HECTOR Instruction Manual-

V1.0

Table of contents

Chapter 1 Overview

Hector remote control system is a remote control system that supports HTTP/WEB SOCKET, HTTPS/WEB SOCKET over TLS protocols, and uses reverse connection;

The remote control system supports interactive shell command line, file management and other functions:

Chapter 2 Glossary

➢ WEB SOCKET protocol (referred to as WS):

WebSocket is a network transport protocol that enables full-duplex communication over a single TCP connection and is located at the application layer of the OSI model. WebSocket makes data exchange between the client and the server simpler, allowing the server to actively push data to the client. In the WebSocket API, the browser and the server only need to complete a handshake, and a persistent connection can be created between the two for bidirectional data transmission.

The difference from the http protocol is that the http protocol server does not support actively sending requests to the client, while the WEB SOCKET protocol allows the server to actively push data to the client;

➢ WEB SOCKET over TLS (WSS for short):

The security design of the WebSocket protocol stipulates transmission based on TLS/SSL. This encryption form is similar to HTTPS and is called WSS (WEB SOCKET over TLS).

That is, high-level application layer protocols can be transparently built on top of the TLS protocol. The TLS protocol has completed the encryption algorithm, communication key negotiation and server authentication before application layer protocol communication. After this, the data transmitted by the application layer protocol will be encrypted to ensure the privacy of communication.

> Controlled terminal (client): the target machine (Linux system) where the Trojan program is installed.

>Control terminal (console): the main program that manages the controlled terminal host (windows system).

> Reverse connection: Rebound online method, that is, after the Trojan program on the controlled terminal is installed, it will actively connect to the controlling terminal.

Chapter 3 Product Functions

1. Communication protocol: supports HTTP/WEB SOCKET, HTTPS/WEB SOCKET over TLS protocol:

2. Remote control function:

1)Interactive shell command line:

2) File directory browsing

View graphically and support direct execution of an executable file;

Supports directly entering absolute paths to browse specified directories:

supports recording recently entered path information

3)File transfer

File upload, download, run, delete, small file content viewing, etc.; supports

breakpoint resumption, supports pausing, starting, and deleting transfer tasks

3. Host management function: Management of online hosts, supporting group management, modifying notes, modifying groups, etc.

4. Host log: record target host name, user name, online IP, online time, offline time, host base hardware information and

other data:

Chapter 4 Product Features and Parameters

Hector remote control system				
Configuration list	Quantity: One set of software (client, control terminal)			
index	Product form	☑Pure software □ Hardware-integration □System equipment	Product source	☑Independent research and development □Technical transformation □Product introduction
Basic parameters	Basic parameters			
	system structure	CS Architecture	target operating system	Centos, ubuntu
Remote control features	Start mode	Application layer startup, stable and reliable		
	Internet connection	Supports reverse connections of HTTP/WEB SOCKET and HTTPS/WEB SOCKET over TLS protocols;		
	File management	File directory browsing, file upload, download, delete, refresh and run.		
	Shell command	interactive shell command		

Chapter 5 Applicable Environment

program	Supported operating systems
Control program	Win 2003, Win 7, Win 10, Win 2008, Win2012 systems (also supports 32/64-bit systems);
Controlled end program	x64: Centos 5, 6, 7: ubuntu 14, 16, 18:

Note: Systems supported by the controlled terminal: Centos 5, 6, 7; ubuntu 14, 16, 18; refers to the large version number, including centos 5.xxx, 6.xxx, 7.xxx;

Chapter 6 Instructions for use

6.1 Overall file structure

Console	2019/8/1 15:14	folder
Door	2019/8/5 11:49	folder
tools	2019/8/7 15:47	folder

illustrate:

Console: stores the control program;

Door: stores the Trojan configurator program;

Tools: stores tools for generating https certificates;

6.1.1 Control terminal-console

Plug-in	2019/8/1 15:14	folder	
Plug-Out	2019/8/1 10:35	folder	
Engine.dll	2019/8/1 14:42	application extension	521 KB
Engine.pdb	2019/8/1 14:42	PDB file	2,875 KB
FileManager.dl	2019/8/1 11:32	application extension	213 KB
Hector.exe	2019/8/1 14:53	app	267 KB
Hector.ini	2019/7/30 17:13	Configuration settings	1 KB
Hector.pdb	2019/8/1 14:53	PDB file	6,715 KB
InfcStorage.dll	2019/7/31 18:30	application extension	95 KB
InfcStorage.pdb	2019/7/31 18:30	PDB file	1,435 KB
mfc100u.dll	2019/7/22 14:08	application extension	4,320 KB
msvcp100.dll	2019/7/22 14:08	application extension	412 KB
msvcr100.dll	2019/7/22 14:08	application extension	756 KB
SQLite3.dll	2019/3/22 10:21	application extension	444 KB
terminal.exe	2014/11/21 0:00	app	374 KB

illustrate:

Hector.exe: the main program of the control terminal;

Hector.ini:Control terminal configuration file;

6.1.2 Controlled terminal-door

ca.der	2019/7/31 15:54	security certificate	2 KB
conf64.dat	2019/8/5 14:06	DAT file	1 KB
config54.exe	2019/8/5 11:49	app	5,696 KB
Reptile64.out	2019/8/5 14:06	OUT file	1,717 KB

illustrate:

Config64.exe: Trojan configurator program;

Ca.der: configure the certificate of https protocol;

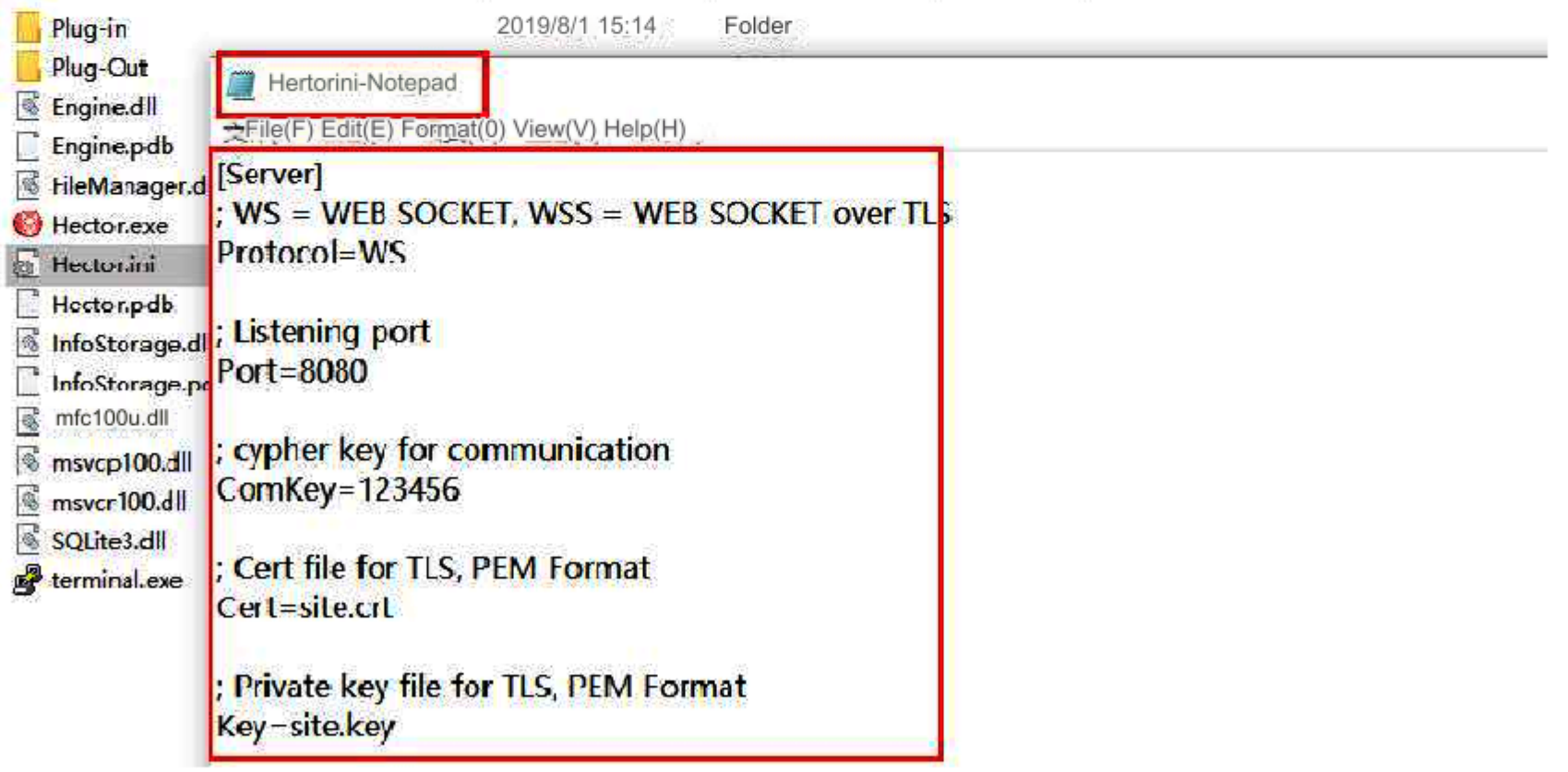
6.1.3 Certificate Tool

Note: For specific usage details, please refer to the MakeSelfSignedCert.txt document.

cert_write.exe	2019/7/4 10:06	app	255 KB
gen_key.exe	2019/7/4 10:06	app	178 KB
MakeSelfSignedCert.txt	2019/7/30 11:03	text document	2 KB
pem2der.exe	2019/7/4 10:06	app	76 KB

6.2 Control terminal configuration and activation

6.2.1 Modify the configuration file Hector.ini



Parameter Description:

1. protocol: protocol, currently supports WEB SOCKET, referred to as WS, WEB SOCKET over TLS, referred to as WSS;

2. Port: The listening port can be customized by the user, but it cannot be the same as the port being used by the system;

3. comkey: The secret key of the connection. After configuration, the Trojan configurator must be consistent with this;

4. cert, key: This certificate needs to be configured when using the WSS protocol, and the certificate must be recorded on the same day as hector.exe;

6.2.2 Open the console

1. After configuring the configuration file Hector.ini file, save it;

2. Run the main program Hector.exe of the control terminal to open the control terminal;

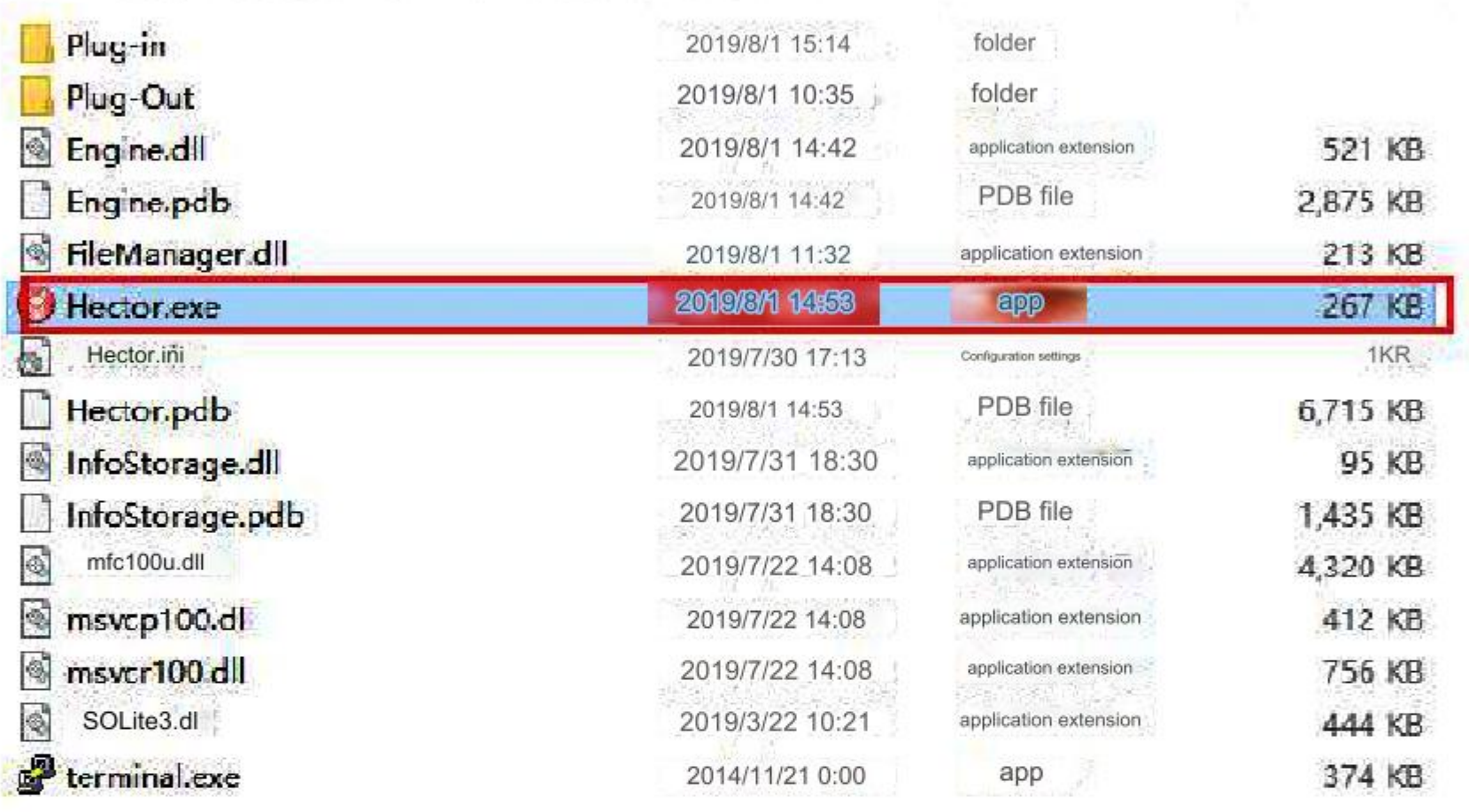


Figure 6.1: Control terminal main program

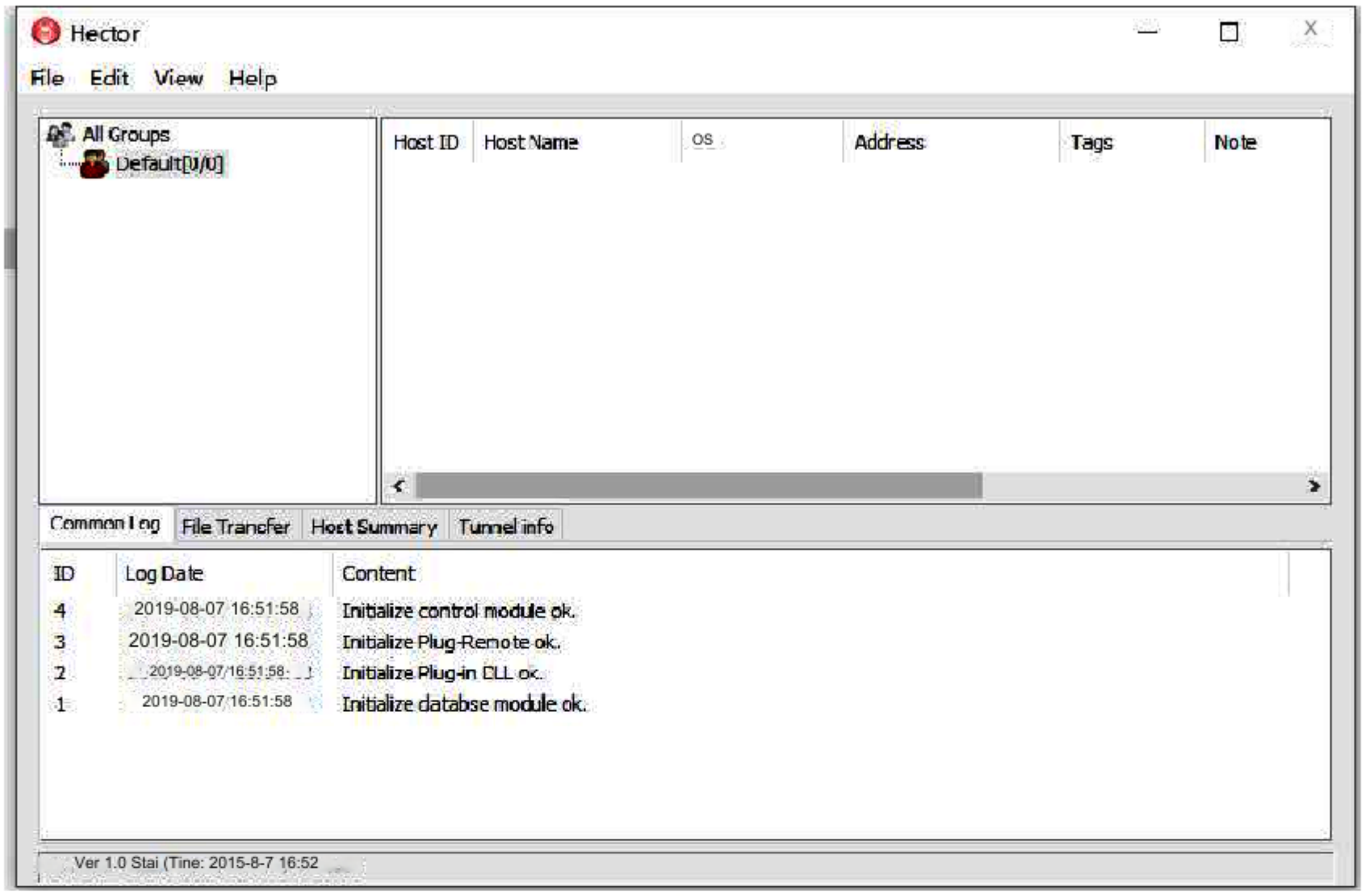


Figure 6.2: Main interface of the control terminal

6.3 Controlled terminal program configuration and installation

6.3.1 Trojan configuration

1. Use the Trojan Configurator program

Figure 6.3: Controlled end program directory

File description:

Ca. der: HTTPS is the certificate required for WSS protocol. For details on how to generate the certificate, see the tools folder;

Config61.exe: Trojan configurator;

Conf64. dat: Configurator memory file, recording the last configuration information;

Reptile64. out: Use the configurator to configure the generated Trojan program.

