# Contents

1 Operation Guide ...................................................................................................................... 1  
2 Enabling VSS ............................................................................................................................. 2  
  2.1 Editions ........................................................................................................................................................................... 2  
  2.2 Buying VSS ............................................................................................................................................................................ 3  
  2.3 Increasing Domain Quotas .................................................................................................................................................. 7  
  2.4 Upgrading to the Advanced Edition ............................................................................................................................... 10  
3 Website Vulnerability Scan ................................................................................................. 12  
  3.1 Adding a Domain Name ..................................................................................................................................................... 12  
  3.2 Verifying a Domain Name ................................................................................................................................................. 16  
  3.3 Configuring Website Login Methods .............................................................................................................................. 21  
  3.4 Creating a Scan Job .............................................................................................................................................................. 25  
  3.5 Viewing the Website Scan Details ................................................................................................................................... 29  
  3.6 Downloading a Website Scan Report ................................................................................................................................... 33  
  3.7 Deleting a Domain Name .................................................................................................................................................. 38  
4 Security Monitoring .............................................................................................................. 40  
  4.1 Adding a Monitoring Job .................................................................................................................................................... 40  
  4.2 Suspending Monitoring ....................................................................................................................................................... 44  
  4.3 Editing a Monitoring Job .................................................................................................................................................... 44  
  4.4 Deleting a Monitoring Job .................................................................................................................................................... 47  
  4.5 Viewing the Security Monitoring List ............................................................................................................................. 47  
  4.6 Viewing Job Details .............................................................................................................................................................. 48  
5 Dashboard ........................................................................................................................................ 53  
6 Key Operations Recorded by CTS ...................................................................................... 56  
  6.1 Auditable Operations ....................................................................................................................................................... 56  
  6.2 Viewing an Audit Trace ................................................................................................................................................... 56  
A Change History .................................................................................................................... 58
Table 1-1 describes the process to use VSS.

Table 1-1: Process to use VSS

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Buy VSS.</strong></td>
<td>VSS provides basic, professional, and advanced editions for you. You can use services within the quota of the basic edition free of charge. If you choose to use professional or advanced edition, you will be billed based on the pricing mode. For details, see Buying VSS.</td>
</tr>
<tr>
<td><strong>Verify a domain name.</strong></td>
<td>For details, see Authenticating a Domain Name.</td>
</tr>
<tr>
<td><strong>Create a scan job.</strong></td>
<td>You can create a scan job to scan your website. For details, see Creating a Scan Job.</td>
</tr>
<tr>
<td><strong>Create a monitoring job.</strong></td>
<td>You can create a monitoring job to implement asset monitoring. For details, see Adding a Monitoring Job.</td>
</tr>
<tr>
<td><strong>View the scan result.</strong></td>
<td>You can view the scan result on the job details page after the scan is complete. For the website scan result, see Viewing the Website Scan Details.</td>
</tr>
</tbody>
</table>

Vulnerability Scan Service User Guide

1 Operation Guide

Issue 03 (2021-01-14) Copyright © Huawei Technologies Co., Ltd. 1
2 Enabling VSS

2.1 Editions

VSS provides basic, professional, and advanced editions for you. You can use services within the quota of the basic edition free of charge. If you choose to use professional or advanced edition, you will be billed based on the pricing mode.

You can select a service edition based on your business requirements. The following describes the billing modes, functions, and specifications of different VSS editions.

**Table 2-1 Billing modes of different VSS editions**

<table>
<thead>
<tr>
<th>Edition</th>
<th>Supported Billing Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic edition</td>
<td>Free of charge for services within the quota</td>
<td>VSS services (5 domain names; 5 scans per day) provided within the quota of the basic edition are free of charge.</td>
</tr>
<tr>
<td>Professional edition</td>
<td>Yearly/Monthly</td>
<td>In yearly/monthly billing mode, you are billed based on the required duration of your order.</td>
</tr>
<tr>
<td>Advanced edition</td>
<td>Yearly/Monthly</td>
<td></td>
</tr>
</tbody>
</table>

**Table 2-2 Functions of different VSS editions**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Common vulnerability scan</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Re-scan</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------------</td>
<td>----------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Scheduled scan</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Port detection</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Customization of login methods</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Scan of Web 2.0 crawlers</td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Query of vulnerability fixing suggestions</td>
<td>×</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Download of scan reports</td>
<td>×</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Weak password scan</td>
<td>×</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>CVE vulnerabilities scan</td>
<td>×</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Security monitoring</td>
<td>×</td>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>

Table 2-3 Scan quotas supported by VSS service editions

<table>
<thead>
<tr>
<th>Edition</th>
<th>Number of Domains</th>
<th>Number of Scan Times</th>
<th>Duration of a Single Job</th>
<th>Job Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic edition</td>
<td>5</td>
<td>Five times a day</td>
<td>2 hours</td>
<td>Low</td>
</tr>
<tr>
<td>Professional edition</td>
<td>Each scan quota package contains one level-2 domain name or IP address:Port.</td>
<td>Unlimited</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Advanced edition</td>
<td>Each scan quota package contains one top-level domain name or public IP address. There is no limit on the number of second-level domain names or on the port number supported by each public IP address.</td>
<td>Unlimited</td>
<td>High</td>
<td></td>
</tr>
</tbody>
</table>

2.2 Buying VSS

Scenario

This section describes how to buy the VSS professional edition and advanced edition.
If you are a professional edition user and want to upgrade the level-2 domain name quota to the top-level domain name quota, you can directly upgrade the professional edition to the advanced edition.

VSS does not support the using of multiple editions at the same time.

**Prerequisites**

You have obtained the login account (with the **VSS Administrator** and **BSS Administrator** permissions) and password for logging in to the management console.

**Procedure**

**Step 1** Log in to the management console.

**Step 2** In the upper left corner of the page, click , select a region or project, and choose **Security > Vulnerability Scan Service**.

**NOTE**

- If you use VSS for the first time, you can click **Buy Now** on the left of the page to access the VSS purchase page.
- If you have experienced the basic VSS edition, click **Upgrade** at the upper right corner of the page to access the VSS purchase page.

**Step 3** On the purchase page, set the parameters based on your needs.

- Set **Billing Mode** to **Yearly/Monthly**. **Table 2-4** shows the parameter description. After setting the parameters, go to **Step 4**.

