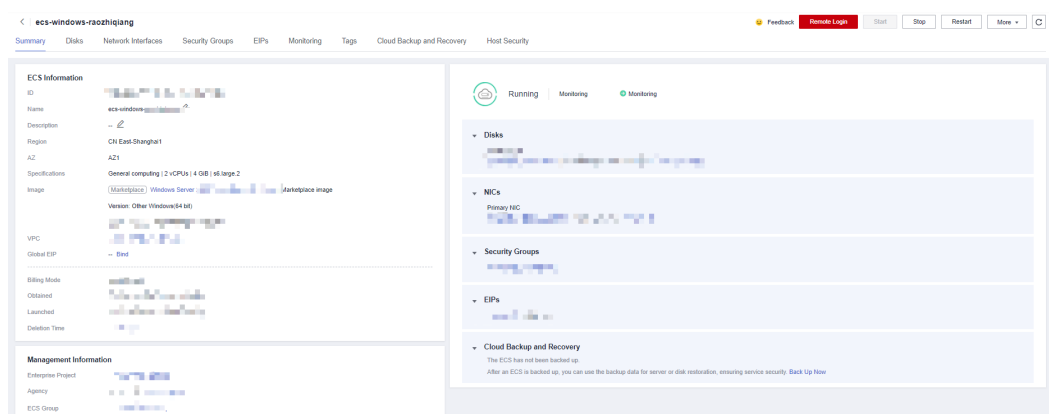
If no problem is found, only the task start and finished information is displayed in the list. If the scanning has risks, the risk items are displayed in the list. All the risk items need to be resolved and the scanning needs to be performed again.

Step 4 Provide scan results

the partner needs to provide the following materials by email: (You do not need to mosaic the screenshot.). The server information in different snapshots must be the same.

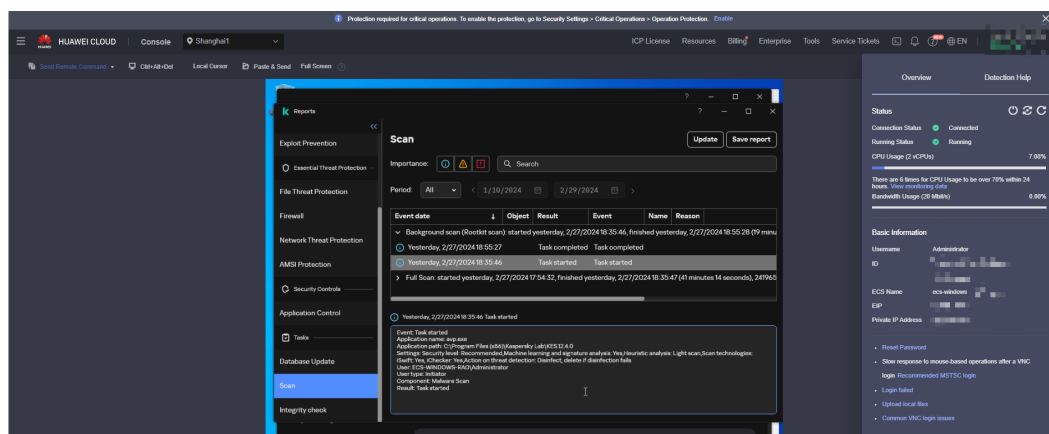
- Screenshot of the scanning server

Figure 1-116



- Screenshot of the final full-disk scanning result (screenshot of the remote login page of the ECS console)

Figure 1-117

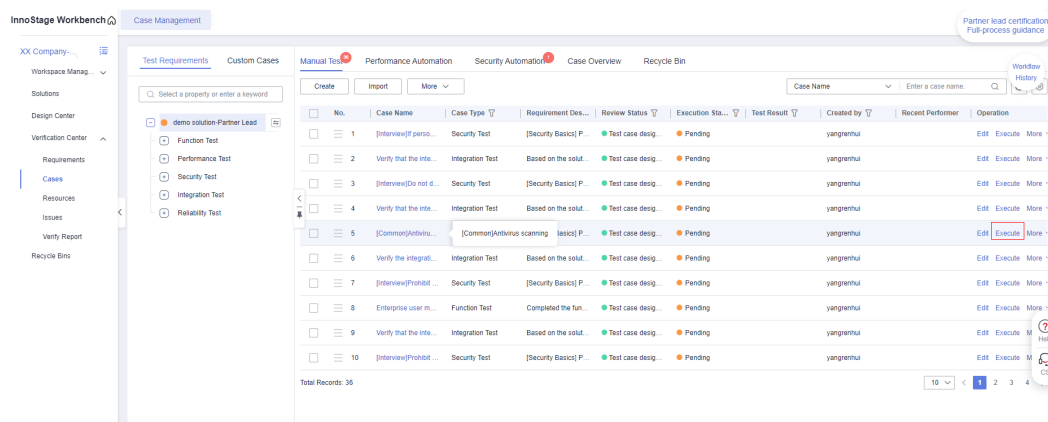
**NOTE**

If the scanning has risks, the risk items are displayed in the list. All the risk items need to be resolved and the scanning needs to be performed again.

- Description of the document corresponding to the false positive file (if any)

Step 5 After the scan is passed, go back to the innostage workbench and enter the case management page. Click the [Execution] button of the binary test case.

Figure 1-118 Test Case Management



Copy the expected result to the actual result, and paste the screenshot in step 4 to the actual result,

Case Status:Completed

Execution Result:Passed

Figure 1-119 Case Execution

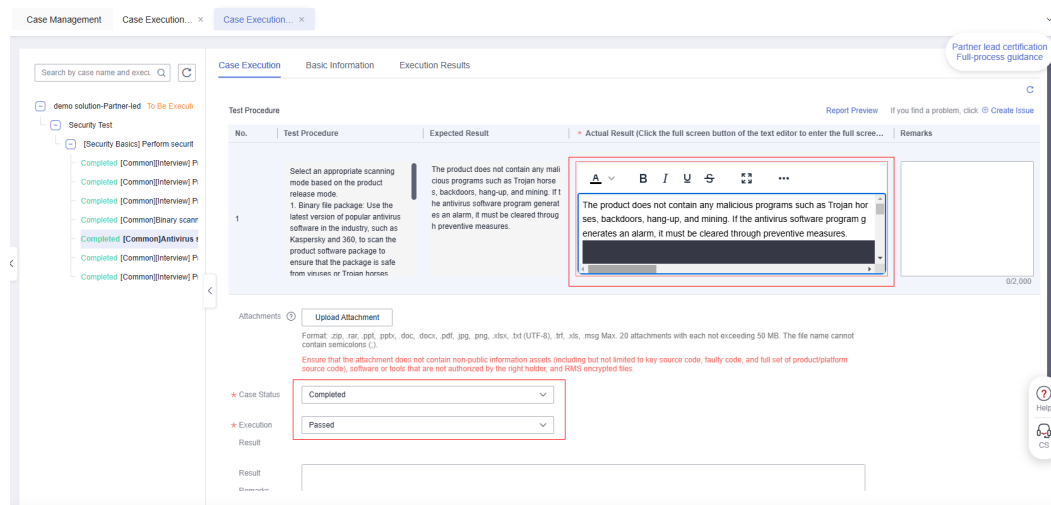


Figure 1-120 Test Case Execution

Step 6 Click[Confirm and go to Next] or click[OK].

----End