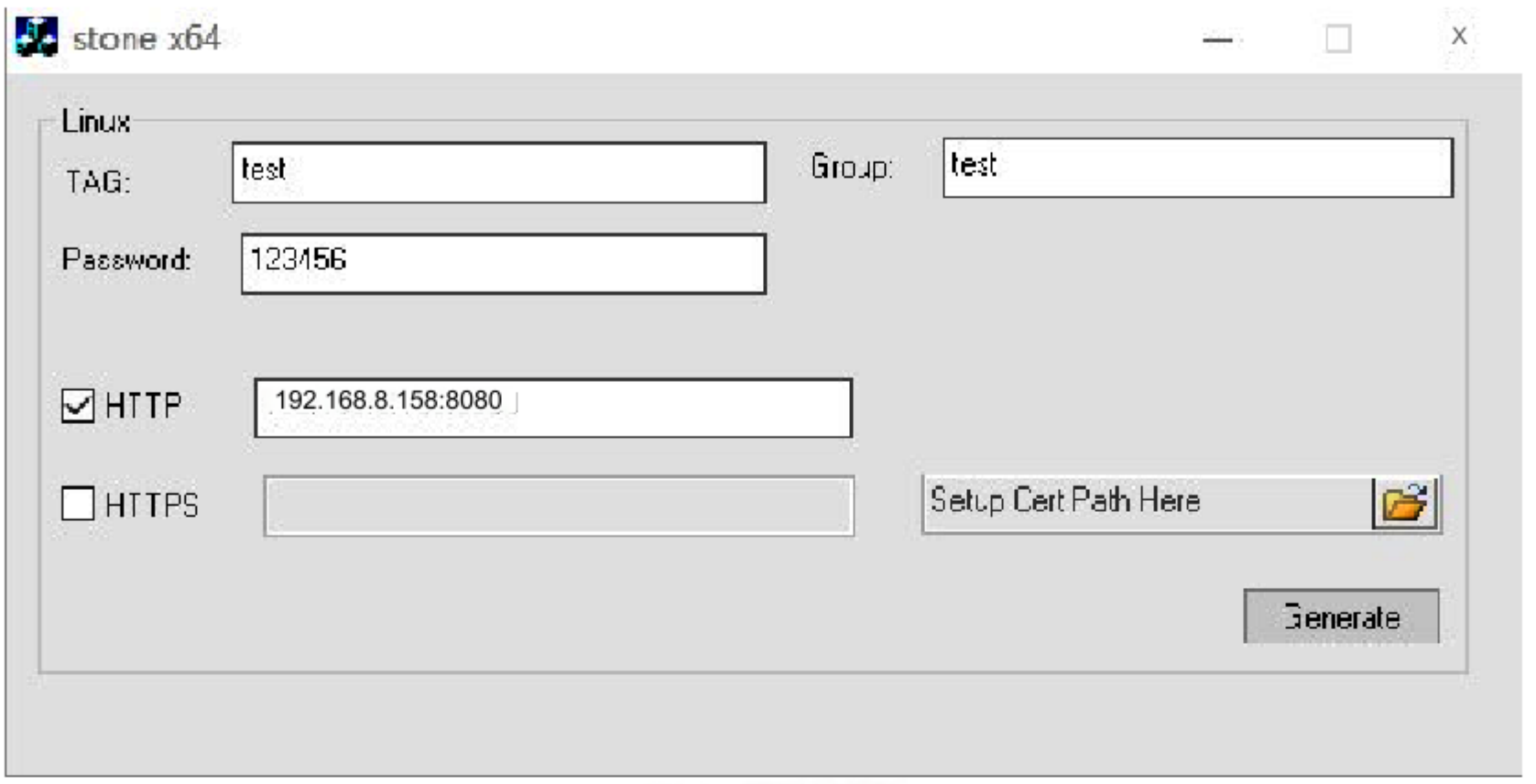


Figure 6.4: Configurator interface

Parameter Description:

1) TAG: tag, user can set it arbitrarily;

2) Group: Group setting. After setting, the host will be displayed in the group in the console;

3) Password: The key of the communication connection, which is consistent with the value of the cypher key for communication in the control terminal configuration file hector.ini;

4) Protocol: (Currently only supports configuring one protocol at a time)

http corresponds to the WS protocol in the control end configuration file hector.ini;

https corresponds to the control terminal configuration file hector.ini and WSS protocol, and the certificate needs to be imported;

2. Configuration: the IP of the control terminal + the port opened by the corresponding protocol

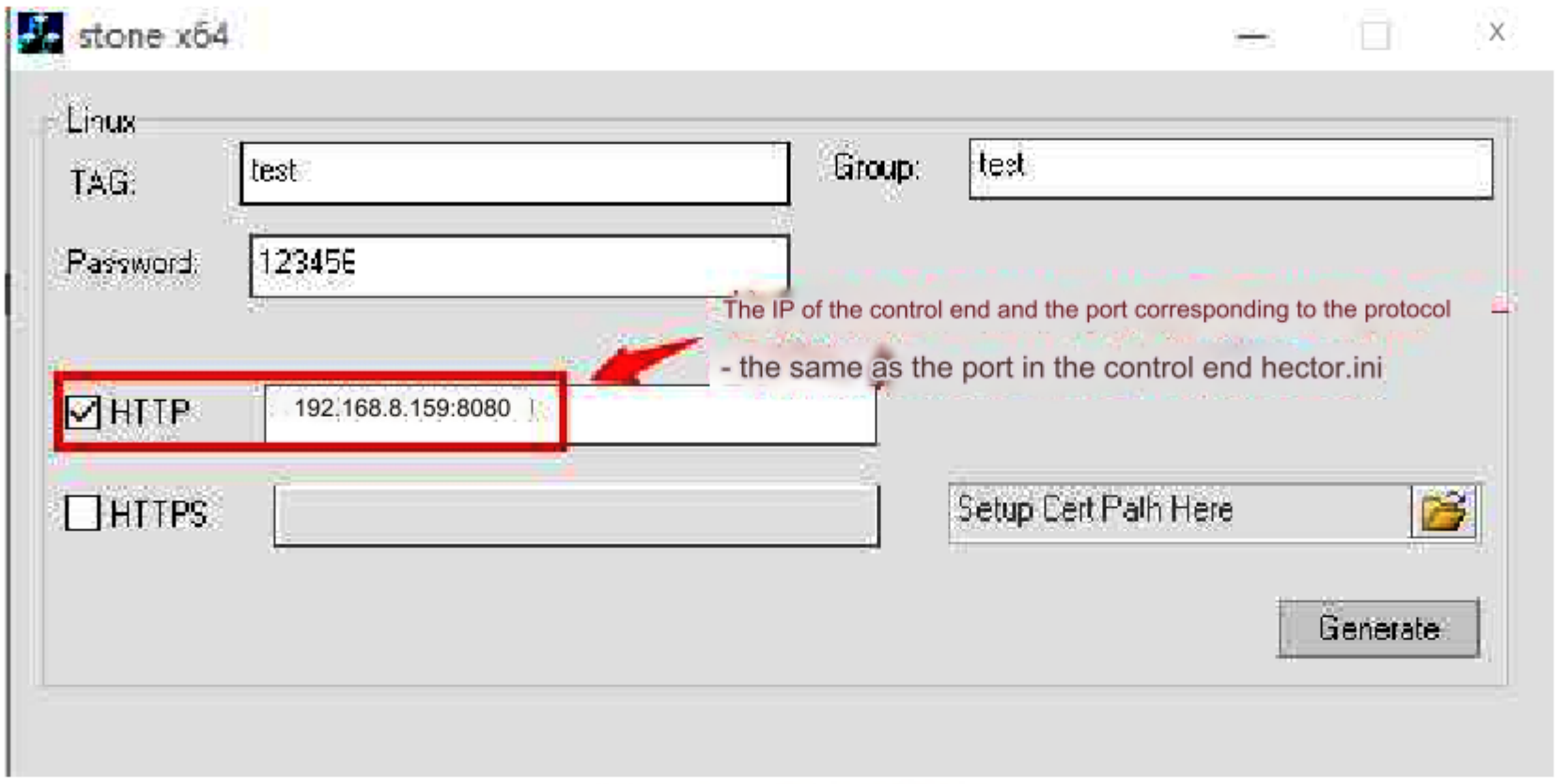
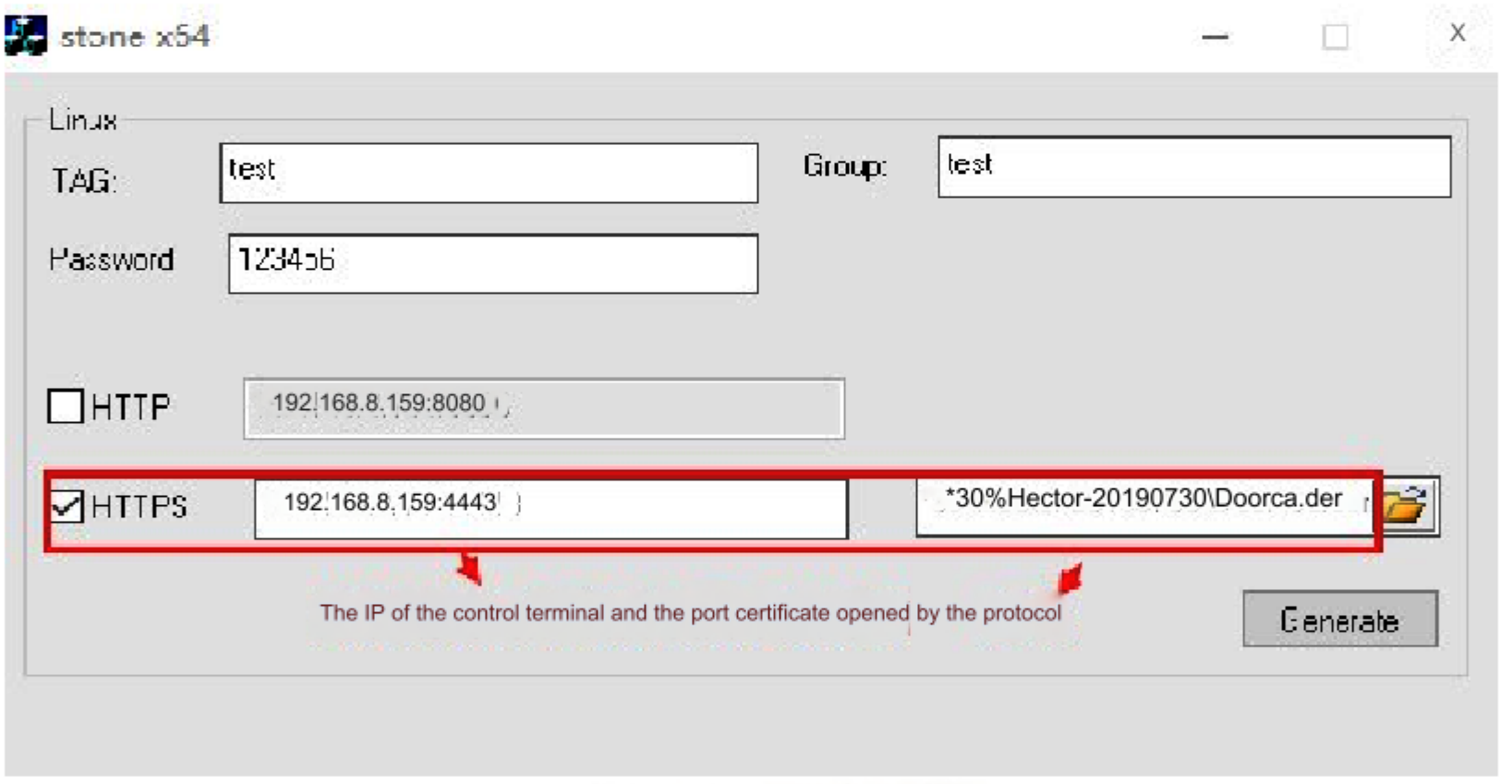


Figure 6.5: Configuration of http/WS protocol



6.6: Configuration of https/WSS protocol

3. After the configuration is completed, click Generate to update the Reptile64. out program;

Figure 6.7: Configuration update file

4. Copy the generated Reptile64.out file to the target machine (Linux system) for installation;

6.3.2 Installation and execution of Trojan programs

Copy the generated Reptile64.out file to the target machine (linux system) for installation: Here

we take centos 7.6 x64 as an example:

1. Copy the files to centos 7.6 x64+;

2. Installation requires root privileges;

3. Go to the file log and execute ./Reptile64.out to install.

(If Reptile64.out does not have execution permissions, you need to use the chmod +x Reptile64.out command to increase execution permissions)

Note: After the current installation is completed, it needs to be restarted to take effect (the self-starting aspect still needs to be optimized later)

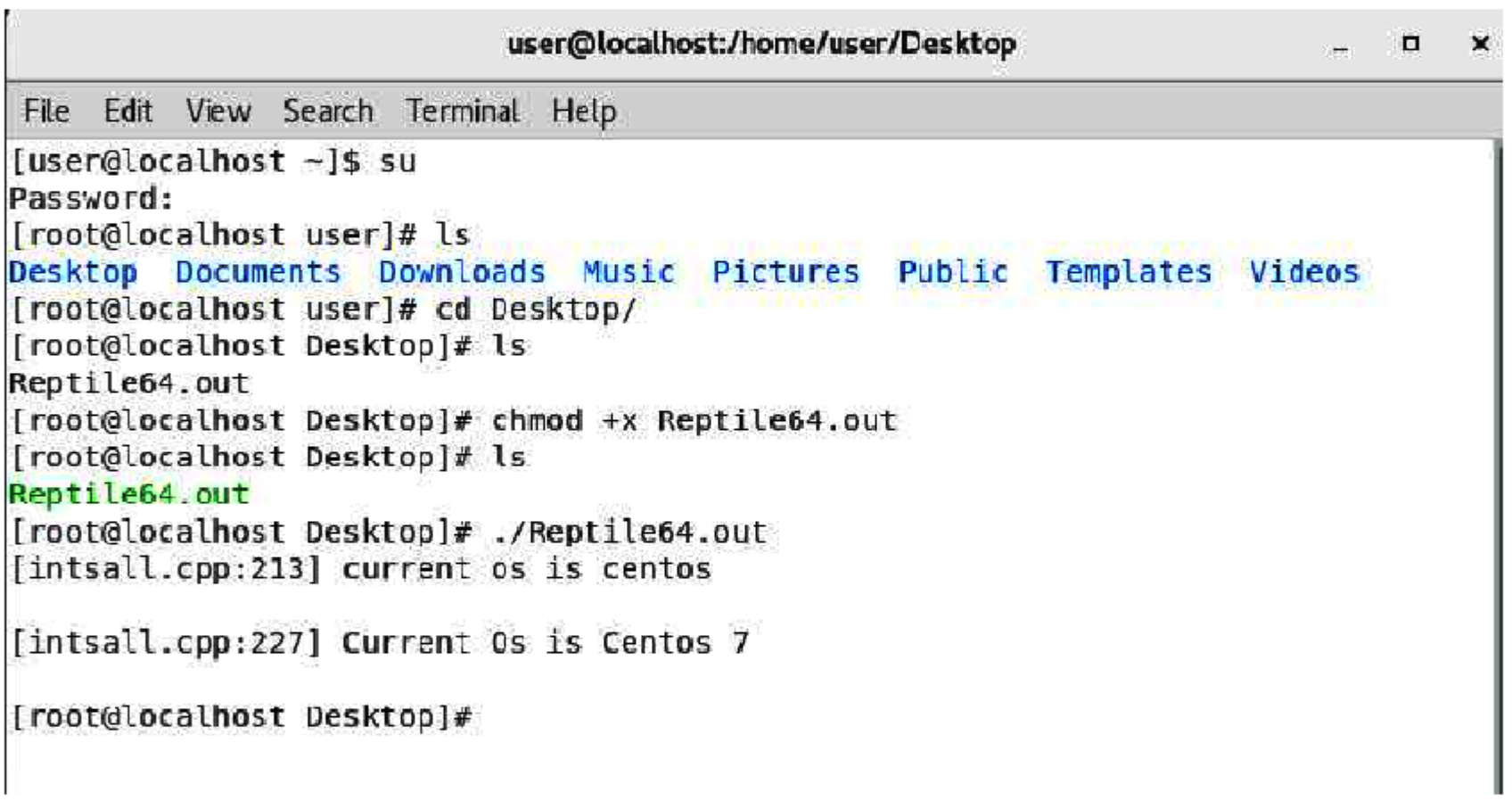


Figure 6.8: Installation in centos 7.6 x64

Chapter 7 Remote Control Function

7.1 Plug-in distribution

This remote control system adopts the plug-in management method to deliver the required plug-ins to the online client and perform corresponding plug-in function operations;

The plug-in distribution function includes two methods:

One is a single delivery, which delivers specified plug-ins to all online clients.