**NOTE**

- If you are a basic edition user, you can continue using functions of the basic edition with a maximum of five domain names added.
- If you want to increase your domain quotas in the professional, advanced, or enterprise edition, the quantity of the scan quota package must be greater than or equal to the existing number of domain names. Increasing domain quotas does not change the expiration time.
VSS provides basic, professional, and advanced editions for you. You can use services within the quota of the basic edition free of charge. If you choose to use professional or advanced edition, you will be billed based on the pricing mode.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edition</td>
<td>VSS provides basic, professional, and advanced editions for you. You can use services within the quota of the basic edition free of charge. If you choose to use professional or advanced edition, you will be billed based on the pricing mode.</td>
</tr>
<tr>
<td>Specifications</td>
<td>Functions provided by your chosen edition.</td>
</tr>
</tbody>
</table>
| Required Duration| - Professional edition  
                  - One month to three years can be set.                                |
|                  | - Advanced edition  
                  - One month to three years can be set.                                |
### Parameter | Description
--- | ---
Scan Quota Package | - **Scan Quota Package** needs to be configured if you select the **Professional** edition. Each scan quota package contains one second-level domain name or public IP address. There is no limit on the port number supported by each public IP address. The value of **Scan Quota Package** cannot be less than the existing number of websites in the asset list.

**NOTICE**
- If you have used Basic Edition before purchasing Professional Edition, set **Scan Quota Package** to a number greater than or equal to the existing number of websites in the asset list.
- If you do not want to upgrade an existing domain name to Professional Edition, delete it before purchasing Professional Edition.
- If you only want to upgrade all domain names of Basic Edition to Professional Edition, set **Scan Quota Package** to a number equal to the existing number of websites in the asset list.
- If you want to scan more websites, set **Scan Quota Package** to your desired number, which must be greater than the existing number of websites in the asset list.
- Once Professional Edition is purchased, all existing domain names of Basic Edition are upgraded to Professional Edition by default.

- **Scan Quota Package** needs to be configured if you select the **Advanced** edition. Each scan quota package contains one top-level domain name or public IP address. There is no limit on the number of second-level domain names or on the port number supported by each public IP address.

---

**Step 4** In the lower right corner of the page, click **Next**.

⚠️ **NOTE**
For any doubt about the pricing, click **Price Details**.

**Step 5** Confirm your order and read the *HUAWEI CLOUD Vulnerability Scan Service Agreement*. If you agree to the agreement, select **I have read and agree to the HUAWEI CLOUD Vulnerability Scan Service Agreement** and click **Pay Now**.

If the order is incorrect, click **Previous** to go back to the last step and modify your order.

**Step 6** On the **Pay** page, select a payment method to pay for your order.

----End
2.3 Increasing Domain Quotas

Scenario

This section guides you to increase domain quota if you have purchased the professional edition or advanced edition.

**NOTICE**

- If you have used Basic Edition for scanning, all existing domain names of Basic Edition occupy the domain quota of Professional Edition when your purchase Professional Edition.

Prerequisites

- You have obtained the login account (with the VSS Administrator and BSS Administrator permissions) and password for logging in to the management console.
- You have purchased VSS professional edition or advanced edition.

Increasing the Quota of the Professional Edition

**Step 1** Log in to the management console.

**Step 2** Access the page for upgrading the specifications of the professional edition.

**Figure 2-3** Navigation path for accessing the upgrade page of the professional edition

**Step 3** Set the quota.
Click \( + \) in **Scan Quota Package** to increase the scan quota package quantity.

**NOTE**

- **Scan Quota Package** indicates the number of domain names or IP addresses. Currently, its value ranges from 1 to 100.
- The number of required **Scan Quota Package** must be greater than the existing number of domain names.
- Each scan quota package contains one second-level domain name or public IP address.

**Step 4** In the lower right corner of the page, click **Next**.

**NOTE**

For any doubt about the pricing, click **Price Details**.

**Step 5** Confirm your order and read the **HUAWEI CLOUD Vulnerability Scan Service Agreement**. If you agree to the agreement, select **I have read and agree to the HUAWEI CLOUD Vulnerability Scan Service Agreement** and click **Apply Now**.

If the order is incorrect, click **Previous** to go back to the last step and modify your order.

**Step 6** On the **Pay** page, select a payment method to pay for your order.

----End
Increasing the Quota of the Advanced Edition

Step 1  **Log in to the management console.**

Step 2  Access the upgrade page of the advanced edition.

**Figure 2-5** Navigation path for accessing the upgrade page of the advanced edition

Step 3  Set the quota.

**Figure 2-6** Quota increase for the advanced edition

Click + in **Scan Quota Package** to increase the scan quota package quantity.
Step 4 In the lower right corner of the page, click Next.

NOTE
For any doubt about the pricing, click Price Details.

Step 5 Confirm your order and read the HUAWEI CLOUD Vulnerability Scan Service Agreement. If you agree to the agreement, select I have read and agree to the HUAWEI CLOUD Vulnerability Scan Service Agreement and click Apply Now.

If the order is incorrect, click Previous to go back to the last step and modify your order.

Step 6 On the Pay page, select a payment method to pay for your order.

---End

2.4 Upgrading to the Advanced Edition

If you are a professional edition user and want to upgrade the level-2 domain name quota to the top-level domain name quota, you can directly upgrade the professional edition to the advanced edition.

This section describes how to upgrade the professional edition to the advanced edition.

Prerequisites
- You have obtained the login account (with the VSS Administrator and BSS Administrator permissions) and password for logging in to the management console.
- VSS professional edition has been purchased.

Upgrading to the Advanced Edition

Step 1 Log in to the management console.

Step 2 In the upper left corner of the page, click , select a region or project, and choose Security > Vulnerability Scan Service.

Step 3 On the displayed page, click Upgrade to go to the upgrade page.

Step 4 On the displayed page, select Advanced for Edition and specify the Scan Quota Package.
Click + in **Scan Quota Package** to increase the scan quota package quantity.

**NOTE**

- **Scan Quota Package** indicates the number of domain names or IP addresses. Currently, its value ranges from 1 to 100.
- By default, the number in the **Scan Quota Package** field is the number of professional edition quotas.
- The number in the **Scan Quota Package** field can be greater than or equal to the current professional edition quota. VSS supports the upgrading of only all the professional edition quotas.
- Each scan quota package contains one top-level domain name or public IP address.

**Step 5** Confirm your order and read the *HUAWEI CLOUD Vulnerability Scan Service Agreement*. If you agree to the agreement, select *I have read and agree to the HUAWEI CLOUD Vulnerability Scan Service Agreement* and click *Apply Now*. If the order is incorrect, click *Previous* to go back to the last step and modify your order.

