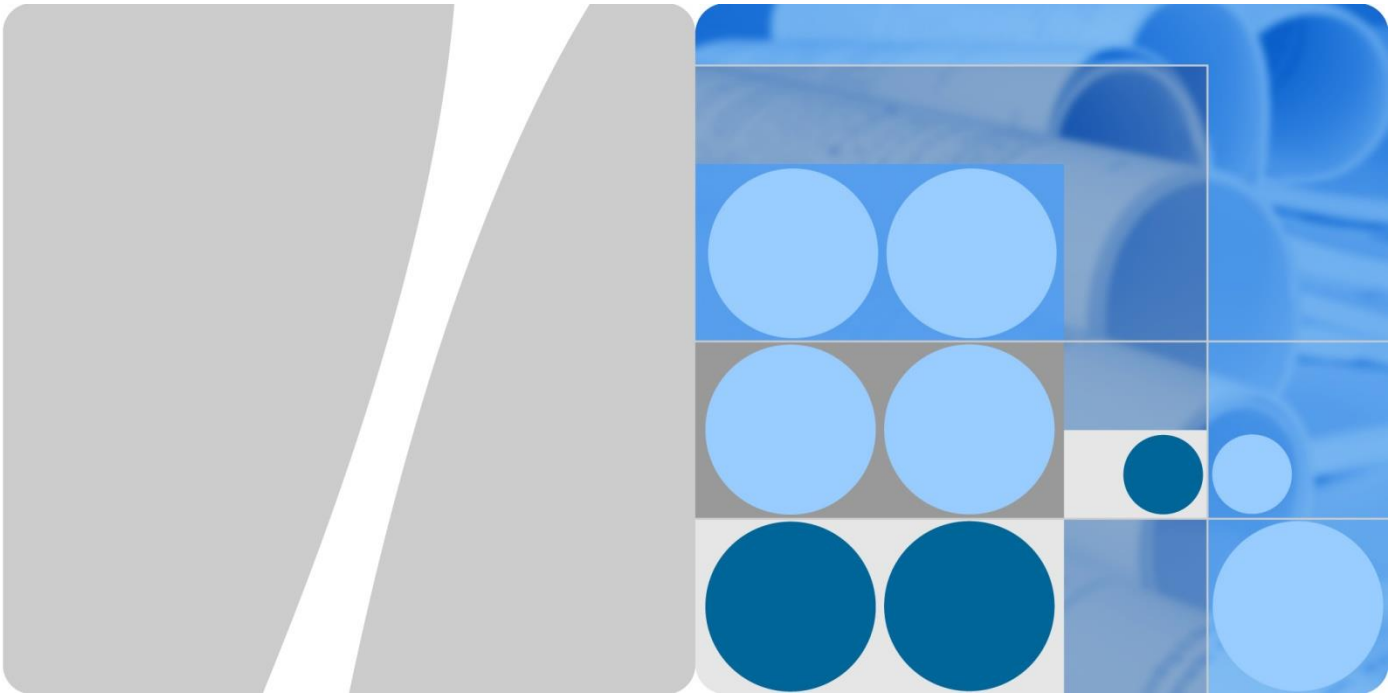


Huawei FusionAccess V100R006C20

Feature Description

Issue 01

Date 2018-03-23

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://e.huawei.com

Contents

1 Basic Features

1.1 Basic Virtual Desktop Services

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●		●

Introduction

The Huawei FusionAccess Desktop Solution provides Windows 7 and Windows 10 desktops and flexible desktop configuration (such as CPU, memory, storage, and network resources) to meet different requirements.

Users can log in to their virtual desktops using a thin client (TC) or software client (SC) to work like using a PC.

NOTE

In this document, unless otherwise specified, the virtual desktop is also referred to as the virtual machine (VM).

Benefits

The basic virtual desktop services can meet requirements for security office automation (OA), research and development (R&D), and educational institutions.