The second is to automatically load and distribute the specified plug-in for a single online customer;

7.1.1 Instructions for delivering a single plug-in

You can individually deliver a plug-in to an online host in the console. The specific steps are:

1. Select the online host to which the plug-in is to be delivered in the host list on the right side of the console, right-click and select the "Host Panel" menu item

in the pop-up menu bar to open a single plug-in delivery window, as shown in the figure;

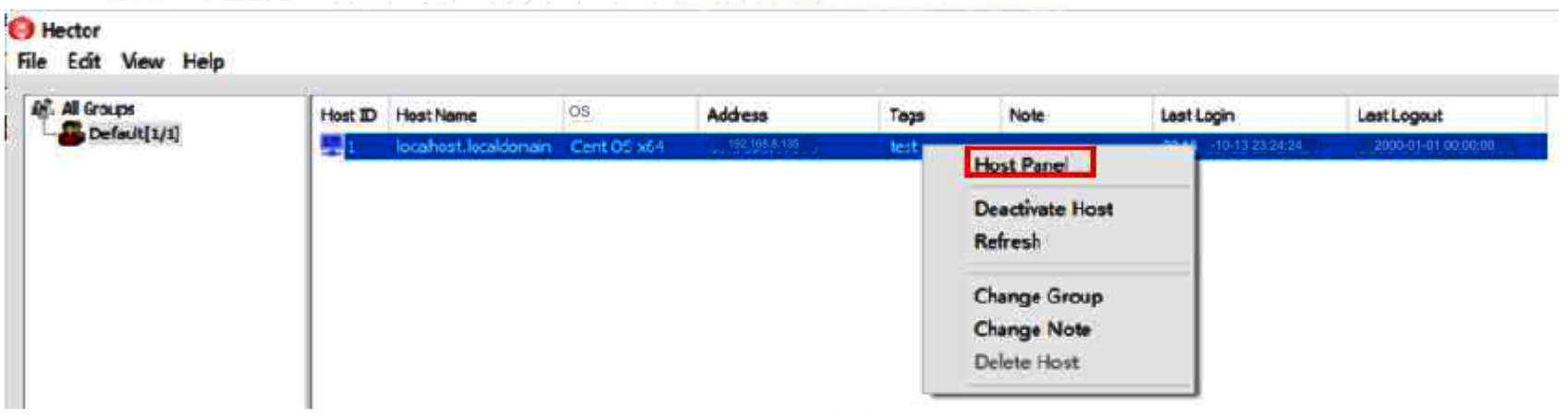


Figure 7.1: Host panel window

2. Select the plug-in type in the single plug-in delivery window, click the "Update Ext" button, and the selected plug-in can be delivered

to the selected online host.

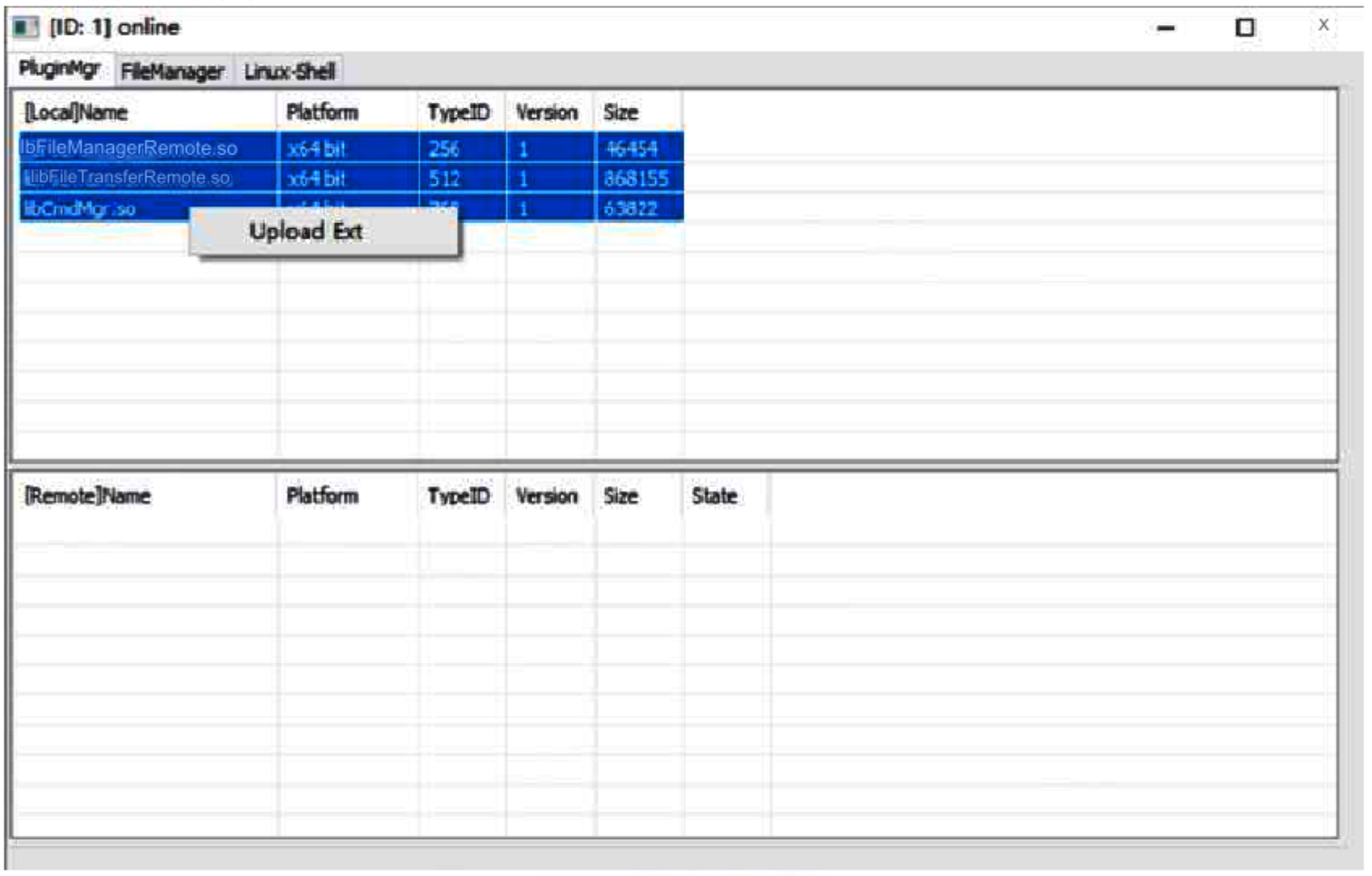


Figure 7.2: Manually distributing plug-ins

3. Right-click on the host below and select "Refresh host Exts" to update and upload the plugin you just selected.

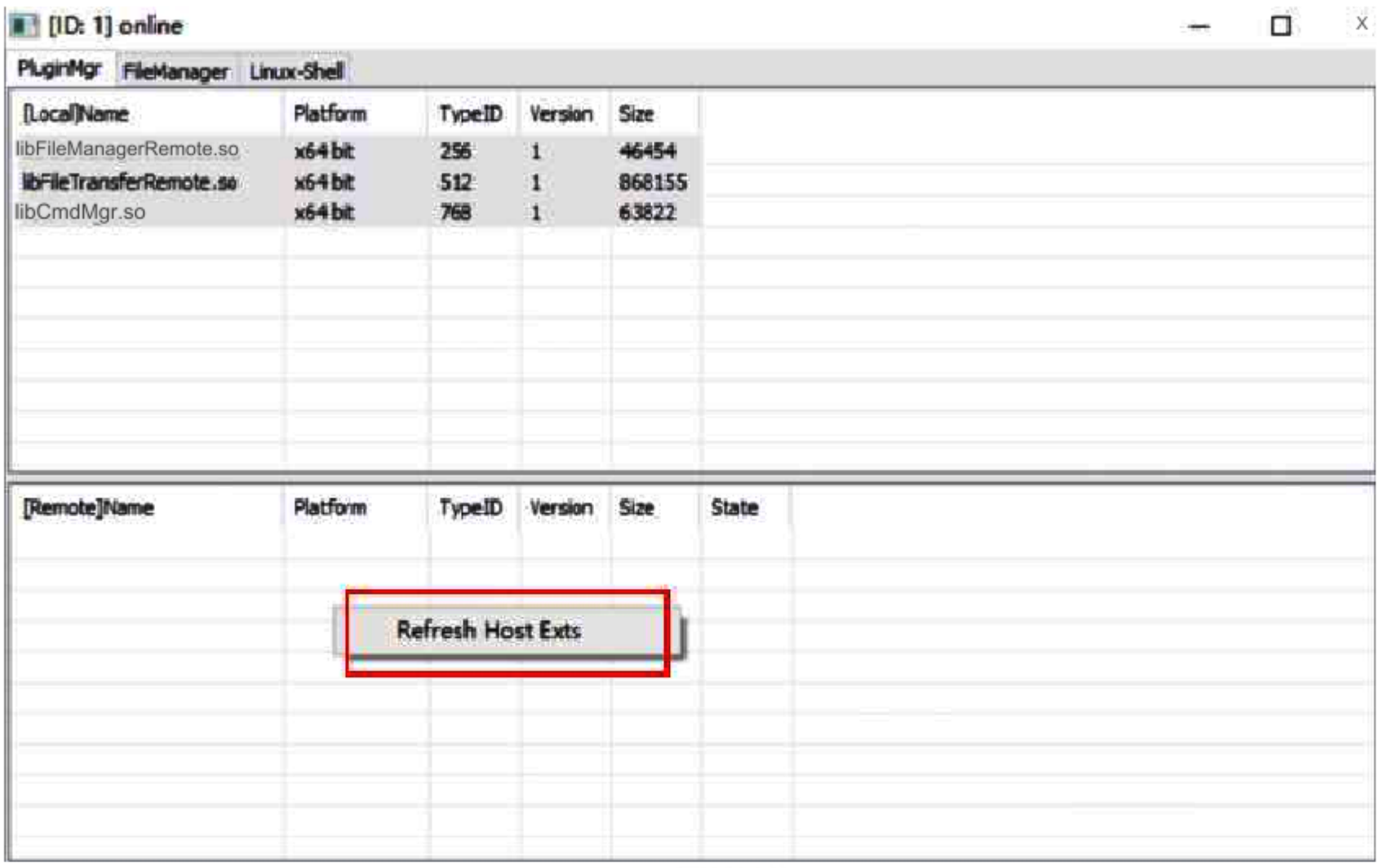


Figure 7.3: Update plugin

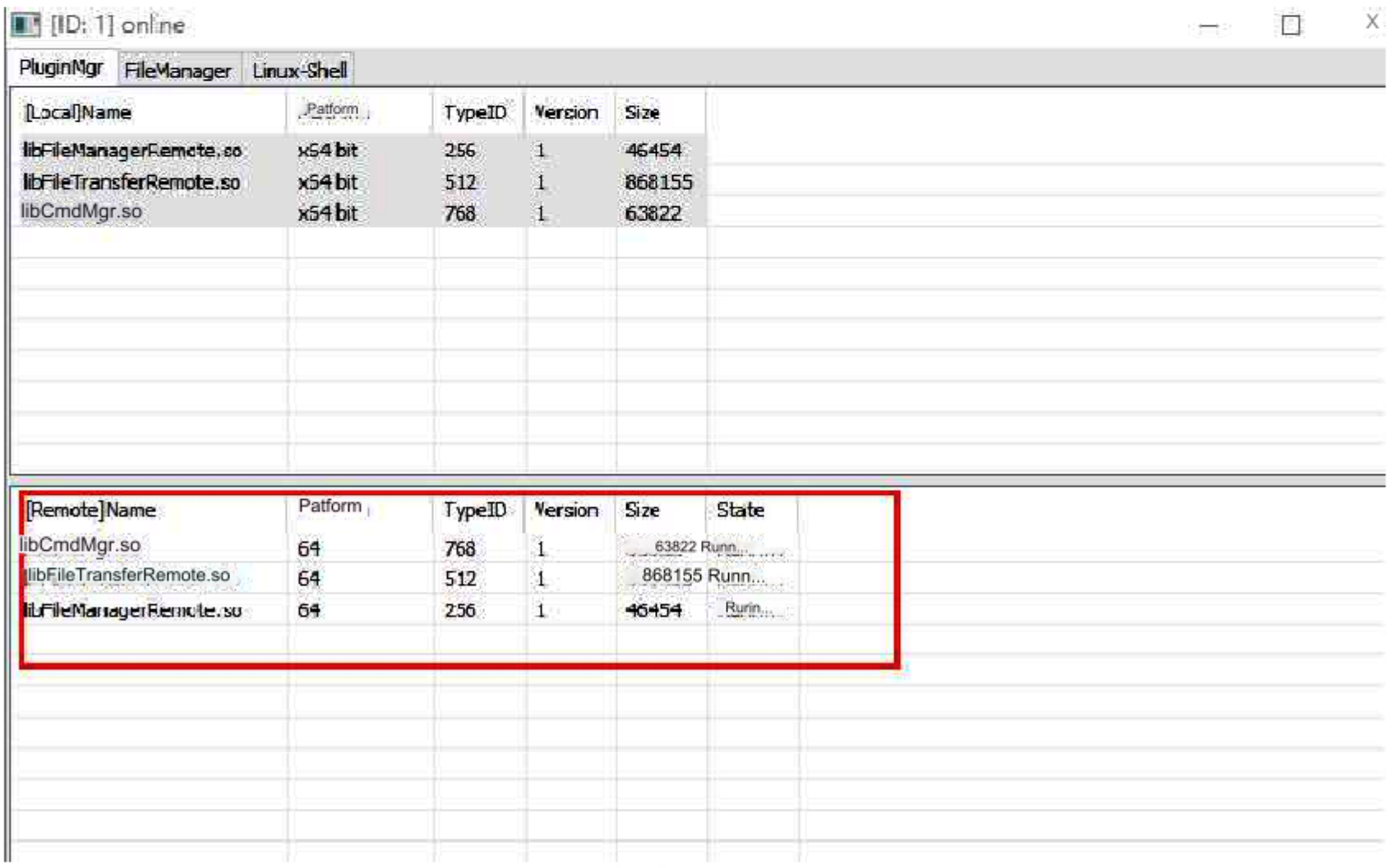


Figure 7.4: Plug-in update completed

7.1.2 Host plug-in automatic loading

Click to open the cmd and fileManager windows in the host, and the plug-in will be loaded automatically.

If there are prompts indicating whether the loading is successful or failed, reopen the panel window and reload: After the plug-in is uploaded successfully, you can

Right click Refresh to refresh.