**Step 6** On the *Pay* page, select a payment method to pay for your order.

----End
3 Website Vulnerability Scan

3.1 Adding a Domain Name

This section describes how to add a domain name. Before using VSS, add a domain name or IP address to VSS and verify domain ownership so that VSS can perform scanning.

If your website contains web pages only accessible to logged-in users, configure the website login method (username and password or cookie) before using VSS.

⚠️ NOTE

During domain name addition, if the message "The number of domain names that can be added to the current package has reached the maximum allowed limit" is displayed and no domain name can be added, perform the following operations:

- Expand the domain name quota by referring to Increasing Domain Quotas. When you purchase Scan Quota Package, its value must be greater than the existing quota of the current version.
- If your asset list contains domain names that do not need to be protected, delete them and then add new ones.

Prerequisites

Login credentials have been obtained.

Procedure

- **Step 1**  Log in to the management console.
- **Step 2**  Go to Add Domain Name page by following the steps in Figure 3-1.
In the upper corner of the list, you can view the number of domain names that can be added.

**Step 3** In the displayed dialog box, set **Domain Name/IP Address** and **Remarks**.

**NOTE**

VSS scans domain names through the public network/IP address. Ensure that the target domain name/IP address can be accessed through the public network. For details about how to scan private domain names, see **Scanning Websites on an Internal Network**.
**Step 4** Click OK and verify the domain name.

![NOTE]

- If you do not want to verify the domain name ownership temporarily, close the dialog box. You can verify the domain name ownership later by referring to Verifying a Domain Name.
- If the server of your site to be detected is deployed on HUAWEI CLOUD and you own the server, you can select one-click verification.
- File verification

![Figure 3-3 File Verification]

**Figure 3-3 File Verification**

- One-click verification

![Figure 3-4 One-Click Verification]

**Figure 3-4 One-Click Verification**

Select I have read and agree to the HUAWEI CLOUD Vulnerability Scan Service Agreement. Click Verify. The domain name status changes to Verified if verification succeeds.

**Step 5** Configure website information by referring to Table 3-1.
● If some web pages are only accessible to logged-in users, configure login settings so that VSS can perform a full scan. For details about configuring login settings, see Configuring Website Login Methods.

● VSS provides two login methods: username/password and cookie. To improve the login success rate, configure both methods.

Figure 3-5 Website Login Settings

Table 3-1 Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Example Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Login method 1: Username and password</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Login Page</td>
<td>Address of the website login page</td>
<td><a href="https://auth.example.com/">https://auth.example.com/</a></td>
</tr>
<tr>
<td>Username</td>
<td>Username for logging in to the website</td>
<td>vsstest</td>
</tr>
<tr>
<td>Password</td>
<td>Password for logging in to the website</td>
<td>None</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Enter the password again.</td>
<td>None</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Example Value</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Login method 2: Cookies</td>
<td>If login verification is enabled on your website, you must configure the cookie login method.</td>
<td></td>
</tr>
<tr>
<td>Cookie Value</td>
<td>Cookie value of the website</td>
<td>domain_tag</td>
</tr>
</tbody>
</table>

**Website Login Verification**

| Website Address | Enter a website that is only accessible to logged-in users for VSS to quickly determine whether your login information is valid. | https://console.example.com/ |

**Step 6** Read *HUAWEI CLOUD Vulnerability Scan Service Agreement* and check I have read and agree to the HUAWEI CLOUD Vulnerability Scan Service Agreement. Click OK.

----End

**Follow-up Procedure**

After setting the website login methods, you can then create a scan job. For details, see *Creating a Scan Job*.

**Related Operations**

- Can the Verification File in the Root Directory of the Website Be Deleted After Domain Name Verification Is Complete?
- Why Does Domain Name Verification Fail?
- Why Is the Verification File Not Displayed After I Click Download Verification File?
- Can I Delete an Existing Domain Name?

**3.2 Verifying a Domain Name**

This section describes how to verify a domain name.

**Prerequisites**

- Login credentials have been obtained.
- The domain name status is Pending verification.

**Procedure**

**Step 1** Log in to the management console.

**Step 2** Go to the domain name verification page by following the steps in *Figure 3-6*. 
Step 3 In the **Verify Domain Ownership** dialog box, select the domain verification mode to complete domain name verification.

- File verification. See **Figure 3-7**.

**Figure 3-7** File Verification

- One-click verification. See **Figure 3-8**.
Step 4 Read **HUAWEI CLOUD Vulnerability Scan Service Agreement** and check I have read and agree to the HUAWEI CLOUD Vulnerability Scan Service Agreement. Click Verify.

After the operations are complete, the domain name status becomes **Verified**.

-----End

Example for Configuring the Root Directory of the Website to Which a Verification File Is to Be Uploaded

During domain name verification, upload the downloaded verification file to the root directory of the website. The file upload location varies according to the server used by the user. To upload a verification file, perform the following steps based on the corresponding scenario. The following scenarios cannot cover all scenarios. If another scenario is involved, perform operations based on the corresponding scenario.

**Scenario 1: The website is deployed on the Tomcat, Apache, IIS, or WebLogic server.**

Perform the following steps:

**Step 1** Log in to your web server.

If you are not user root, run the `su -root` command to switch to user root.

**Step 2** Go to the root directory of the server hosting your website. **Table 3-2** lists the root directories of common servers.

<table>
<thead>
<tr>
<th>Server Used by a Website</th>
<th>Root Directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tomcat</td>
<td>Tomcat deployment address/webapps/ROOT/</td>
</tr>
<tr>
<td>Apache</td>
<td>The default value is <code>/var/www/html</code>. Set the directory based on the site requirements.</td>
</tr>
<tr>
<td>IIS</td>
<td>The default value is C:\inetpub\wwwroot. Set the directory based on the site requirements.</td>
</tr>
</tbody>
</table>
Server Used by a Website | Root Directory
---|---
WebLogic | The default value is `/applications/DefaultWebApp/`. Set the directory based on the site requirements.

**Step 3**  Save the verification file to the directory found in **Step 2**.

**NOTE**  
The following is an example for your reference only.

Example:
1. Run the `cd root directory` command to go to the root directory of the server.
2. Run the `vi hwwebscan_verify.html` command to create a file with the same name as the verification file.
3. Press `i` to enter the edit mode.  
   Paste the content of the verification file here.
4. Press `Esc` to exit the editing mode, and then run the `:wq` command to save the settings and exit.
5. Enter `ll` to check whether the verification file is successfully uploaded.