1.1.1 Pooled Desktop

Version Requirements

The Pooled Desktop feature has been available since version 5.0.

In FusionAccess 5.3, full copy VMs are supported, and dynamic pooled desktops support power management and self-help console functions.

In FusionAccess 6.0, FusionSphere 5.1 Update1 and later versions are supported. FusionStorage supports the shutdown restoration function.

In FusionAccess 6.1, the function of binding a user with a VM within a period of time is supported and the function of specifying user rights by comprehensively copying dynamic pool user groups is added.

In FusionAccess 6.2, the single-account pooled desktop feature is added. In scenarios where a dynamic pool has no personalized programs and data, users can use a single account to log in to the dynamic pool and randomly allocate desktops.

Summary

The Pooled Desktop feature is provided to assign desktop VMs to users based on the resource pool. Both the dynamic and static pooled desktop functions are supported.

Feature Description

Desktop VMs are assigned to users based on the resource pool. FusionAccess 5.3 supports linked clone static pooled and dynamic pooled desktops, and full copy static pooled and dynamic pooled desktops.

- Dynamic Pooled Desktop refers to a desktop group of the M:N pool type. The binding relationship between VMs in the desktop pool and users is not fixed. When a user logs in to the desktop pool through the Web interface (WI), the Huawei Desktop Controller (HDC) dynamically assigns an available VM to the user. However, if the user has been assigned with a VM and the VM has not been deregistered, the HDC will assign the original VM to the user when the user logs in to the desktop pool again.
- Static Pooled Desktop refers to a desktop group of the 1:1 pool type. Originally, the binding relationship between VMs in the desktop pool and users is not fixed. However, the binding relationship between a VM and user is fixed after the user logs in to the VM for the first time. After that, the user will be assigned with the same VM each time the user logs in to the desktop pool, and the VM will not be assigned to other users.
- Linked Clone Pooled Desktop enables multiple VMs to share a desktop image in linked-clone mode and supports automatic VM restoration after shutdown and one-click restoration in storage area network (SAN) virtualization and FusionStorage scenarios.
- Full Copy Pooled Desktop does not support automatic VM restoration after shutdown or one-click restoration. Dynamic Pooled Desktop supports power management and self-help console functions.
- The single-account pooled desktop feature allows you to set the maximum number of desktops that can be logged in to by a single account when the account logs in to the dynamic pool. The single-account pooled desktop feature cannot be used together with the MAC computer binding feature.

  Note that the full memory pooled desktop is not supported when the VRM (KVM) platform is used.

Application Scenario

Windows Virtual Desktop
●

1.1.2 Dedicated Desktop

Version Requirements

The Dedicated Desktop feature has been available since version 5.0.

Summary

The Dedicated Desktop feature is provided to assign a dedicated VM to each user. A user can install personal application programs and save customized data on the dedicated VM.

Feature Description

Each user is assigned with a dedicated VM. A user can install personal application programs and save customized data on the dedicated VM. Dedicated Desktop is related to full copy.

The application programs and customized data for the user are not affected if the dedicated VM is shut down or restarted.

Application Scenario

Windows Virtual Desktop
●

1.1.3 Server Desktop (Commercially Used Under Control)

Version Requirements

The Server Desktop feature has been available since version 5.3.

Windows Server 2016 is supported in version 6.1.

Summary

The Server Desktop feature supports Windows Server independent virtual desktops in VDI scenarios.

Feature Description

Windows Server 2008 R2, Windows Server 2012 R2, and Windows Server 2016 desktops are supported. This feature is a controlled commercial feature.

Windows Server 2008 R2 Standard, Windows Server 2008 R2 Enterprise, and Windows Server 2008 R2 Data Center editions are supported. Windows Server 2012 R2 Standard and Windows Server 2012 R2 Data Center editions are supported. In addition, Windows Server 2016 Standard and Windows Server 2016 Data Center editions are supported.