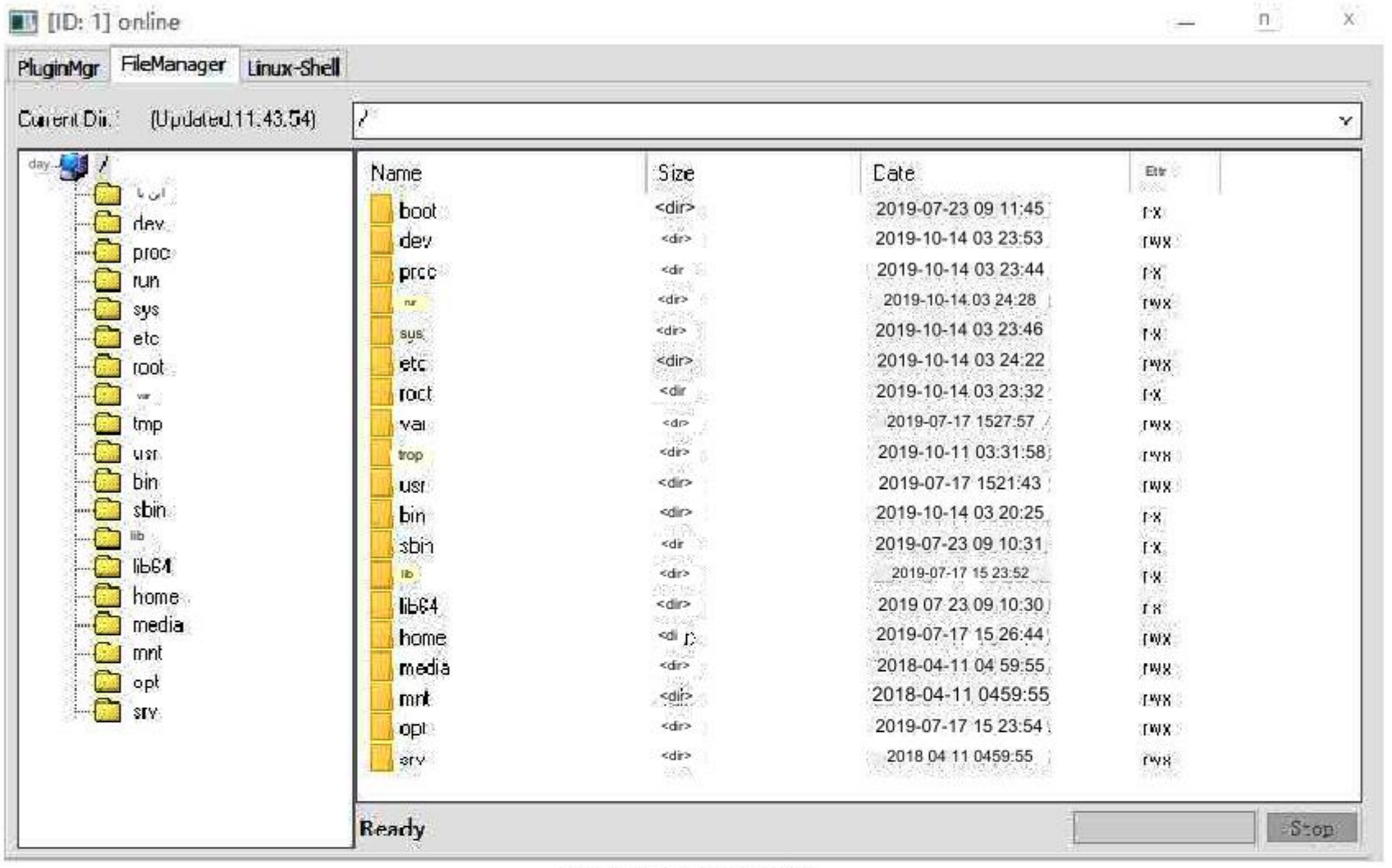


Figure 7.5: Plug-in loaded successfully

7.2 File management

Document management includes:

1) File directory browsing

View graphically, support direct execution of an executable file; support direct

input of absolute path to browse specified directory; support

recording of recently entered path information

2)File transfer

File upload, download, run, delete, small file content viewing, etc.; supports

breakpoint resumption, supports pausing, starting, and deleting transfer tasks;

1. File directory browsing

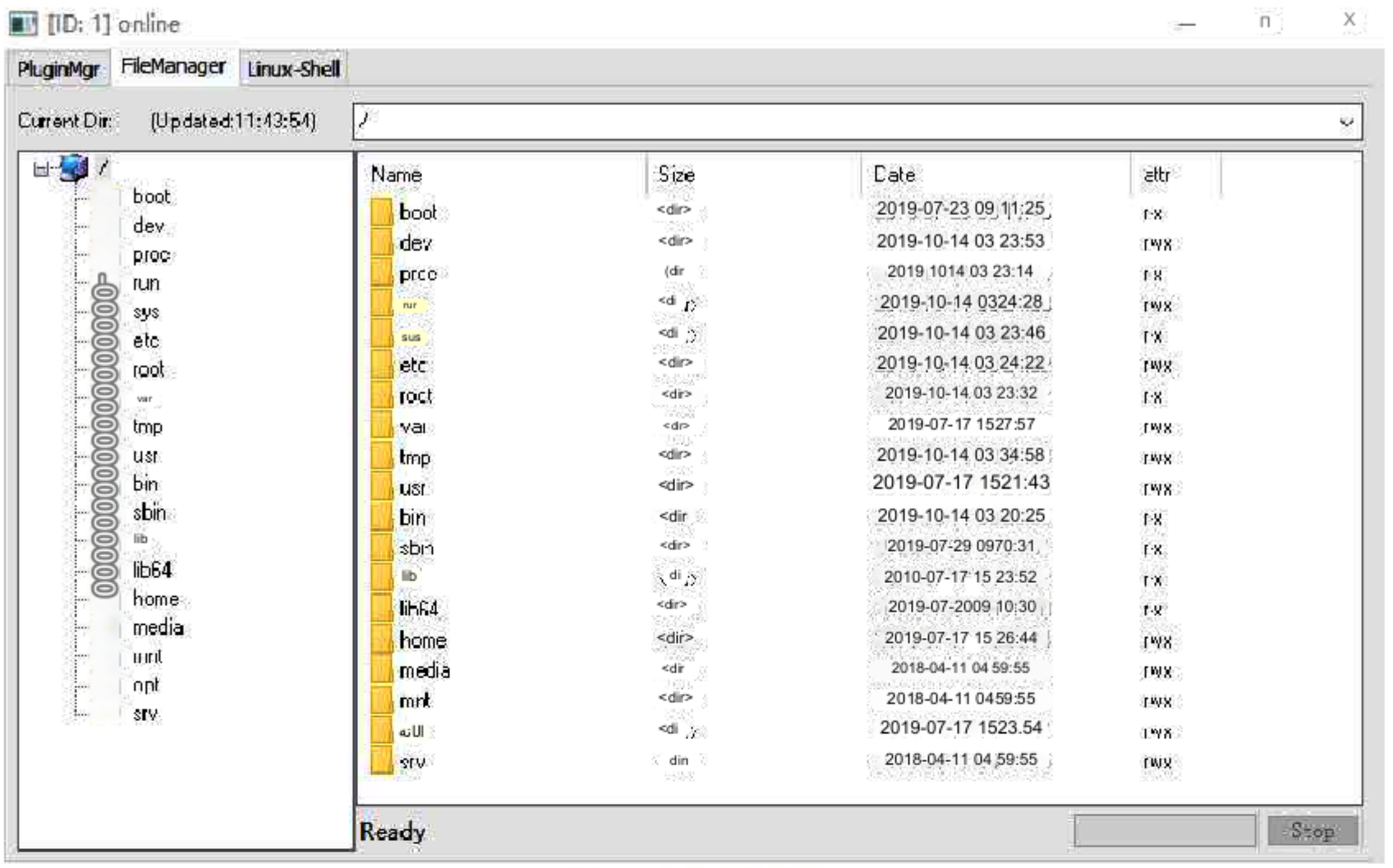


Figure 7.6: File directory browsing

2. File transfer

File upload, download, run, delete, small file content viewing, etc.;

Supports breakpoint resuming, and supports pausing, starting, and deleting transmission tasks;

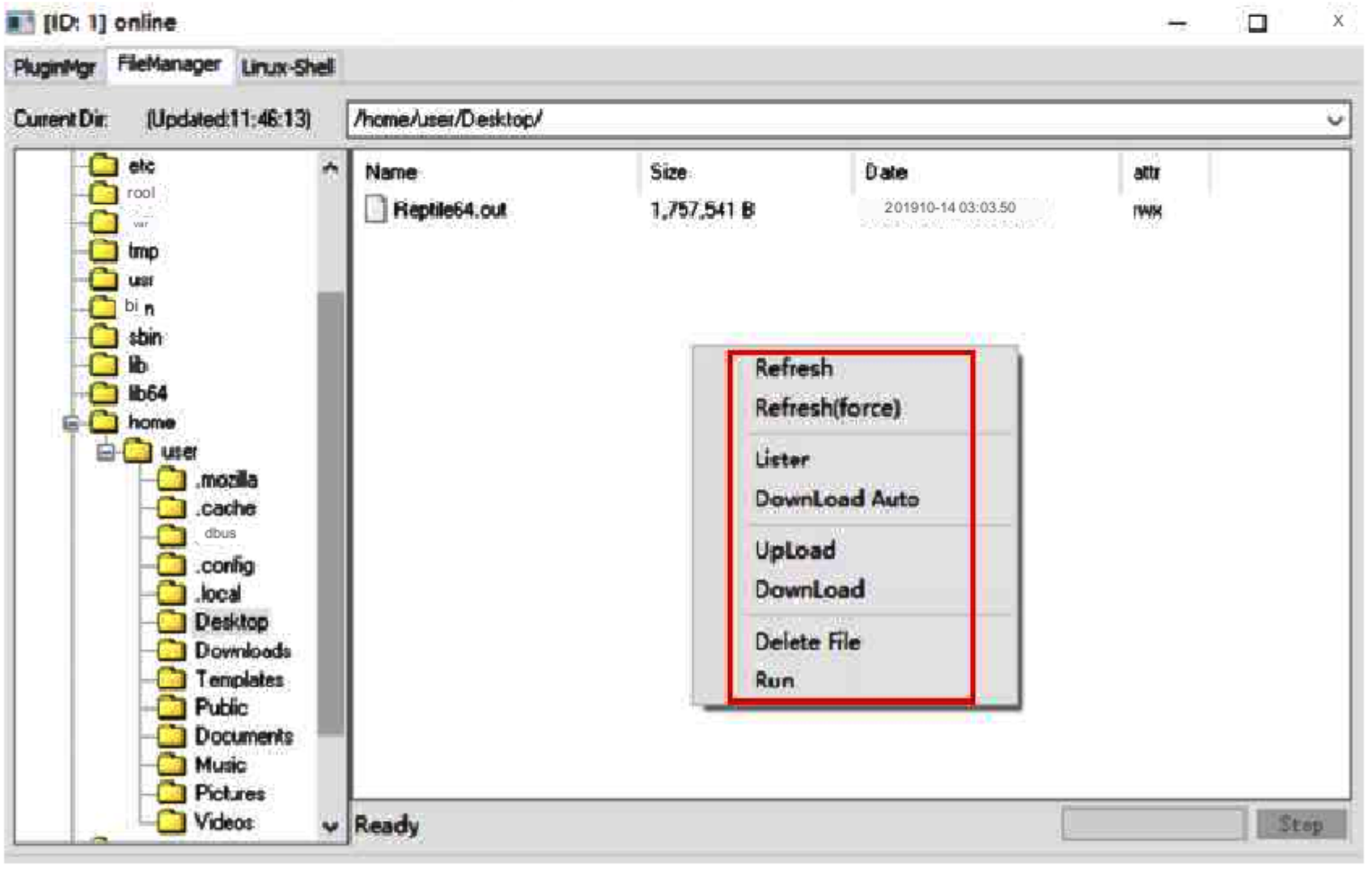


Figure 7.7: File transfer operation

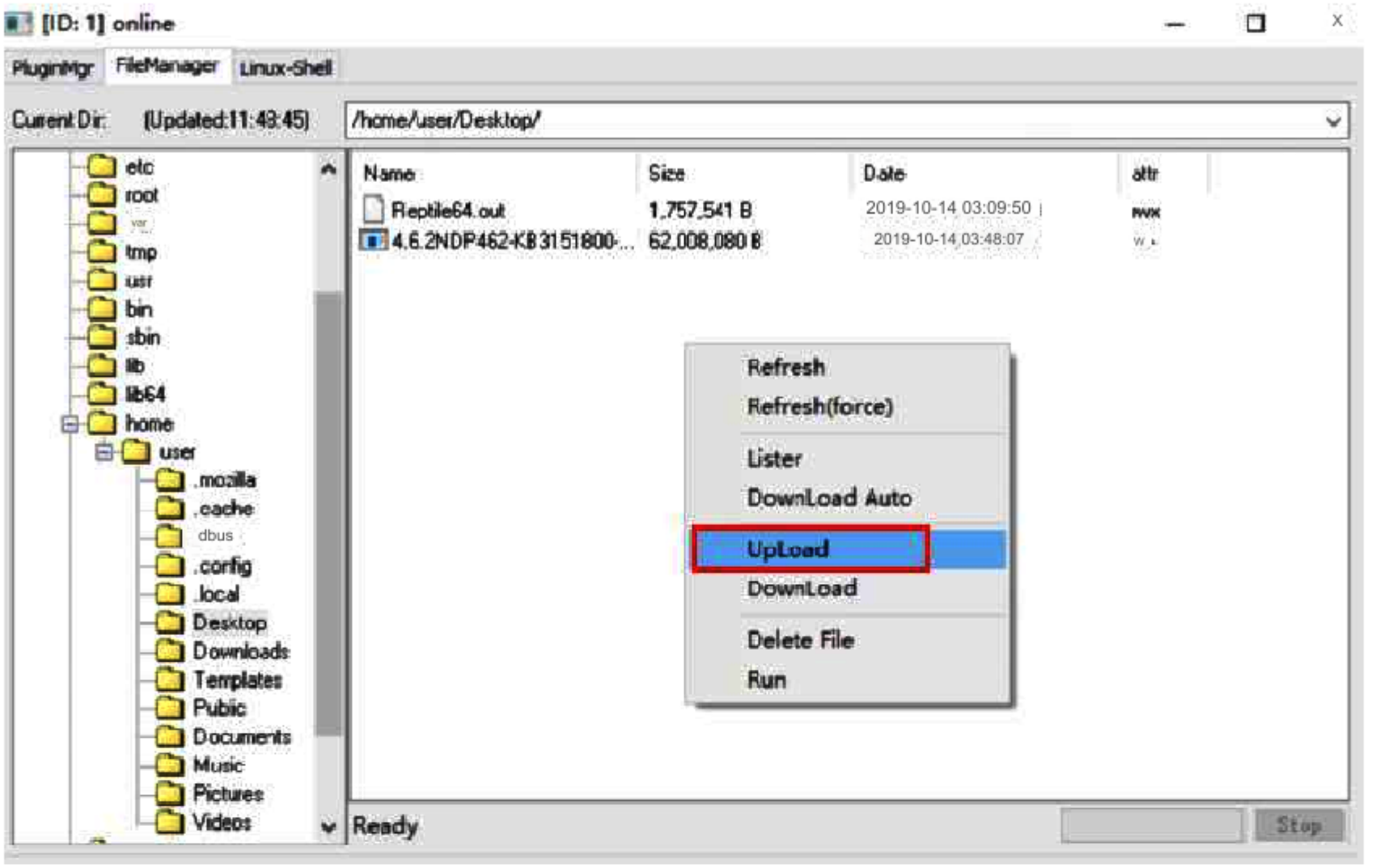


Figure 7.8: Perform upload operation

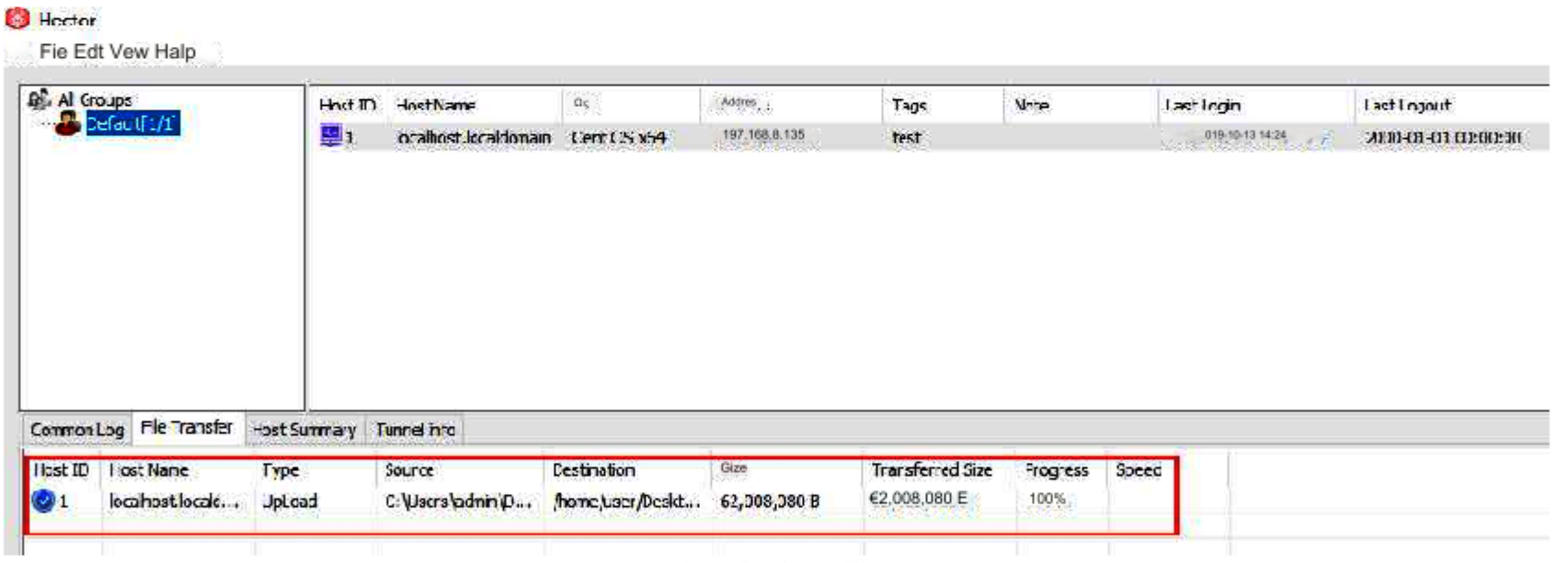


Figure 7.9: File upload record

7.3 Shell commands

Interactive shell command line: execute the shell command of the controlled terminal