**Figure 3-9 Example**

```
[root@S3X1000429182 ~]# cd /opt/ampp/htmldocs
[root@S3X1000429182 htmldocs]# vi hwwebscan_verify.html
[root@S3X1000429182 htmldocs]# ll
```

**Step 4**  Enter `domain name/hwwebscan_verify.html` in the address box of the browser to check whether the verification file is uploaded. If the file can be accessed, the upload is successful.

---End

**Scenario 2: The website is deployed on the Nginx server.**

Perform the following steps to redirect the access to hwwebscan_verify.html to a local file:

**Step 1**  Log in to the Nginx server.

If you are not user `root`, run the `su -root` command to switch to user `root`.

**Step 2**  Upload the verification file to any directory (the Nginx process only has the read permission on this directory). The following uses the `/opt/mock` directory as an example.
Example:

1. Run the `cd /opt/mock` command to open the `/opt/mock` directory.
2. Run the `vi hwwebscan_verify.html` command to create a file with the same name as the verification file.
3. Press `i` to enter the edit mode.
   Paste the content of the verification file here.
4. Press `Esc` to exit the editing mode, and then run the `:wq` command to save the settings and exit.

**Step 3** Open the `nginx.conf` file and configure the location information of the HTTP module of Nginx. After the configuration is successful, you can read the verification file from the `/opt/mock` directory.

1. Run the `vi nginx.conf` command to open the `nginx.conf` file.
2. Modify the following content based on site requirements and overwrite the original HTTP module.

```
http {
  default_type "application/json;charset=utf-8";
  server {
    listen ${your website port};# Replace with the actual value.
    location /hwwebscan_verify.html {
      ${user} /opt/mock;
    }
  }
}
```

**Figure 3-10** Configuration of location information

---

Copyright © Huawei Technologies Co., Ltd.
**3.3 Configuring Website Login Methods**

**Scenario**

This section describes how to configure the website login method and modify the website information in VSS.

If your website is accessible to logged-in users only, configure login parameters so that VSS performs a thorough scan. VSS provides two login methods. Select one based on your website access restrictions.

- **Method 1: username and password**
  
  If your website requires only a username and password for logins, use method 1.

- **Method 2: cookie**
  
  If your website requires other authentication methods, such as dynamic verification code, in addition to usernames and passwords, select method 2 and set cookies.

**NOTICE**

- If no cookies are available, add your own header in the **Advanced Settings** area for login scanning.
- If no cookies and headers are set, VSS cannot scan the website.

To improve the login success rate, select both login methods.

**Prerequisites**

- Login credentials have been obtained.
- A domain name has been added.

**Procedure**

1. **Log in to the management console.**
2. Go to the website login setting page by following the steps in **Figure 3-11**.
Step 3  On the page for editing a domain name, modify the website information and website login settings, as shown in Figure 3-12. Table 3-3 describes the parameters.
Figure 3-12 Edit page

### Edit Website Information

**Basic Information**

- **Domain Name/IP Address**: http://
- **Remarks**: scan_x

**Login Settings**

If your site includes content that is only accessible to logged-in users, VSS will need login credentials to scan that content. VSS can log in using a username and password or cookies. If your entire website is accessible to all users, these fields are not required.

**Login method 1: Username and password**

- **Login Page**: https://auth.example.com
- **Username**: vsstest
- **Password**: 
- **Confirm Password**: 

**Login method 2: Cookies**

- **Cookie Value**: domain_tag

**Website Login Verification**

Enter the address of a page that is only accessible to logged-in users so that VSS can test the login credentials you have supplied.

- **Website Address**: https://console.example.com

- **Advanced Settings**

- **Set Header**: Key value

- **I have read and agree to the HUAWEI CLOUD Vulnerability Scan Service Agreement.**

---

Table 3-3 Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Information</td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Domain Name/IP Address</td>
<td>Only domain names/IP addresses in the <strong>Pending verification</strong> state can be changed.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong> After a domain name is verified, the value of <em>Domain Name/IP Address</em> cannot be changed. To change it, delete this domain name, and add the new IP address.</td>
</tr>
<tr>
<td>Remarks</td>
<td>User-defined name for a domain, which can be changed.</td>
</tr>
</tbody>
</table>

**Login Settings**

If your website is accessible to logged-in users only, configure login parameters so that VSS performs a thorough scan.

- If you only need a username and password to log in to the website, use method 1.
- If your website has other access restrictions in addition to username and password, such as to enter a dynamic verification code, use method 2.

There are two login methods. To improve the login success rate, set both of them.

**Login method 1: Username and password**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Page</td>
<td>Address of the website login page</td>
</tr>
<tr>
<td>Username</td>
<td>Username for logging in to the website</td>
</tr>
<tr>
<td>Password</td>
<td>Password for logging in to the website</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Enter the password again.</td>
</tr>
</tbody>
</table>

**Login method 2: Cookies**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cookie Value</td>
<td>Cookie value of the website For details about how to obtain the cookie value of the login website, see <a href="#">How Do I Obtain the Cookie Value of the Website?</a></td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong> If no cookies are obtained for logins, add a custom header in the <em>Advanced Settings</em>. When you add a header, obtain the HTTP request header of the related session. For example, HTTP request headers that contain <em>Token</em> or <em>Session</em>.</td>
</tr>
</tbody>
</table>

**Website Login Verification**
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website Address</td>
<td>Enter a website that is only accessible to logged-in users for VSS to quickly determine whether your login information is valid.</td>
</tr>
</tbody>
</table>

#### Advanced Settings

| Set Header             | Custom request header of HTTP requests. A maximum of five HTTP request headers can be added. If the website to be scanned requires a special HTTP request header, you can configure one. |

---

**Step 4** Read *HUAWEI CLOUD Vulnerability Scan Service Agreement* and check I have read and agree to the *HUAWEI CLOUD Vulnerability Scan Service Agreement*. Click OK.

---

### 3.4 Creating a Scan Job

#### Scenario

This section describes how to create a scan job.