Windows Server 2008 R2, Windows Server 2012 R2, and Windows Server 2016 provide 64-bit versions only. However, most software and drives run on 32-bit versions. Software incompatibility problems may exist although 32-bit applications can run on 64-bit OSs.

Windows Server 2012 R2 does not support video redirection, USB key login, GPU passthrough and virtualization, and remote assistance features.

In the desktop cloud leasing scenario, to meet OS license authorization requirements of Microsoft, you can use Windows Server 2008 R2 experience package (released by Microsoft) to provide Windows 7 experience, and use Windows Server 2016 experience package (released by Microsoft) to provide Windows 10 experience.

Application Scenario

Windows Virtual Desktop
●

1.1.4 Windows Virtual Desktop

Version Requirements

The Windows Virtual Desktop feature has been available since version 5.0.

The OS supports traditional Chinese and Portuguese in version 5.3.

Windows 10 Desktop is supported in version 6.0.

Summary

The Huawei FusionAccess Desktop Solution provides Windows XP, Windows 7, Windows 8.1, and Window 10 virtual desktops of various specifications to meet different requirements.

Feature Description

The Huawei FusionAccess Desktop solution provides Windows XP (32-bit) and Windows 7 (32-bit and 64-bit) virtual desktops of various specifications to meet different requirements.

The Huawei FusionAccess Desktop Solution supports virtual desktops running on the following OSs:

- Windows XP Professional (32-bit) with service pack 3 or later
- Windows 7 Professional (32-bit or 64-bit)
- Windows 7 Ultimate (32-bit or 64-bit)
- Windows 8.1 Professional (32-bit or 64-bit) and Windows 8.1 Enterprise (32-bit or 64-bit)
- Windows 10 Professional (32-bit and 64-bit), Windows 10 Enterprise (32-bit and 64-bit), and Windows 10 Educational (32-bit and 64-bit) are supported. For details about the compatible OS versions, see the Compatibility Check Assistant: http://support.huawei.com/onlinetool/datums/fusioncloud/comptool/index.en.jsp

  Windows 8.1 does not support video redirection, USB key login, GPU passthrough and virtualization, and remote assistance features.

  Windows 10 does not support flash redirection and automatic recognition features in audio scenarios.

  Windows10 supports only LTSB and CBB service options, so you need to control its upgrade and adopt the delay update mode.

Microsoft has announced that no technical support will be available for the Windows XP OS after April 2014, and the Windows 7 OS has stronger compatibility and better performance than the Windows XP OS. Therefore, the Windows 7 OS is recommended.

In the desktop cloud leasing scenario, to meet OS license requirements of Microsoft, you can use Windows Server 2008 R2 to install the Windows experience package (released by Microsoft) to provide Windows 7 experience.

The OS supports Chinese (simplified and traditional), English, Arabic, Portuguese, and Spanish. Other languages must be tested.

Note that the Windows XP desktop is not supported when the VRM (KVM) platform is used.

Application Scenario

Windows Virtual Desktop
●

1.1.5 Linux Virtual Desktop (Commercially Used Under Control)

Version Requirements

The Linux Virtual Desktop (commercially used under control) feature has been available since version 6.0.

The FusionAccess 6.1 version supports local account login and AD authenticated emergency channels. It also supports a maximum resolution of 1920 x 2480, dual display, and windows.

Summary

FusionAccess Desktop Solution provides Linux virtual desktops such as Red Hat, Ubuntu, and NeoKylin to meet user requirements on Linux office application scenarios. At the same time, the administrator can batch provision desktops and centralize management and control of the desktops.

Feature Description

FusionAccess Desktop Solution can provide Linux OS virtual desktops to meet user requirements on Linux office application scenarios. At the same time, the administrator can batch provision desktops and centralize management and control of the desktops.

The supported Linux OS includes: Red Hat Enterprise Linux 6.6(RHEL) x86 and x64, Ubuntu 14.04 LTS Desktop x86 and x64, and NeoKylin 6.0 Update1 x64.