1. Switch to the shell plug-in window and execute binding cmd

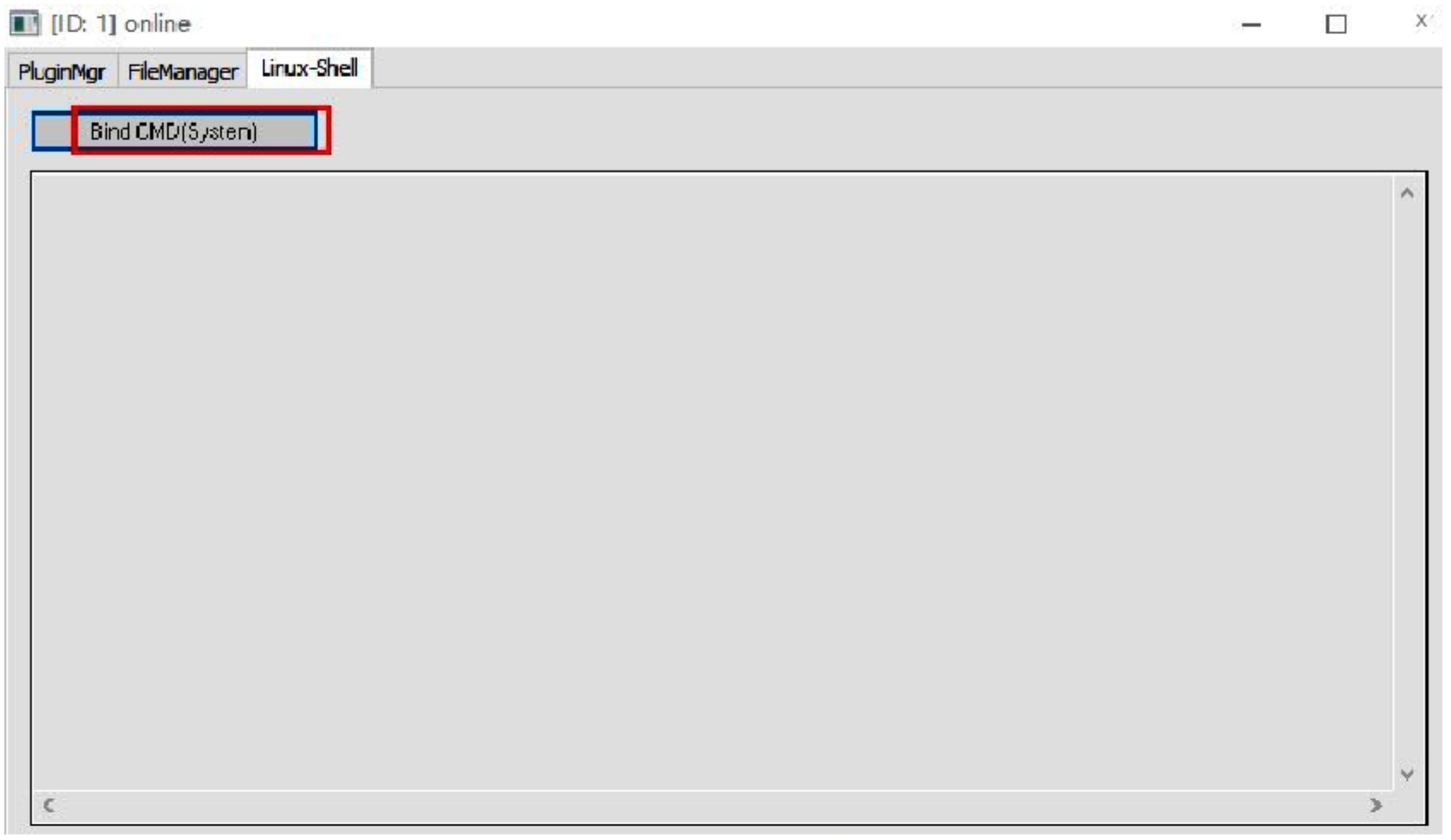


Figure 7.10: Shell plug-in window

2. After executing the binding, a shell window will pop up.

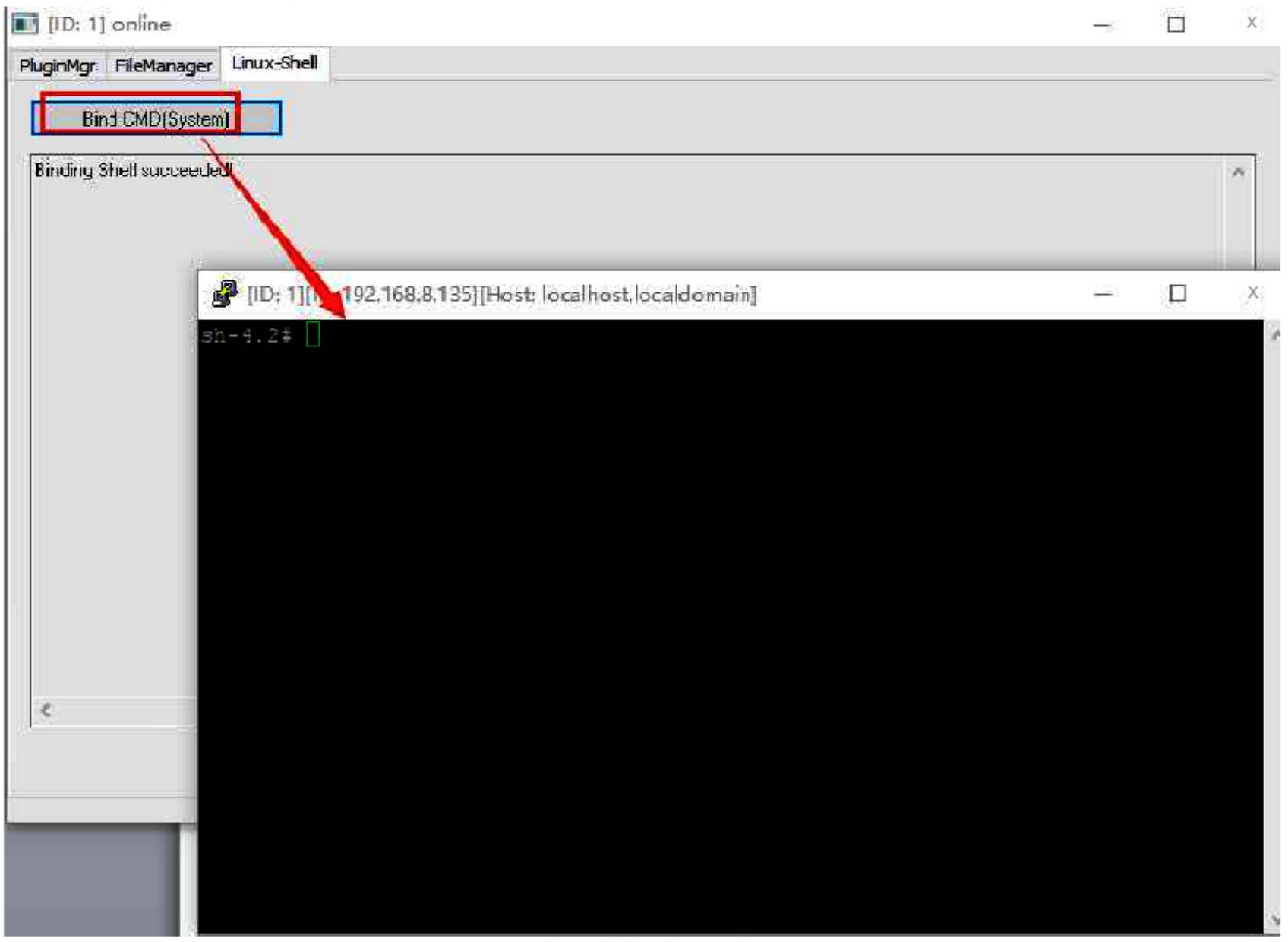


Figure 7.11: Pop-up shell window

3. Execute shell command

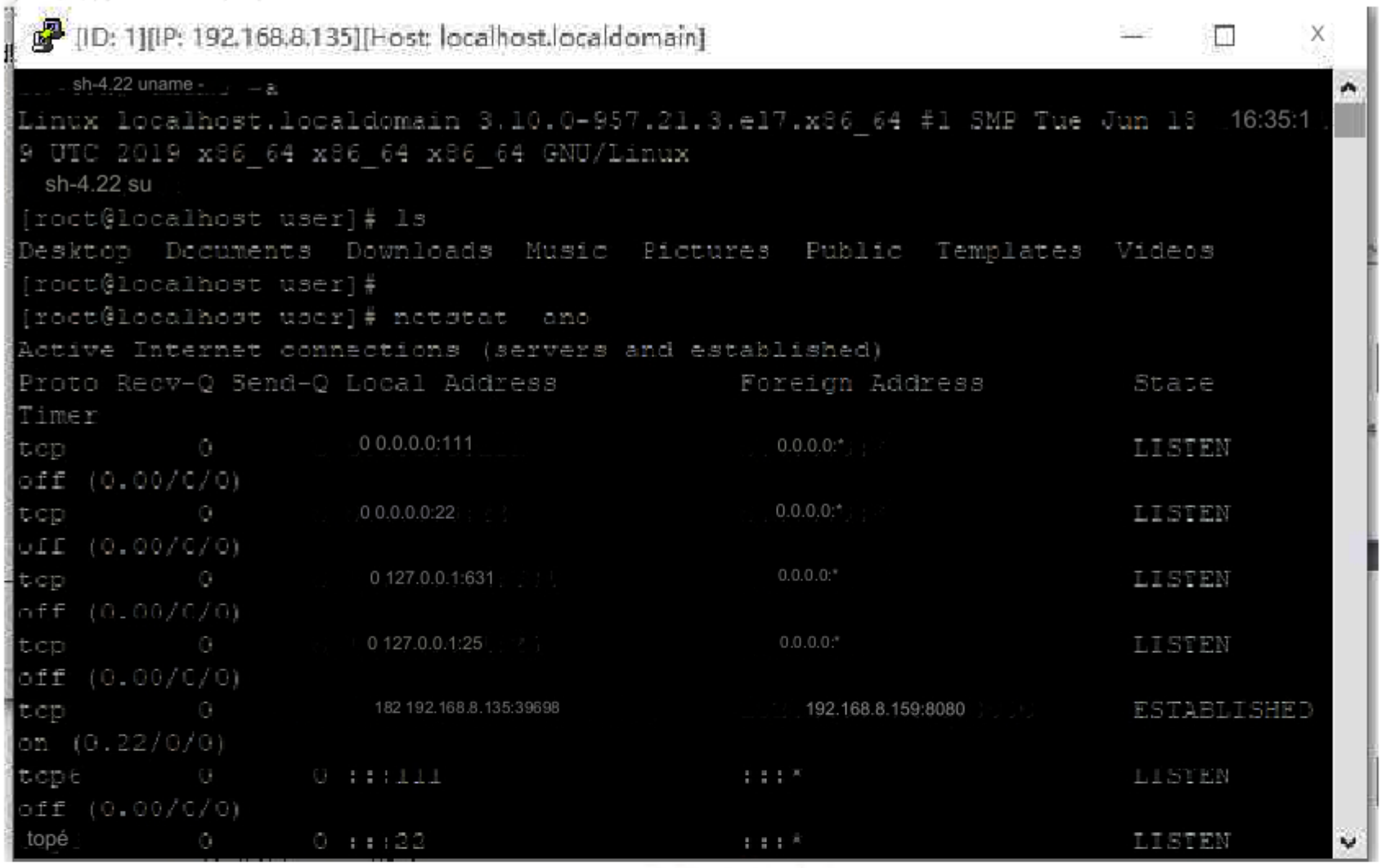


Figure 7.12: Executing shell commands

Chapter 8 Precautions

1. Currently supports x64: Centos 5, 6, 7; ubuntu 14, 16, 18, including centos 5. xxx, 6. xxx, 7.xxx;

2. Installation requires root privileges;

3. The Trojan program is copied to the target machine (Linux environment). If there is no execution permission, the user needs to add execution permission;

4. After the installation is completed, it needs to be restarted to take effect (will be optimized later);

Integrated training platform

Product white paper

(V1.0 version in 2022)

Table of contents

1 Introduction

In the era of rapid development of information technology, network technology has also undergone earth-shaking changes with the iteration of technology. New technologies emerge in endlessly. Driven by the rapid development trend of Internet technology, network penetration technology is also constantly innovating. And the current The international situation is complex and complex, and cyber-GJ incidents are occurring every moment. In addition to cyber-GJ incidents by hostile forces, there are also illegal cyber-GJ activities carried out by criminal groups in order to obtain profits. China is a big cyber country, and also As one of the countries facing the most severe network security threats, it is urgent to establish à•data query platform to provide powerful network offensive and defensive capabilities for network TZ business development.

Currently, there are many types of network security intelligence and other information. The GA team lacks channels to effectively improve search. Traditional searches are too cumbersome and cumbersome.

Moreover, most of the information searched is repetitive and meaningless data, and important data is often difficult to find, thus making it impossible to achieve effective efficiency of TZ team members.

Therefore, in order to meet the current development trend of network TZ, create professional search software and build an integrated data platform.

It is urgent to innovate network information search through the construction of an integrated data platform for search and storage. Through the storage and search platform

Technical means to implement storage and intelligent search modes help the network TZ team to effectively improve its actual combat capabilities and accumulate practical experience.

2 Requirements analysis

A data platform that integrates comprehensive retrieval, multiple data imports, resource management sharing and secure storage. The platform can perform targeted data retrieval based on the daily work needs of network ZC business, support the import and summary of various types of data, and It can conduct unified management and deployment of massive data, thereby effectively providing data support for network ZC work, further improving network ZC business data construction, and improving ZC business efficiency.

> Comprehensive search

Based on data correlation query, it can realize comprehensive query through keywords, and use email, phone number, ID card, etc. as the main correlation objects to check the detailed information of the target person, and support second-level query of massive data.

> Data import

By extending the technical protocol, it supports the safe import of many different types of data. By cleaning and classifying the collected data information and importing it into the integrated data platform, it finally realizes various data information retrieval and extracts value data QB.

> Data management

Based on the data of the current business platform and according to the needs of specific business situations, users can create data collection for each business project or share data with each business platform, ultimately achieving efficient use of data.

> Storage security

Based on the use of distributed storage technology, it naturally supports horizontal expansion, and at the same time, data security comes with redundant backup to prevent data disasters; it also supports elastic scaling cluster architecture, and the physical cluster size can be freely selected according to business needs. In addition, it also supports high availability Load balancing, automatic failover, etc.

3 Product Introduction

3.1 Product introduction

"Anxun Integrated Data Platform" is a data platform that integrates comprehensive retrieval, multiple data imports, resource management sharing and secure storage. The platform can perform targeted data retrieval based on the daily work needs of network ZC business. It supports the import and summary of various types of data, and can conduct unified management and deployment of massive data, thereby effectively providing data support for network ZC work, further-improving network ZC business data construction, and improving ZC business efficiency.

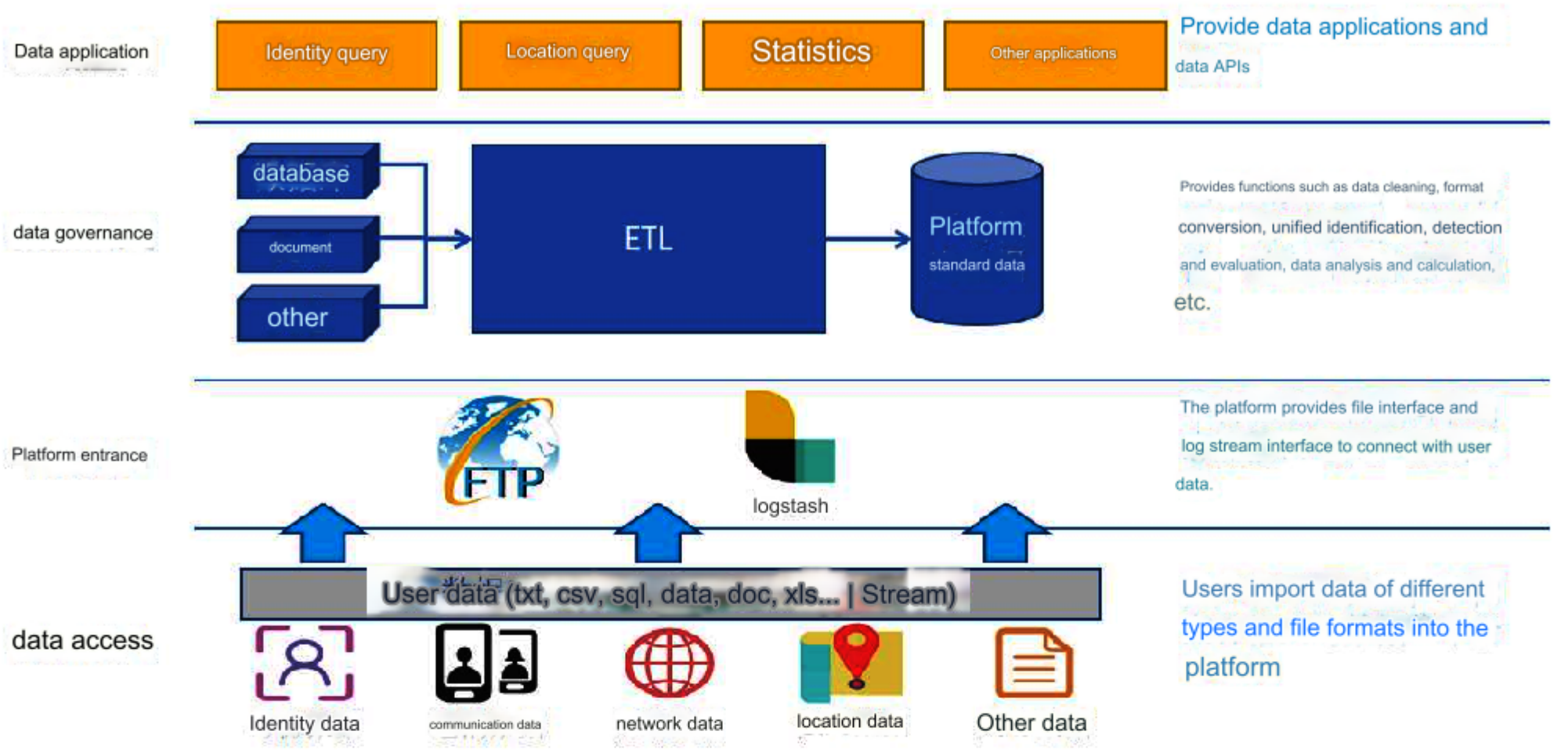
3.2 Product composition

"Anxun Integrated Data Platform" is mainly composed of four layers: data access layer, platform entrance layer, data governance layer and data application layer. By importing, cleaning, identifying, managing and storing data in the data access layer, The file interface and log stream interface are set up at the platform entrance layer to connect with user data. The data governance layer classifies the data through data cleaning, format conversion, unified identification, detection and evaluation, data analysis and calculation, and finally implements data processing at the data application layer. Daily management, maintenance and use of system platform. The product composition list is mainly as follows:

1. Integrated data platform software: 1 set

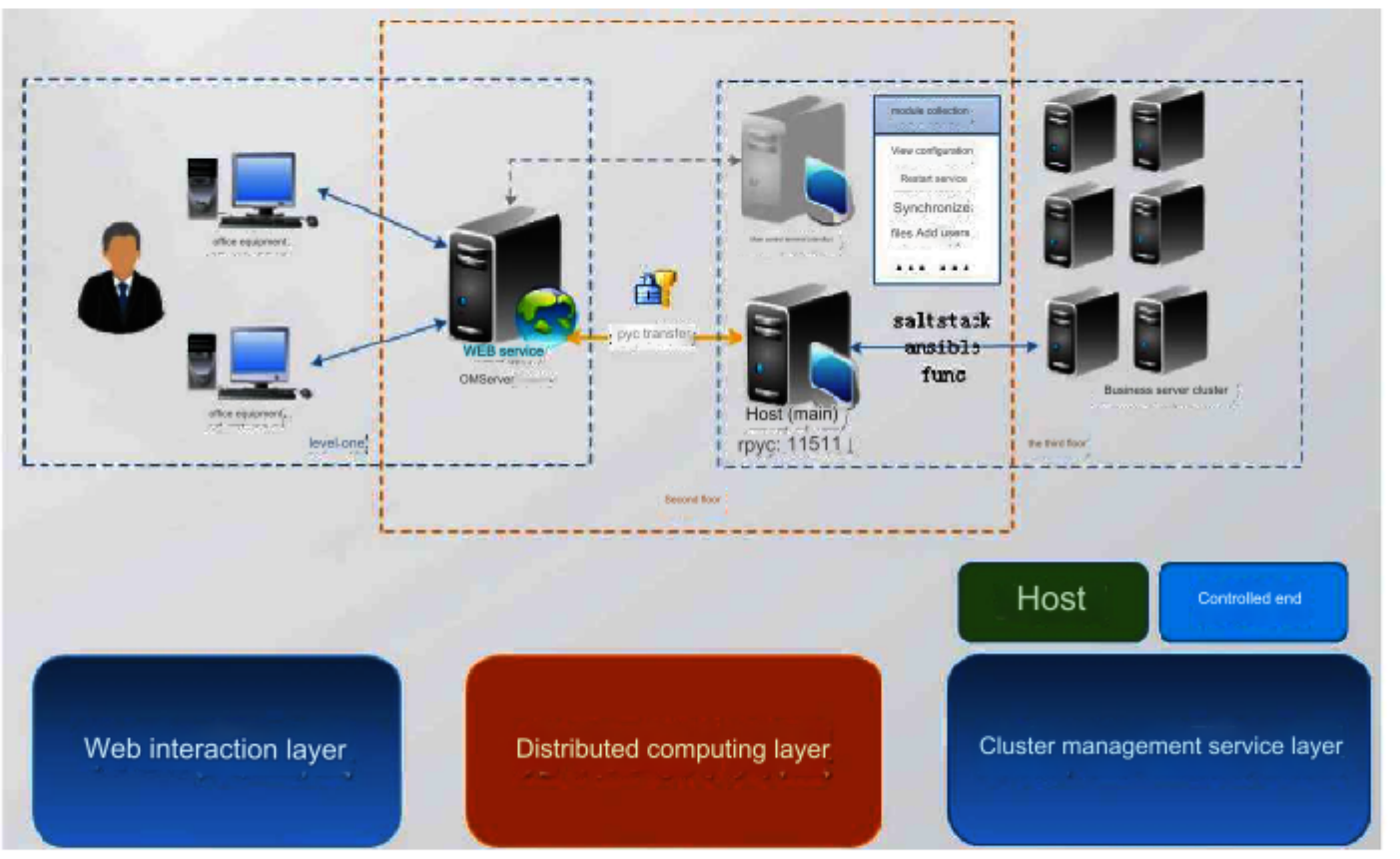
2. Integrated data platform user manual: 1 copy

3.3 Platform architecture



(Integrated data platform platform architecture diagram)

3.4 Network architecture

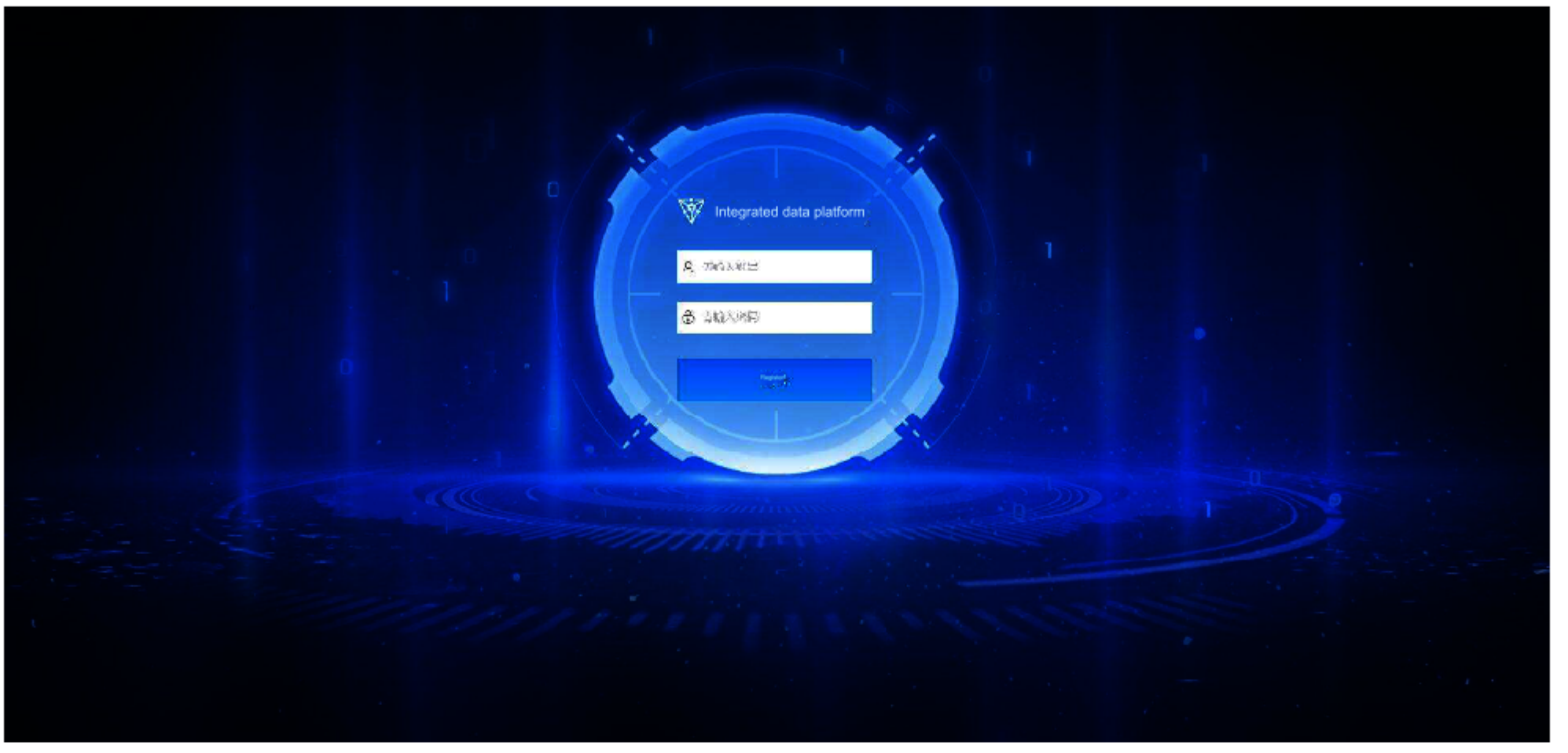


(Integrated data platform network architecture diagram)

"Anxun Integrated Data Platform" adopts B/S architecture, adopts local deployment server method, and can also adopt hosting method. The platform administrator logs in to the background to perform management operations, and edits, manages, and queries target-related data according to his or her own needs.

4 product features

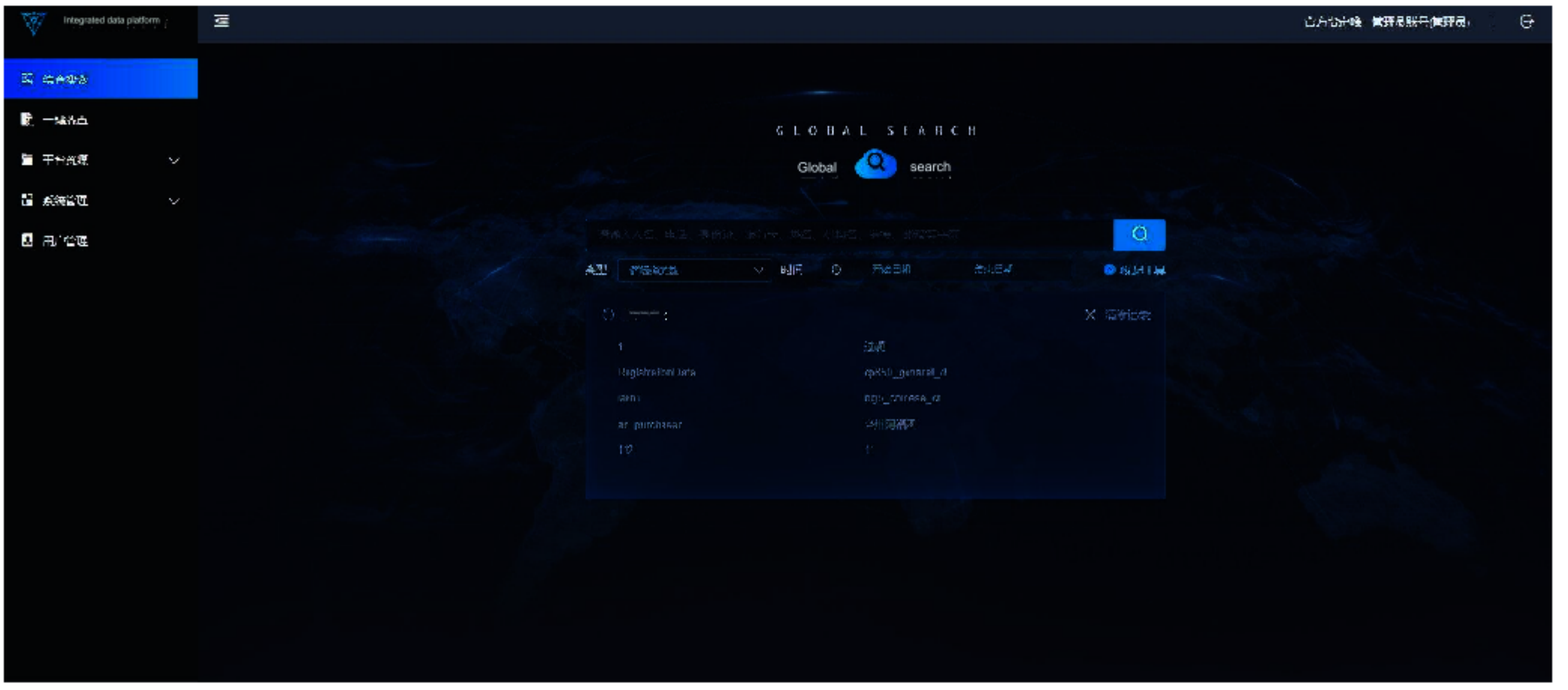
The "Anxun-Integrated Data Platform" data query platform combines the needs of users. The system includes comprehensive search, one-click search, platform resource management, system management, user management and other functions to fully satisfy users' information and related information for specific targets. Inquire.



(Integrated data platform-backend)

4.1 Comprehensive search

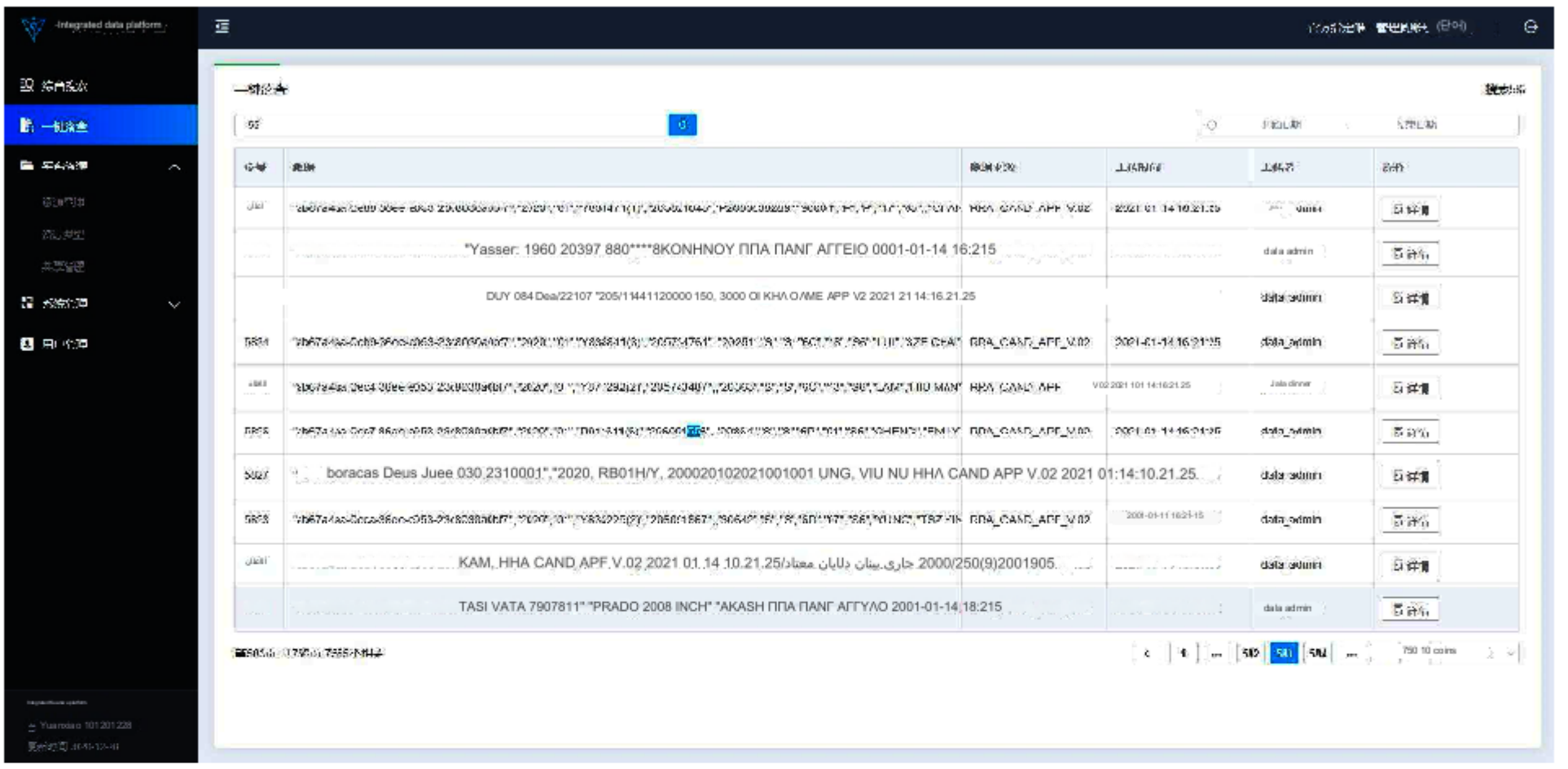
Users can enter the keywords or fuzzy words they want to search in the input box (phone number, name, email, ID card, bank card, address, link) and click "Search" to perform keyword fuzzy search. Date selection is supported. , and realize the query of all related data information such as the target's name, email, phone number, ID number, etc.