#### Prerequisites

- Login credentials have been obtained.
- The domain name status is **Verified**.
- If a firewall or other security policies are configured for your website, IP addresses used by VSS for website scanning will be blocked mistakenly as malicious attackers. Whitelist the following IP addresses used by VSS for scanning before using VSS:
  114.119.183.22, 159.138.88.163, and 159.138.107.165

#### Procedure

**Step 1** Log in to the management console.

**Step 2** Go to the page for creating a scan job by following the steps in Figure 3-13.
Step 3  On the Create Job page, set the scan parameters based on the description in Table 3-4. Figure 3-14 shows the scan settings.
**Figure 3-14 Creating a scan job**

![Job Information]

**Table 3-4 Description of scan parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Name</td>
<td>Customizable job name</td>
</tr>
<tr>
<td>Website Address</td>
<td>Domain name or IP address to be scanned&lt;br&gt;Select an authenticated domain name from the drop-down list. <strong>NOTICE</strong>&lt;br&gt;VSS scans domain names through the public network/IP address. Ensure that the target domain name/IP address can be accessed through the public network.&lt;br&gt;For details about how to scan private domain names, see <a href="#">Scanning Websites on an Internal Network</a>.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Time to start a scan. This parameter is optional. If you do not set this parameter, the scan starts immediately.</td>
</tr>
</tbody>
</table>
### Parameter Description

**Scan Type**

There are three scan types:

- **Quick Scan**: It takes the least amount of time and detects the fewest vulnerabilities.
- **Standard Scan**: It takes more time and detects more vulnerabilities.
- **Complete Scan**: It takes the longest time and detects the most vulnerabilities.

Some interfaces can be accessed only after login. Configure the username and password of the corresponding interface so that VSS can perform in-depth scanning.

**NOTE**

- In a quick scan, the quantity of website URLs to be scanned is limited, and VSS enables the scan plug-in that takes a short time to scan website URLs.
- In a complete scan, the quantity of website URLs to be scanned is not limited, and VSS enables all scan plug-ins to scan all website URLs, which takes a long time.
- In a standard scan, the number of website URLs to be scanned and time required are between those in a quick scan and those in a complete scan.

**Scan Settings**

Supported scan items. For details, see Table 3-5.

- : indicates that the scan for the item is enabled.
- : indicates that the scan for the item is disabled.

### Table 3-5 Scan settings

<table>
<thead>
<tr>
<th>Scan Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common web security vulnerabilities</td>
<td>Scans for more than 30 common vulnerabilities, such as XSS and SQL injection attacks. This function is enabled by default and cannot be disabled.</td>
</tr>
<tr>
<td>Port</td>
<td>Checks which ports are enabled on a host.</td>
</tr>
<tr>
<td>Weak password</td>
<td>Scans for any weak passwords used on your website.</td>
</tr>
<tr>
<td>CVE vulnerabilities</td>
<td>VSS updates vulnerability rules and scans for the latest CVE vulnerabilities. Common Vulnerabilities and Exposures (CVE) is a security vulnerability database.</td>
</tr>
</tbody>
</table>
● If you have subscribed to Professional Edition, the system does not prompt the upgrade.
● Basic Edition supports common vulnerability scan and port scan. You can create a maximum of five scan jobs each day. One job lasts a maximum of two hours.
● Professional Edition supports common vulnerability scan, port scan, and weak password scan. You can execute up to 60 scan jobs each day.
● Advanced Edition supports common vulnerability scan, port scan, and weak password scan. You can execute up to 60 scan jobs each day.

Step 4 After the settings are complete, click Start Scan.

NOTE
If you do not set the start time and the server is not occupied, the newly created job is executed immediately and its status is In progress. Otherwise, the job waits in the queue and its status is Waiting.

Follow-up Procedure
After the scan job is complete, you can view the website details and download the website scan report. For details, see Viewing the Website Scan Details and Downloading a Website Scan Report.

Related Operations
You may encounter problems when creating a scan job. Here are some methods for you to solve some of your problems.

● How Can I Quickly Detect Website Vulnerabilities?
● Why Does the Automatic Login During a Scan Job Fails?
● Why Is a Job Automatically Canceled in the Job Scan Process?
● Why Am I Frequently Prompted that the Domain Name Format Is Incorrect During Job Creation?
● How Long Does a Scan Take?
● What Should I Do When a Website Scan Fails with a Message Displayed Indicating Connection Timeout?
● What Should I Do If a Website Scan Job Fails to Be Created or Restarted?

3.5 Viewing the Website Scan Details
This section describes how to view the scan results of a website, such as scan summary, content risk list, vulnerability list, port list, and site structure.

VSS does not support web_CMS vulnerability scanning.

Prerequisites
● Login credentials have been obtained.
● A domain name has been added and authenticated.
● A scan job has been completed.

Procedure

**Step 1** Log in to the management console.

**Step 2** Go to the website list page by following steps in Figure 3-15.

![Figure 3-15 Navigation path to the website list page](image)

**Step 3** View the website asset list. **Table 3-6** describes the parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Domain Information         | • Domain Name/IP Address  
• Remarks                       |
| Verification Status        | • Verified
  The target domain name has been verified.
• Pending verification
  The target domain name has not been verified. Click **Verify** to complete ownership verification.
• Certificate expired
  If the certificate is invalid, download the verification file again and complete domain name verification. |
| Last Scan Time             | Time when the last scan job begins                                           |
| Last Scan Result           | Information about the last scan job, including the score and number of vulnerabilities at each level. Click the score or **View Details** to view scan details. |

**Step 4** In the **Last Scan Result** column of the target domain name, click the score or **View Details** to view the scan job details.
By default, the scan job details page displays information about the last scan job. If you want to view details of a job at other time, select a time from Historical Scan Report drop-down list.

To re-execute a scan job, click Scan Again.

To modify the job name or scan item, click Edit.

To download a report of the scan job, click Generate Report after the scan completion and then click in the upper right corner. Currently, only PDF reports are available.

**Figure 3-16 Viewing scan job details**

![Scan Job Details](image)

**Step 5** Click the Scan Summary tab to view the check result of the scan items.

**Figure 3-17 Scan Summary tab**

![Scan Summary](image)
If the check result contains vulnerabilities or risks, click **View Details** in the **Result** column to view details about the vulnerabilities or risks.

**Step 6** Click the **Vulnerability List** tab to view vulnerability information.

**Figure 3-18** Vulnerability List tab page

---

---

- Click **View** on the right to view more.
- Click a vulnerability name to view **Vulnerability Details**, **Vulnerability Overview**, and **Recommended Action**.
- If you confirm that the scanned vulnerability does not affect the website, click **Ignore** in the **Operation** column of the row where the target vulnerability is located. The vulnerability will be scanned in subsequent scan tasks, but the scan results will not include the ignored vulnerability. For example, if you ignore two low-risk vulnerabilities, the number of low-risk vulnerabilities in the scan result will decrease by 2 when you perform the scan task again.
- To restore an ignored vulnerability, click **Unignore** in the **Operation** column.