Scenario description: Linux virtual desktops are applicable to simple task-based application scenarios (only simple applications are supported, such as FireFox, OpenWord, OpenExcel, and OpenPDF. Peripherals are not required) instead of R&D scenarios.

Critical functions and constraints include:

1. Supporting Red Hat Enterprise Linux 6.6 (RHEL) 32-bit and 64-bit, Ubuntu 14.04 LTS Desktop 32-bit and 64-bit, and NeoKylin 6.0 Update1 64-bit (Chinese home-made OS, applicable only in China).

2. Supported TC types: CT3200, CT5100, CT6100, ST5110, and ST6110. CT5100, CT6100, ST5100, and ST6110 support Windows and Linux versions.

3. Supporting Windows SC login, not supporting Android/IOS login from mobile terminals

4. Supporting unified user management through AD domain, user password authentication, AD authenticated emergency channels, and local account login. Smart card and fingerprint authentication are not supported.

5. Supporting dual-screen and a maximum resolution of 2480 x 1920 for a single screen. Supporting file redirection.

6. Imported service provisioning is supported, while fast service provisioning is not supported. Full copy VMs are supported, and linked clone and full memory VMs are not supported.

7. Multi-user session and remote assistance are not supported.

8. The GPU function is not supported.

9. Peripherals cannot be used to connect applications (including but not limited to USB ports, serial and parallel port devices).

10. Audios and videos are not supported (including but not limited to video and music playback, and network phones calls).

NOTE

For details of other Linux desktop constraints, refer to Linux features and constraints in Sales Guide.

Application Scenario

Linux virtual Desktop
●

1.2 Virtual Desktop Access Management

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

Desktop cloud access services are provided, including the access protocol (such as HDP) and access mode (such as WI and UNS). Users can log in to their virtual desktops using a TC or SC to work like using a PC.

Benefits

Users can access their desktops in various modes.

1.2.1 Virtual Desktop Access Service

Version Requirements

The Virtual Desktop Access Service feature has been available since version 5.0.

FusionAccess 6.1 supports the forcible power-off function.

Summary

Users can connect to virtual desktops by using the Huawei Desktop Protocol (HDP) and start, restart, or forcibly restart virtual desktops.

Feature Description

Logging In to Windows VMs Using HDP

The HDP protocol is an efficient, secure, and reliable desktop protocol. With this protocol, Internet users can connect to VMs using their accounts and passwords without the IP address or the domain name of the VM. The HDP protocol is the default protocol used by the FusionAccess system.

Starting, Restarting, and Forcibly Restarting VMs

Users can start, restart, or stop a VM through the WI.

When a VM is stopped, users can start the VM through the WI and log in to the VM.

When a VM is faulty, users can restart, forcibly restart, or forcibly stop the VM through the WI.

The VM in dynamic pool mode will restore to the initial status in provisioning phase after being forcibly restarted.

Supported Browsers

The WI supports the following browsers: Internet Explorer 8 to Internet Explorer 11, Firefox 32 to Firefox 49, and Google Chrome 37 to Google Chrome 63.

Only the basic login function is available when Google Chrome and MAC OS Safari are supported. MAC address binding, smart card, and fingerprint login are not supported.

Application Scenario

Windows Virtual Desktop
●

1.2.2 Unified Access Domain Name

Version Requirements

The Unified Access Domain Name feature has been available since version 5.2.

SBC has been available since version 5.3.

Summary

Users can use the uniform access domain name to access virtual desktops or remote applications of Huawei FusionAccess Desktop Solution R2 or R5.