(Comprehensive information inquiry)

4.2 One-click search

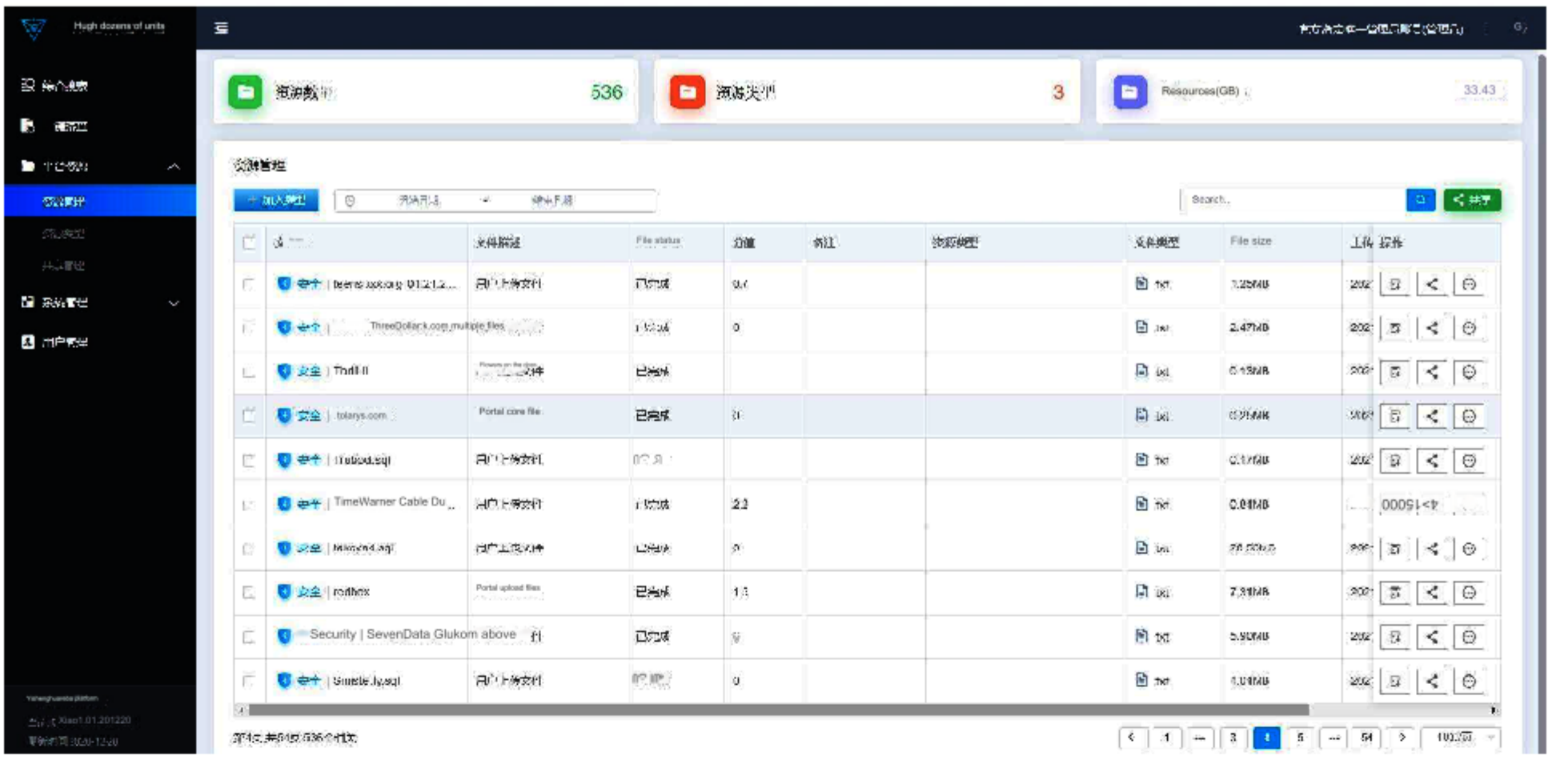
Based on the query requirements for some valuable data in real network ZC business work, users can use the "one-click query" information query toolbar to select the data type corresponding to the search and enter the keywords to be searched in the input box. Click "Search" to perform a keyword search to further query and collect target data information.



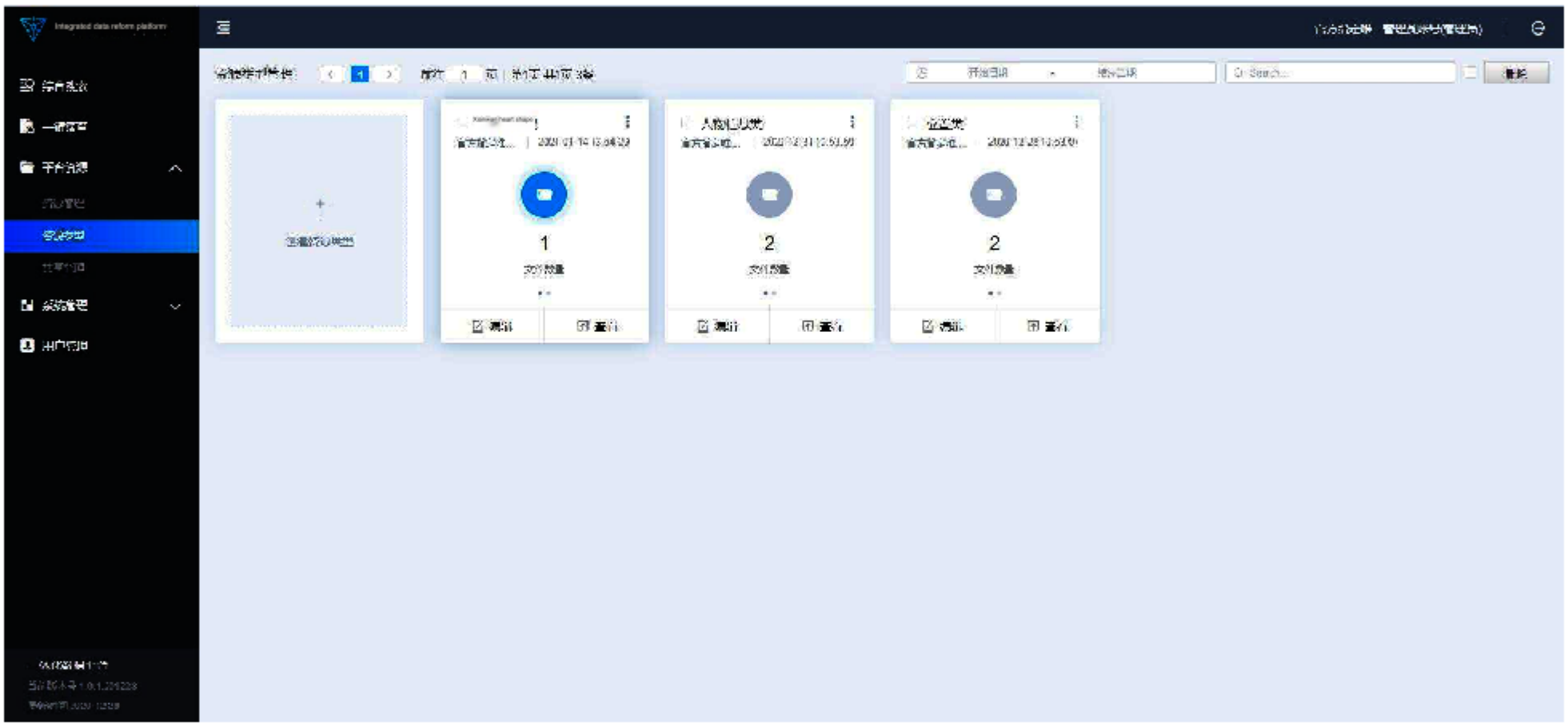
(One-click query)

4.3 Platform resources

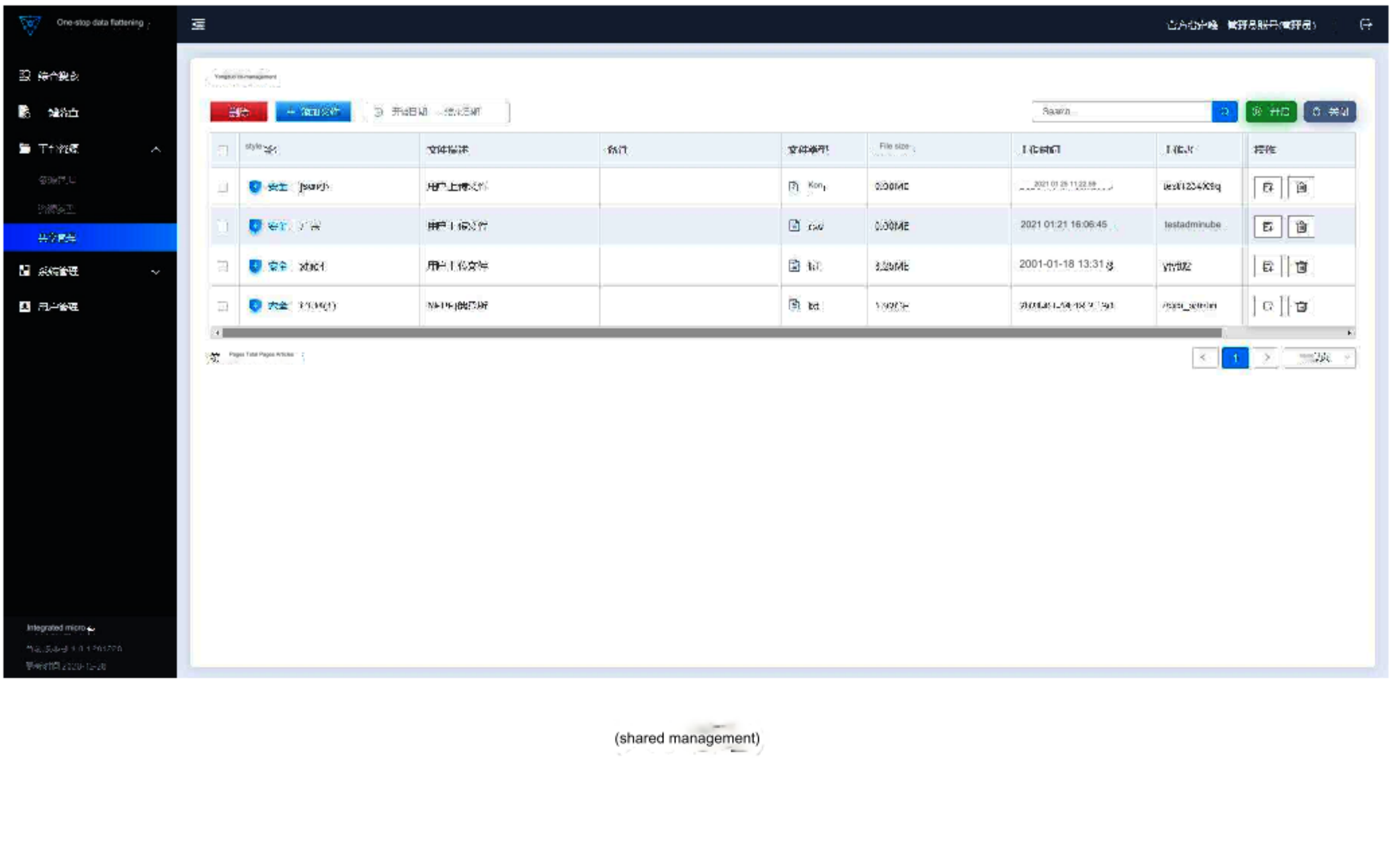
Based on the daily management or query needs of platform resources, users can use the "Resource Management" toolbar to enter the keywords they need to search in the input box, click "Search" to perform keyword searches, and further query the target data. . At the same time, it also supports batch deletion, sharing, editing and other operations of the queried data. Click on the corresponding data to view the source of the data and the security analysis report. At the same time, it also supports creating corresponding resource folders by yourself, and classifying data into different types according to different projects, tasks or types, so that users can use the data clearly and intuitively. In addition, it also supports data sharing. By choosing to add existing data in the resource library to different folders and setting up sharing, multiple departments can share data, greatly improving the efficiency of data use.



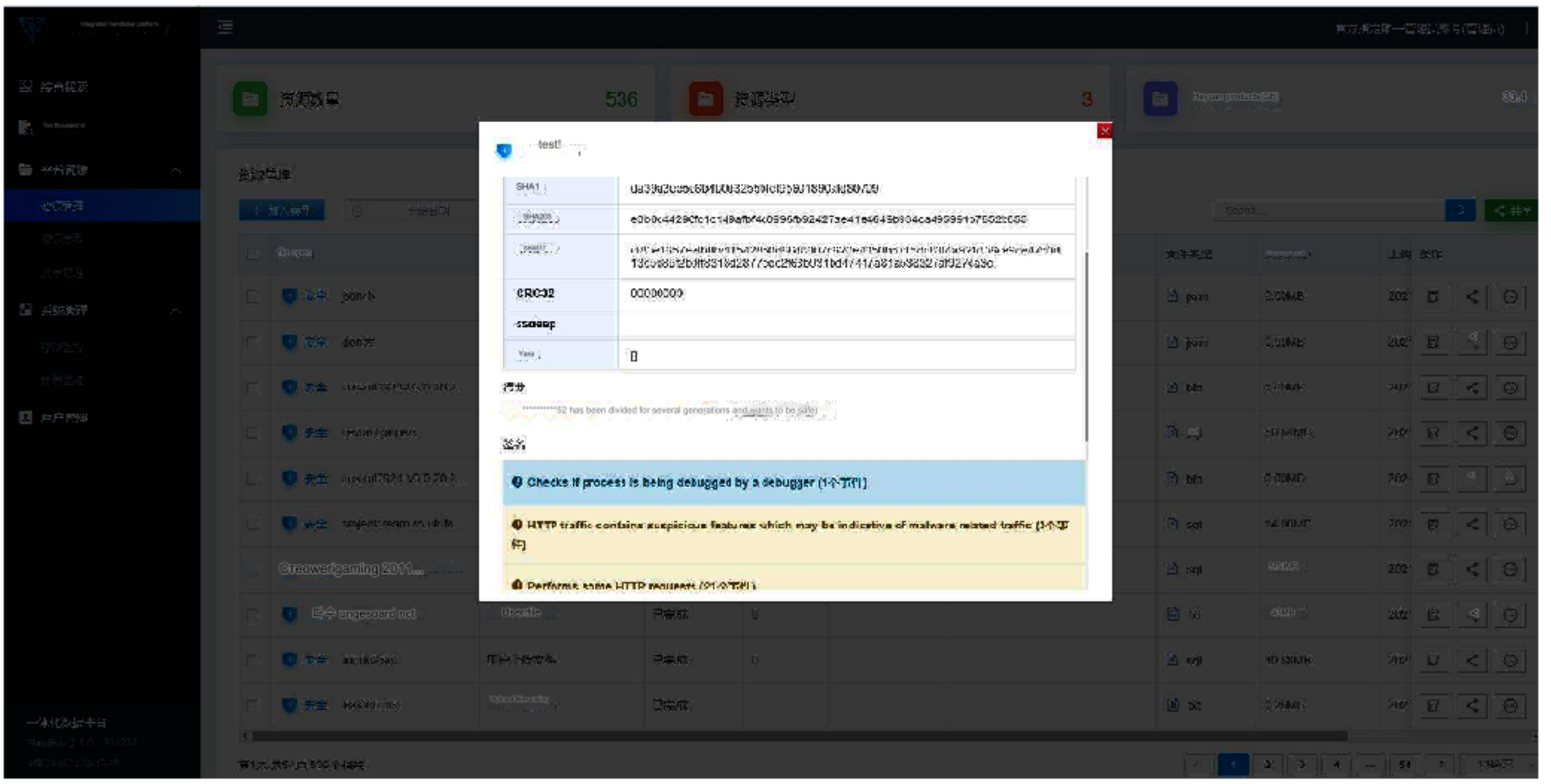
(Resource Management)



(Resource Type)