**Step 7** Click the **Content Risk List** tab to view the content risk information, as shown in **Figure 3-19**.

**Figure 3-19** Content Risk List tab page

---

---

**Step 8** Click the **Port List** tab to view the port information about the target website.

**Figure 3-20** Port List tab page

---

---

**Step 9** Click the **Site Structure** tab to view the site structure of the target website.
The Site Structure tab page shows locations of vulnerabilities in the target website. If no vulnerabilities have been detected, this page is empty.

The tab page displays basic information about the target website, including:

- **IP Address**: IP address of the target website
- **Server**: Name of the server used for deploying the target website (for example, Tomcat, Apache httpd, and IIS)
- **Language**: Development language used by the target website (for example: PHP, Java, and C#.)

![Figure 3-21 Site Structure](image)

Follow-up Procedure

After you fix the website vulnerability, click **Scan Again** on the right of the scan details page. After the website is scanned again, check whether the vulnerability is fixed on the website scan details page.

Related Operations

- For details about how to calculate the website scan score, see **What Does the Score Mean?**
- For details about how to fix vulnerabilities, see **Does VSS Fix Discovered Vulnerabilities?**

3.6 Downloading a Website Scan Report

Scenario

After a website scan job is complete, you can download a website scan report in PDF.
Prerequisites

A website scan job has been completed, and the status of Last Scan Result of the target domain name is Completed.

Procedure

Step 1 Log in to the management console.

Step 2 Go to the page for downloading a website scan report by following the steps in Figure 3-22.

Figure 3-22 Page for downloading a website scan report

Step 3 Click in the upper right corner to generate a website scan report. Figure 3-23 shows an example.

Figure 3-23 Generate Report
NOTE

The generated scan report will expire in 24 hours. To download the scan report after it expires, click Generate Report to generate a latest one.

**Step 4** Generate the latest scan report. Click in the upper right corner to download the website scan report. Figure 3-24 shows an example.

**Figure 3-24** Downloading the website scan report

---End

**Description of the Website Vulnerability Scan Report Template**

After downloading the scan report, you can fix vulnerabilities based on the scan result. The report template is described as follows:

- **Overview**
  
  Check the number of scanned vulnerabilities for the target website.
Figure 3-25 Viewing the task overview

1 Overview

1.1 Task Information

0 vulnerabilities have been detected. These vulnerabilities categorize into 0 types. 0 vulnerabilities are high-risk.

- Task Name: test
- URL: http://example.com
- Started: 16:01:05
- Finished: 16:20:12
- Duration: 0.32 hours

1.2 Website Fingerprint Information

- IP: unknown
- Server: unknown
- Language: unknown
- Open Ports: 22, 8080

- Vulnerability analysis
  Collect statistics on vulnerability types and distribution.
Figure 3-26 Vulnerability type analysis

2 Vulnerability Analysis

2.1 Vulnerability Overview

<table>
<thead>
<tr>
<th>Score and Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Total</strong></td>
</tr>
<tr>
<td>100</td>
</tr>
</tbody>
</table>

2.2 Vulnerability Types

<table>
<thead>
<tr>
<th>Category</th>
<th>Type</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>CrossSiteRequestForge</td>
<td>Safe</td>
<td></td>
</tr>
<tr>
<td>Emergency vulnerability</td>
<td>Safe</td>
<td></td>
</tr>
<tr>
<td>InformationLeakage</td>
<td>Safe</td>
<td></td>
</tr>
<tr>
<td>Injection Attack</td>
<td>Safe</td>
<td></td>
</tr>
<tr>
<td>Others Problems</td>
<td>Safe</td>
<td></td>
</tr>
<tr>
<td>Path Traverse Attack</td>
<td>Safe</td>
<td></td>
</tr>
<tr>
<td>Unauthorized Problems</td>
<td>Safe</td>
<td></td>
</tr>
<tr>
<td>Weak Password</td>
<td>Safe</td>
<td></td>
</tr>
<tr>
<td>Cross Site Scripting</td>
<td>Safe</td>
<td></td>
</tr>
</tbody>
</table>

- Port list
  View information about all ports of the target website.

Figure 3-27 Port list

3 Port List

<table>
<thead>
<tr>
<th>Port</th>
<th>Status</th>
<th>Protocol</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>Open</td>
<td>TCP</td>
<td>Secure Shell (SSH), secure logins, file transfers (scp, sftp) and port forwarding</td>
</tr>
<tr>
<td>8000</td>
<td>Open</td>
<td>TCP</td>
<td>QuickTime Streaming Server</td>
</tr>
</tbody>
</table>

- Vulnerability root cause and details
  You can fix the vulnerabilities based on the suggestions.
3.7 Deleting a Domain Name

Scenario

This section describes how to delete a domain name.

**NOTICE**

Historical scan data associated with the domain name will be deleted together and cannot be restored. Exercise caution when performing this operation.

Prerequisites

- Login credentials have been obtained.
- A domain name has been added.

Procedure

Step 1  **Log in to the management console.**
Step 2  Go to the page for deleting a domain name by following steps in Figure 3-29.

Figure 3-29 Page for deleting a domain name

Step 3  In the displayed dialog box, click OK. If Domain name deleted successfully is displayed, the domain name is deleted.

----End

Related Operations

For details about how to add a domain name, see Adding a Domain Name.
4 Security Monitoring

4.1 Adding a Monitoring Job

Scenario

VSS scans websites for a wide range of vulnerabilities. Your websites are called Assets in VSS. You can scan and edit your assets on the Security Monitoring page.

This section describes how to add a monitoring job. Security monitoring is enabled once a monitoring job is added.

NOTICE

The security monitoring function is not available in basic edition. If you want to use this function, purchase the professional edition or advanced edition.

Prerequisites

- Login credentials have been obtained.
- The domain name status is Verified.

Procedure

Step 1  Log in to the management console.
Step 2  Go to the page for adding a monitoring job by following the steps in Figure 4-1.
Step 3  On the Create Monitoring Job page, set the scan parameters based on the description in Table 4-1. Figure 4-2 shows the example scan settings.
Figure 4-2 Scan settings

Table 4-1 Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job Name</td>
<td>Customizable job name</td>
</tr>
<tr>
<td>Website Address</td>
<td><a href="http://123.291568000">http://123.291568000</a></td>
</tr>
<tr>
<td>Start Time</td>
<td>Select a date and time.</td>
</tr>
<tr>
<td>Scan Type</td>
<td>Standard Scan</td>
</tr>
</tbody>
</table>
### Parameter Description

#### Website Address
- Domain name or IP address to be scanned
- Select an authenticated domain name from the drop-down list.