Feature Description

The unified access domain name service GUI provides the following functions:

- GUI style 1: Supports deregistration, GUI language change, customized background, and VM list display.
  - R2 VMs: Users can click to choose the ICA protocol to log in to the VM, forcibly restart the VM, and restart the VM.
  - R5 VMs: Users can click to choose HDP to log in to the VM, set power management policies, implement VNC self-service maintenance, forcibly restart the VM, and restart the VM.
- GUI style 2: Supports deregistration, GUI language change, and customized background.
  - R2 VMs: Users can click to choose the ICA protocol to log in to the VM, forcibly restart the VM, and restart the VM.
  - R5 VMs: Users can click to choose HDP to log in to the VM, set power management policies, implement VNC self-service maintenance, forcibly restart the VM, and restart the VM.

Only Chinese and English are supported.

Multiple FusionAccess systems interconnected with UNS must share a same domain. Multiple domains are not supported.

The application virtualization of R002C01 is not supported.

NOTE

R3 virtual desktops are not supported by default. If R3 virtual desktops are required, contact the desktop cloud maintenance department.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.2.3 Unified Desktop Access Pool

Version Requirements

The Unified Desktop Access Poll feature has been available since version 6.2.

Summary

Multiple dynamic pool desktop groups in one or more sets of FusionAccess environments can be logically grouped using the UNS to merge into a larger unified desktop access pool.

This feature improves the usage of desktops in multiple dynamic pools, presents the unified desktop group information regardless of the production environment or DR environment, and provides the affinity by working with the GSLB.

Feature Description

This feature applies to the following scenarios:

1. Improving the usage of the dynamic pool desktops

- ✓ Assign multiple dynamic pool desktop groups in one or multiple FusionAccess environments to the same user group.
- ✓ Deploy a set of UNS to connect to the FusionAccess environment, configure the UNS, and set the dynamic pool desktop groups to a desktop group collection where the priorities of the desktop groups are the same.
- ✓ When a terminal user logs in to the desktop pool using the UNS, the system randomly assigns a proper pooled desktop to the user.

2. Shielding the production or DR environment

- ✓ Assign multiple dynamic pool desktop groups in the FusionAccess production or DR environment to the same user group.
- ✓ Deploy a set of UNS to connect to the FusionAccess environment, and set the dynamic pool desktop groups to a desktop group collection. In the desktop group collection, the desktop groups in the production environment have a higher priority, while that in the DR environment have a lower priority.
- ✓ When a terminal user logs in to the desktop pool using the UNS, the system randomly assigns a proper pooled desktop to the user.

3. Access affinity

- ✓ Assign multiple dynamic pool desktop groups in the FusionAccess environments in different regions to the same user group.
- ✓ Deploy multiple sets of UNSs to connect to the FusionAccess environments, set the dynamic pool desktop groups to a desktop group collection, and plan the priorities of the desktop groups in each UNS.
- ✓ Deploy GLSBs at the front end of the UNSs. When the terminal user accesses a set of UNS through GLSB and logs in to the unified desktop access pool, the system allocates a proper pooled desktop to the user based on the UNS configuration.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.2.4 Dual-Desktop on a Single Client

Version Requirements

The Dual-Desktop on a Single Client feature has been available since version 5.3.

Summary

If only one screen connects to the VM (HDP disables multi-display and the client uses a single screen in full screen mode) when multiple monitors connect to the client, users can drag the client window to the other screen, or display the local desktop in one screen and remote desktop in the other.

Feature Description

In common VDI scenarios without HDP multi-display disabled, the client window can be dragged to the other screen.

When an SC is used, one screen can be used to display the local desktop, and the other can be used to display the remote desktop.

Application Scenario

Windows Virtual Desktop
●

1.3 Application Virtualization

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

The FusionAccess Desktop solution provides the Application Virtualization feature with the SBC technology. With this technology, application programs are installed in the data center, and users access the data center to use the applications using a TC, PC having an SC installed,

or mobile user terminal. Similar to virtual desktops, the running environment and data of applications are stored in the data center. The clients only transmit information about the keyboard, mouse, and screen updates.

The Application Virtualization feature applies to scenarios requiring simple operations, such as the client for querying security information, and training and exam systems.

Benefits

This feature enables centralized management and maintenance of applications deployed in data centers. Users can use applications without installing the applications.