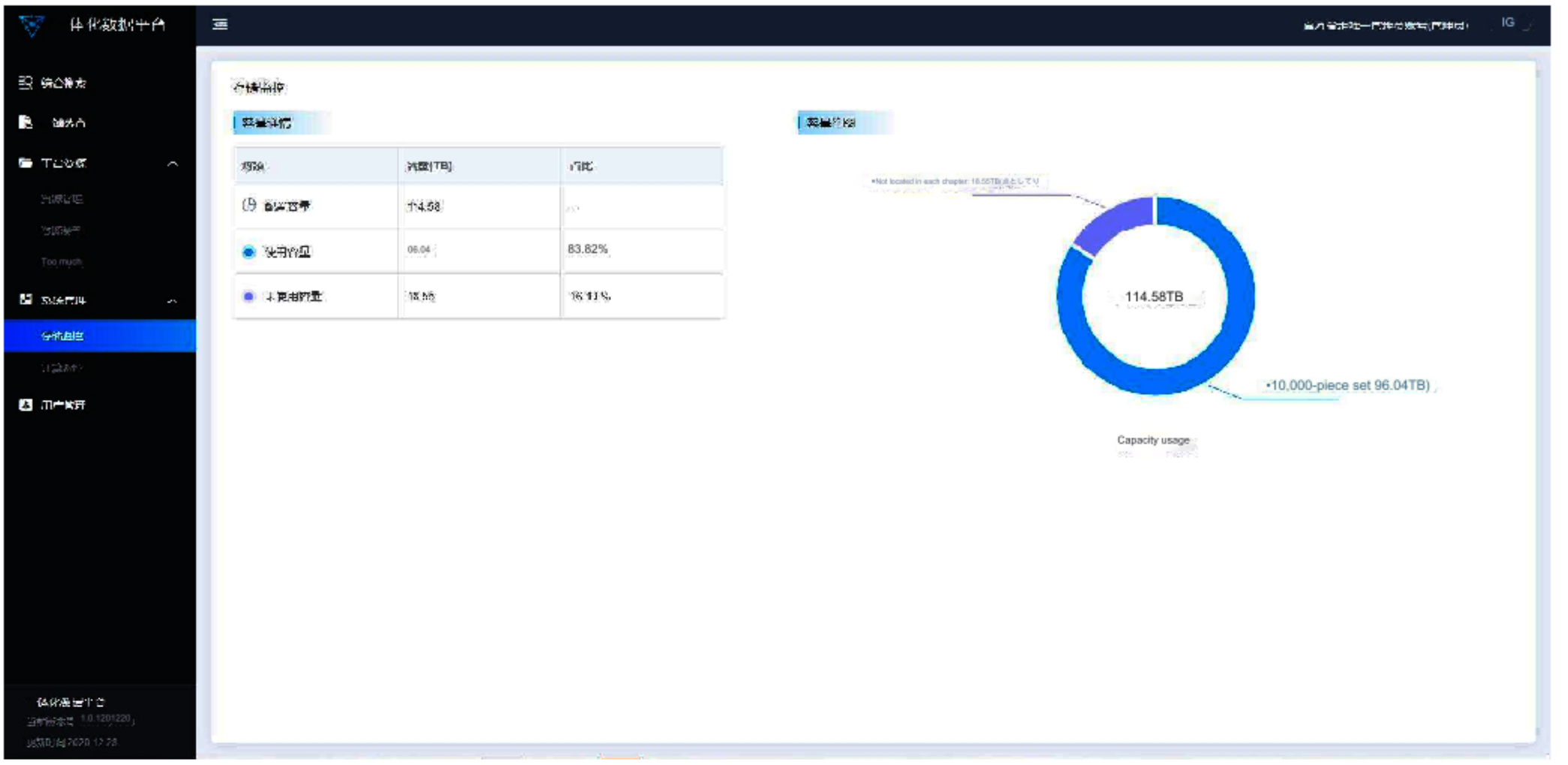
(shared management)

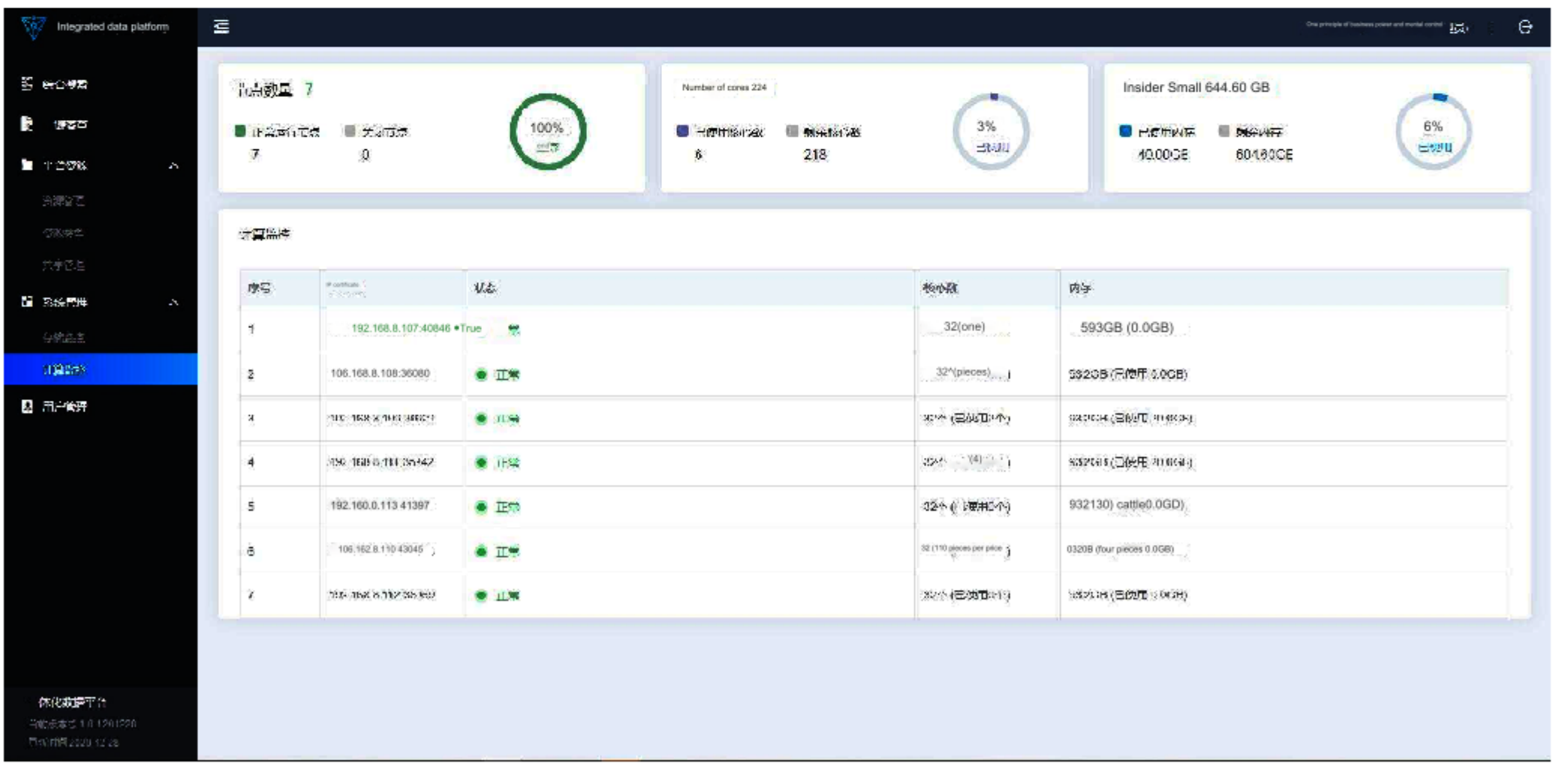


(security analysis)

4.4 System management

Users can view and monitor the real-time data and status of the backend server through the "System Management" toolbar, including server memory usage, configuration capacity, number of nodes, number of cores, IP address, etc. Through system management, customers can promptly discover whether the server is working abnormally or have insufficient memory problems, so that they can respond early.



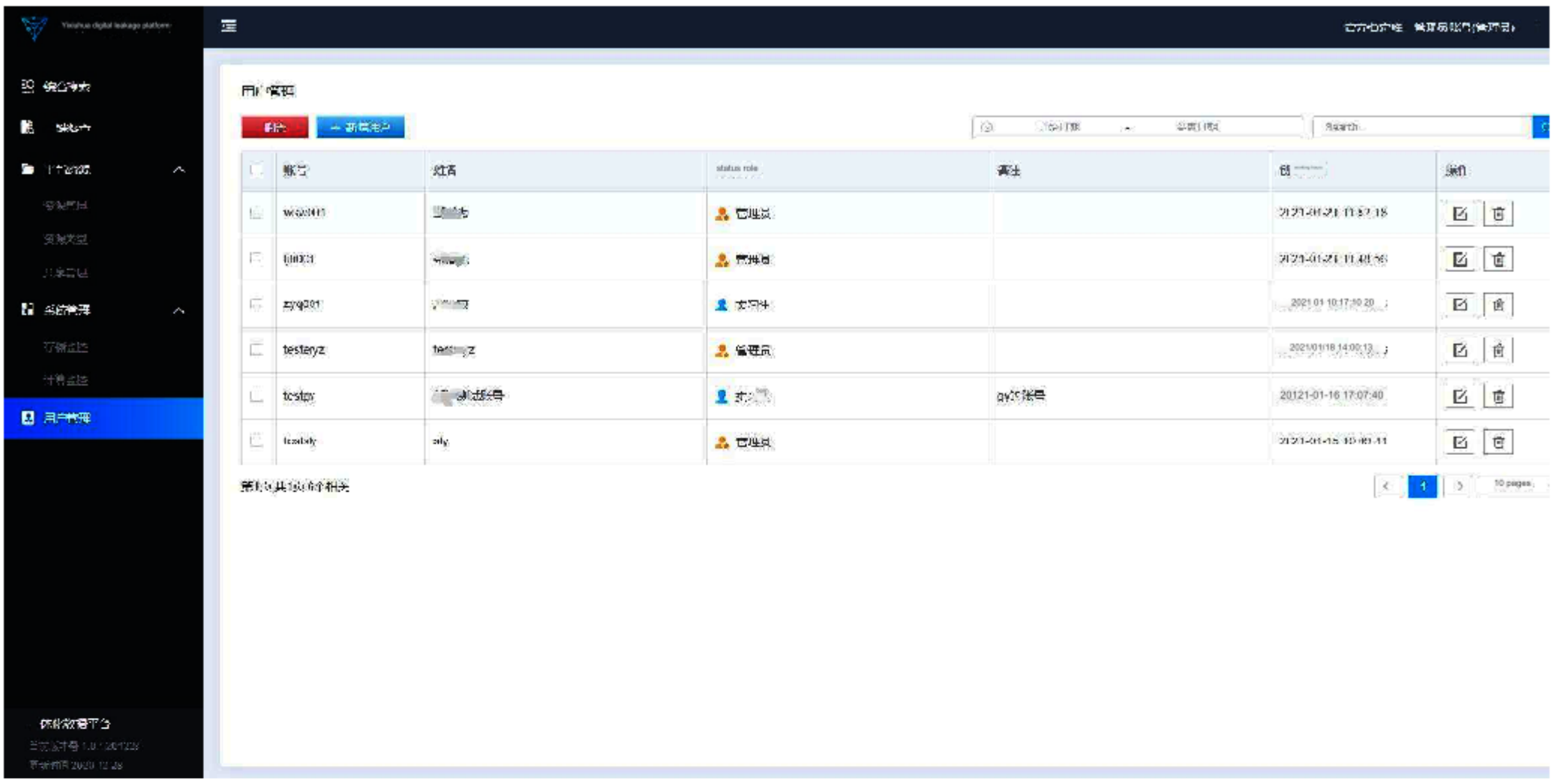


(System Management)

4.5 User management

In the "User Management" toolbar, the account of the currently logged-in user can be displayed, and the user can edit (nickname, password, delete)

operations on the current account.

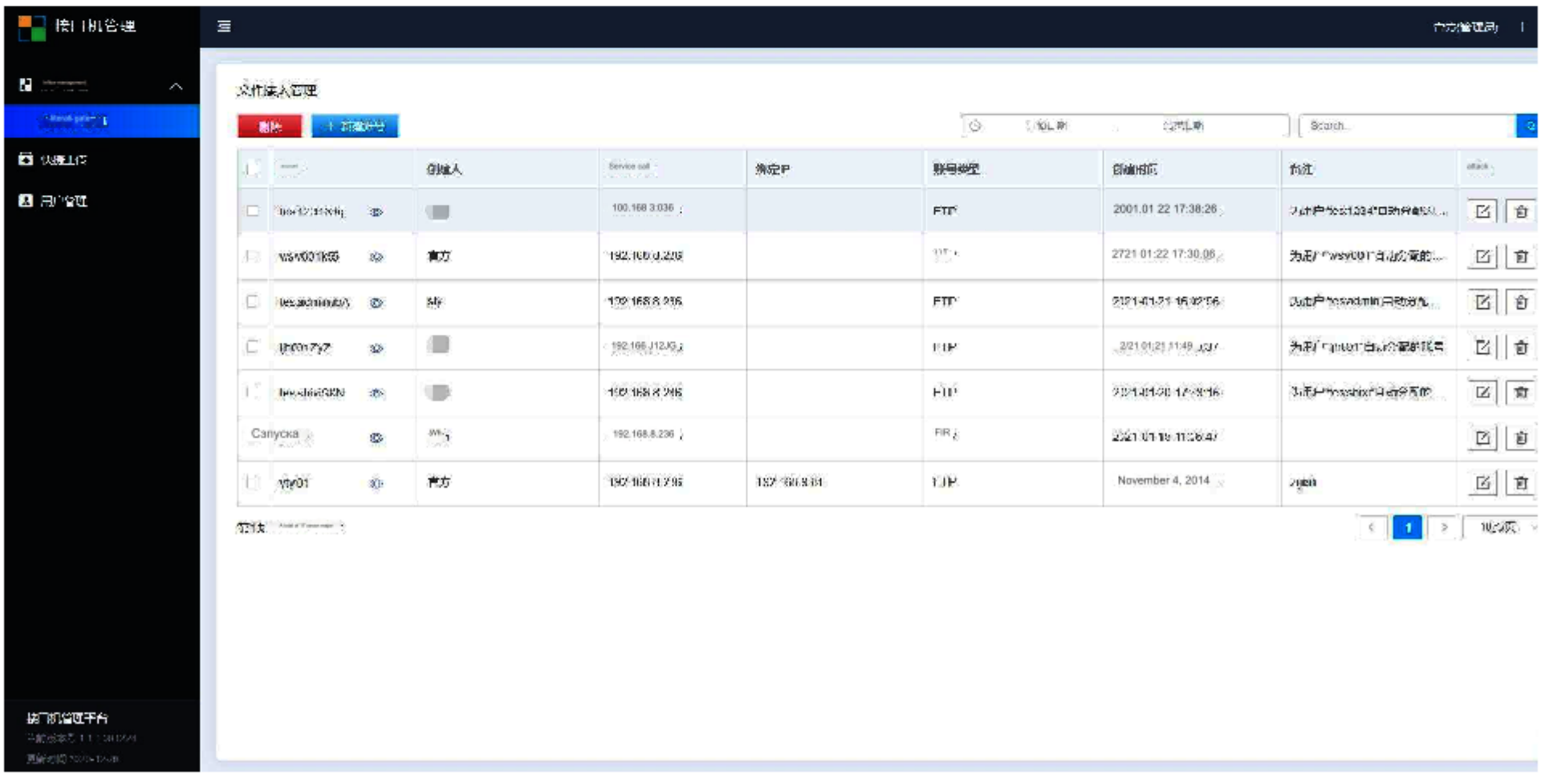


(User Management)

4.6 Data import

By logging in to the client software or interface machine platform management interface and connecting to our-integrated data platform, you can perform operations

such as batch import, transmission, deletion and editing of data files.



(data import)

5 product deployment

Configuration Environment	Environmental parameters
Hardware environment	Any computer model can be used
	At least one USB2.0 or above interface
	It is recommended that the computer requires a dual-core CPU, 4GB of running memory, and a discrete graphics card or above.
	The storage computing server recommends 64 cores, 128G running memory, and 8T hard disk.
	Web server recommended 32 core 64G running memory hard disk 1T
Software Environment	The operating system requires win7 and above.
	Browsers that support HTML5, Chrome and Firefox are recommended
	Install the .Net Framework 4.6 framework
Web environment	Internet access

6.1 Applicable environment

"Anxun Integrated Data Platform" is suitable for scenarios where users analyze and judge massive amounts of data. The platform adopts a B/S architecture. Users store data on a server that meets the configuration, log in to the backend management platform on a computer, and gain network access. permission, you can log in and use it.

6.2 Deployment method

Anxun-integrated data platform uses B/S architecture to provide services to users, so users can choose to build their own servers or use hosting. The Platform can be accessed and used via a qualified computer and an available Internet network. Specific computer configuration requirements are as follows:

Configuration Environment	Environmental parameters
Hardware environment	Any computer model can be used
	At least one USB2.0 or above interface

	It is recommended that the computer requires a dual-core CPU, 4GB of running memory, and a discrete graphics card or above.
	The storage computing server is recommended to have 64 cores, 128G running memory, and 8T hard disk.
	The web server recommends 32-core 64G running memory hard disk 1T
Software Environment	The operating system requires win7 and above.
	Browsers that support HTML5, Chrome and Firefox are recommended
	Install the .Net Framework 4.6 framework
Web environment	Internet access

6 product advantages

> Rich data types

Supports data import of multiple data types, intelligent identification, and automatic extraction of important information. After the platform cleans and classifies the data, users can select the corresponding data to perform query tasks according to their own needs. The data types cover basic personal information (data, identity) certificate, phone number), population data, operator data, network data and other data, which can effectively meet the work needs of business departments.

> Query speed is fast

Data query speed block, after selecting the corresponding data query module, through keyword related search, you can query data related to keywords in seconds, effectively improving query efficiency.

> High security

Imported data supports identity authentication, IP whitelisting and security scanning analysis. In addition, the server supports built-in redundant backup to prevent data disasters. By adopting a cluster architecture, the physical cluster size can be freely selected according to business needs to ensure load balancing and automatic failover.

> Ease of use

The platform has a simplified structure, is easy to operate, and has a beautiful interface. It does not require complex configuration to perform data query tasks, which greatly improves the experience. At the same time, distributed storage is used to naturally support horizontal expansion. It is easy to operate and has good compatibility with third-party systems and platforms.