#### Scan Interval
- Select a value from the drop-down list.
  - Every day
  - Every 3 days
  - Every week
  - Every month

#### Started
- Time to start a monitoring job

#### Scan Mode
- There are three scan types:
  - **Quick Scan**: It takes the least amount of time and detects the fewest vulnerabilities.
  - **Standard Scan**: It takes more time and detects more vulnerabilities.
  - **Complete Scan**: It takes the longest time and detects the most vulnerabilities.

#### Scan Settings
- Supported scan items. For details, see Table 4-2.
  - <: enabled
  - : disabled

### Table 4-2 Scan settings

<table>
<thead>
<tr>
<th>Scan Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common web security vulnerabilities</td>
<td>Scans for more than 30 common vulnerabilities, such as XSS and SQL injection attacks. This function is enabled by default and cannot be disabled.</td>
</tr>
<tr>
<td>Port</td>
<td>Checks which ports are enabled on a host.</td>
</tr>
<tr>
<td>Weak password</td>
<td>Scans for any weak passwords used on your website.</td>
</tr>
<tr>
<td>CVE vulnerabilities</td>
<td>VSS updates vulnerability rules and scans for the latest CVE vulnerabilities. Common Vulnerabilities and Exposures (CVE) is a security vulnerability database.</td>
</tr>
</tbody>
</table>

**Step 4** Click **OK**.
NOTE

If you do not set the start time and the server is not occupied, the newly created job is executed immediately and its status is In progress. Otherwise, the job waits in the queue and its status is Waiting.

----End

4.2 Suspending Monitoring

Scenario

This section describes how to suspend monitoring.

Prerequisites

- Login credentials have been obtained.
- A monitoring job has been started.

Procedure

Step 1 Log in to the management console.

Step 2 Click in upper left corner of the page, choose Vulnerability Scan Service under Security. On the displayed page, choose Security Monitoring in the navigation pane on the left.

Figure 4-3 Security Monitoring page

Step 3 In the Operation column of the target job, click Suspend Monitoring. In the displayed dialog box, click OK.

NOTE

To enable monitoring on the job again, click Enable Monitoring in the Operation column.

----End

4.3 Editing a Monitoring Job

Scenario

This section describes how to edit a monitoring job.

Prerequisites

- Login credentials have been obtained.
● A monitoring job has been created.

Procedure

**Step 1** Log in to the management console.

**Step 2** Click in upper left corner of the page, choose Vulnerability Scan Service under Security. On the displayed page, choose Security Monitoring in the navigation pane on the left.

![Security Monitoring page](image)

**Step 3** In the Operation column of the target monitoring job, click Edit Job.
**Figure 4-5 Scan settings**

Note: If your website is accessible to logged-in users only, go to the asset list to configure login parameters so that we can discover vulnerabilities for your website.

*Job Name*

*Website Address*:
http://29.166.8000

*Start Time*:
Select a date and time.

*Scan Type*:
Standard Scan

---

**Step 4** Reconfigure basic information and scan settings.

----End
4.4 Deleting a Monitoring Job

Scenario

This section describes how to delete a monitoring job.

Prerequisites

- Login credentials have been obtained.
- A monitoring job has been created.

Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner of the page, choose Vulnerability Scan Service under Security. On the displayed page, choose Security Monitoring in the navigation pane on the left.

Step 3 In the Operation column of the target job, click Delete Job. In the displayed dialog box, click OK.

----End

4.5 Viewing the Security Monitoring List

Scenario

This section describes how to view the security monitoring list.

Prerequisites

- Login credentials have been obtained.
- A monitoring job has been created.

Procedure

Step 1 Log in to the management console.

Step 2 Click in the navigation tree on the left, choose Vulnerability Scan Service under Security. On the displayed page, choose Security Monitoring in the navigation pane on the left. Table 4-3 lists related parameters.
4.6 Viewing Job Details

Scenario

This section describes how to view job details.

Prerequisites

- Login credentials have been obtained.
- A monitoring job has been started.

Procedure

1. **Log in to the management console.**

2. Click in the upper left corner of the page, choose **Vulnerability Scan Service** under Security. On the displayed page, choose **Security Monitoring** in the navigation pane on the left.
Step 3 In the Latest Scan Information column of the target monitoring job, click the score or View details. The job details page is displayed, as shown in Figure 4-9.

- By default, the scan job details page displays information about the last scan job. If you want to view details of a job at other time, select a time from Historical Scan Report drop-down list.
- To re-execute a scan job, click Scan Again.
- To modify the job name or scan item, click Edit.
- To download a report of the scan job, click Generate Report after the scan completion and then click in the upper right corner. Currently, only PDF reports are available.

Step 4 Click the Scan Summary tab to view the check result of the scan items.
If the check result contains vulnerabilities or risks, click **View Details** in the **Result** column to view details about the vulnerabilities or risks.

**Step 5**  Click the **Vulnerability List** tab to view vulnerability information.
NOTE

- Click View on the right to view more.
- Click a vulnerability name to view Vulnerability Details, Vulnerability Overview, and Recommended Action.
- If you confirm that the scanned vulnerability does not affect the website, click Ignore in the Operation column of the row where the target vulnerability is located. The vulnerability will be scanned in subsequent scan tasks, but the scan results will not include the ignored vulnerability. For example, if you ignore two low-risk vulnerabilities, the number of low-risk vulnerabilities in the scan result will decrease by 2 when you perform the scan task again.
- To restore an ignored vulnerability, click Unignore in the Operation column.

Step 6  Click the Content Risk List tab to view the content risk information, as shown in Figure 4-12.

Figure 4-12 Content Risk List tab page

Step 7  Click the Port List tab to view the port information about the target website.

Figure 4-13 Port List tab page

Step 8  Click the Site Structure tab to view the site structure of the target website.

NOTE

The Site Structure tab page shows locations of vulnerabilities in the target website. If no vulnerabilities have been detected, this page is empty.

The tab page displays basic information about the target website, including:
- **IP Address**: IP address of the target website
- **Server**: Name of the server used for deploying the target website (for example, Tomcat, Apache httpd, and IIS)
- **Language**: Development language used by the target website (for example: PHP, Java, and C#.)
Figure 4-14 Site Structure

No data available.

----End
5 Dashboard

Scenario

This section describes how to view the website scanning summary on the Dashboard page, including the asset information, latest scan result, and latest scan job list.

Prerequisites

- Login credentials have been obtained.
- You have added a website.

Taking an Overview

Step 1 Log in to the management console.

Step 2 In the navigation pane on the left, click Security > Vulnerability Scan Service to go to the Dashboard page.

Step 3 View the scanning overview.
- View the assets. Table 5-1 lists asset parameters.

Figure 5-1 Asset information
## Table 5-1 Asset parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Websites</td>
<td>Displays the total number of websites, and number of authenticated/unauthenticated websites.</td>
<td>- Click the number to go to the corresponding asset list.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE</strong></td>
<td>- Displays the number of authenticated/unauthenticated websites.</td>
</tr>
<tr>
<td></td>
<td>If the total number of websites is 0, click <strong>Add Asset</strong> to go to the asset list page to add a website.</td>
<td></td>
</tr>
<tr>
<td>Website Risk Statistics</td>
<td>Displays risk details of all websites.</td>
<td>--</td>
</tr>
<tr>
<td>Most Vulnerable Website</td>
<td>- The website with the lowest score is the most vulnerable website.</td>
<td>- Click <strong>Most Vulnerable Website</strong>.</td>
</tr>
<tr>
<td></td>
<td>- If two websites have the same score, the website with the maximum number of high-risk vulnerabilities is the most vulnerable website.</td>
<td>- The latest scan job details of the website are displayed.</td>
</tr>
<tr>
<td></td>
<td>- If the score of all scanned websites is 100, there is no most vulnerable website. This field is displayed as --.</td>
<td>- Risk levels are: <strong>High</strong>, <strong>Medium</strong>, <strong>Low</strong>, and <strong>Informational</strong>.</td>
</tr>
<tr>
<td></td>
<td>- Displays the number of website risks by risk severity level</td>
<td></td>
</tr>
</tbody>
</table>

- View the latest scan information. **Table 5-2** lists related parameters.

### Figure 5-2 Latest scan information

![Latest scan information](image)

**NOTE**

- If a scan job is not finished, only its status is displayed, such as **Waiting** and **InProgress**.
- If a scan job fails, details about the last successful scan job are displayed.
Table 5-2 Parameter description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>Website to be scanned</td>
<td>Click the website to view job details.</td>
</tr>
<tr>
<td>Started</td>
<td>Time when a scan job begins</td>
<td>--</td>
</tr>
<tr>
<td>Duration</td>
<td>How long a scan job lasts</td>
<td>--</td>
</tr>
<tr>
<td>Status</td>
<td>Completed</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>In progress</td>
<td>--</td>
</tr>
<tr>
<td></td>
<td>Waiting</td>
<td>--</td>
</tr>
<tr>
<td>Vulnerabilities</td>
<td>Displays the number of website risks by risk severity level</td>
<td>Risk levels are: <strong>High</strong>, <strong>Medium</strong>, <strong>Low</strong>, and <strong>Informational</strong></td>
</tr>
<tr>
<td>Top Risks</td>
<td>Sorts from high vulnerabilities to low in a descending order.</td>
<td>--</td>
</tr>
</tbody>
</table>

- View the list of the latest scan jobs. Table 5-3 lists the parameters.

Figure 5-3 List of the latest scan jobs

Table 5-3 Job list parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>Website to be scanned</td>
<td>Click the website to view job details.</td>
</tr>
<tr>
<td>Number of Vulnerabilities</td>
<td>Displays the total number of vulnerabilities detected in a website.</td>
<td>--</td>
</tr>
<tr>
<td>Status</td>
<td>The options are <strong>Waiting</strong>, <strong>In Progress</strong>, and <strong>Completed</strong>.</td>
<td>--</td>
</tr>
<tr>
<td>Started</td>
<td>Time when a scan job begins</td>
<td>--</td>
</tr>
<tr>
<td>Duration</td>
<td>How long a scan job lasts</td>
<td>--</td>
</tr>
</tbody>
</table>
6 Key Operations Recorded by CTS

6.1 Auditable Operations

Table 6-1 lists VSS operations recorded by CTS.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Resource Type</th>
<th>Trace Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a scan job</td>
<td>SCAN</td>
<td>createScanTask</td>
</tr>
<tr>
<td>Adding a domain name</td>
<td>DOMAIN</td>
<td>createDomain</td>
</tr>
<tr>
<td>Deleting a domain name</td>
<td>DOMAIN</td>
<td>deleteDomain</td>
</tr>
</tbody>
</table>

6.2 Viewing an Audit Trace

After you enable CTS, the system starts recording operations on VSS. Operation records for the last seven days can be viewed on the CTS console.

Viewing a VSS Trace on the CTS Console

Step 1 Log in to the management console.

Step 2 In the navigation pane on the left, click and choose Management & Deployment > Cloud Trace Service.

Step 3 Choose Trace List in the navigation pane.

Step 4 Click Region at the top of the Trace List page to set the corresponding conditions.

You can query traces using a combination of the following dimensions:
• **Trace Type, Trace Source, Resource Type, and Search By.**
  
  – Select the filter from the drop-down list. Set Trace Source to VSS.
  
  – When you select **Trace name** for Search By, you also need to select a specific trace name.
  
  – When you select **Resource ID** for Search By, you also need to select or enter a specific resource ID.
  
  – When you select **Resource name** for Search By, you need to select or enter a specific resource name.

• **Operator**: Select a specific operator (a user rather than tenant).

• **Trace Status**: Available options include **All trace statuses, normal, warning, and incident**. You can only select one of them.

• In the upper right corner of the page, you can query traces in the last 1 hour, last 1 day, last 1 week, or within a customized period.

**Step 5** Click **Query**.

**Step 6** Click on the left of a trace to expand its details.

**Figure 6-1** Expanding trace details

![Figure 6-1 Expanding trace details](image)

**Step 7** Click **View Trace** in the Operation column. On the displayed View Trace dialog box shown in **Figure 6-2**, the trace structure details are displayed.

**Figure 6-2** Viewing a trace

![Figure 6-2 Viewing a trace](image)
## Change History

<table>
<thead>
<tr>
<th>Released On</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2020-01-14</td>
<td>This issue is the third official release. Added descriptions of scanning of customized Header in <a href="#">Configuring Website Login Methods</a>.</td>
</tr>
<tr>
<td>2020-10-22</td>
<td>This issue is the second official release. Added the procedure for generating a scan report in <a href="#">Downloading a Website Scan Report</a>.</td>
</tr>
<tr>
<td>2020-04-23</td>
<td>This issue is the first official release.</td>
</tr>
</tbody>
</table>