1.3.1 Centralized Application Provisioning Management

Version Requirements

The Centralized Application Provisioning Management feature has been available since version 5.3.

The FusionAccess 6.1 version supports application classification in the provisioning process.

The FusionAccess 6.2 version supports icon customization in the provisioning process.

Summary

The Centralized Application Provisioning Management feature centrally manages applications and provides virtual applications to users who are in different locations and use different terminals. The Centralized Application Provisioning Management feature provides application server management and application creation, publishing, query, and deletion functions.

Feature Description

The Centralized Application Provisioning Management feature centrally manages applications and provides virtual applications to users who are in different locations and use different terminals. The Centralized Application Provisioning Management feature provides application server management and application creation, publishing, query, and deletion functions.

Application classification in the provisioning process is supported, but only level-1 classification catalog is supported.

Users can check the format of a customized application icon and restore the icon to its original form.

Application Scenario

Application Virtualization
●

1.3.2 Unified Application Access Service

Version Requirements

The Unified Application Access Service feature has been available since version 5.3.

The FusionAccess 6.1 version supports the AD and configures the application access under interactive login group policy.

Summary

Users can access remote applications using HDP, remotely start or stop applications, and access applications using an agent.

Feature Description

Users can access remote applications using HDP, remotely start or stop applications, and access applications using an agent.

Remote applications and shared desktops can be managed in a list. Users can save remote applications to favorites, delete them from favorites, and turn pages to view remote applications.

The WI supports Internet Explorer 8 to Internet Explorer 11, Mozilla Firefox 32 to Mozilla Firefox 49, and Google Chrome 37 to Google Chrome 63.

Google Chrome and MAC OS Safari browsers are also supported, but only basic login functions are available on these browsers. MAC address binding, smart card, and fingerprint login are not supported.

AD is supported and the application access under interactive login group policy is configured.

Application Scenario

Application Virtualization
●

1.3.3 Shared Desktop

Version Requirements

The Shared Desktop feature has been available since version 5.3.

In FusionAccess 6.2, Windows Server 2016 can be used as the APS server.

Summary

The Shared Desktop feature supports Windows Server shared desktops in SBC application virtualization scenarios.

Feature Description

Complete desktops are provisioned based on SBC application virtualization, and Windows Server shared desktops are supported. Users are isolated based on sessions, and data is stored in the profile file which is stored on the file server in roaming mode. The Windows Server 2008 R2, Windows Server 2012 R2, and Windows Server 2016 OSs support this feature.

It is recommended that the APS server (application server) run on the Windows Server 2012 R2. Customers have to purchase licenses of Windows Server 2012 R2 and Remote Desktop Services (RDS).

Application Scenario

Application Virtualization
●

1.3.4 Remote Application

Version Requirements

The Remote Application feature has been available since version 5.3.

In FusionAccess 6.2, Windows Server 2016 can be used as the APS server.

Summary

Remote applications are provisioned based on SBC application virtualization. The Windows Server 2008 R2, Windows Server 2012, and Windows Server2016 OSs support this feature.

Feature Description

End users can open multiple shared desktops or remote applications and switch between the shared desktops or remote applications by clicking on the taskbar.

It is recommended that the APS server run on the Windows Server 2012 R2. Customers have to purchase licenses of Windows Server 2012 R2 and RDS.

Application Scenario

Application Virtualization
●

1.3.5 APS Load Balancing

Version Requirements

The APS Load Balancing feature has been available since version 5.3.

Summary

Shared desktops and remote applications can be assigned based on APS loads, and load balancing is implemented based on the number of users, CPU usage, and memory usage.

Feature Description

Shared desktops and remote applications can be assigned based on APS loads, and load balancing is implemented based on the number of users, CPU usage, and memory usage.

Application Scenario

Application Virtualization
●

1.3.6 Window-based Shared Desktops and Remote Applications

Version Requirements

The Window-based Shared Desktops and Remote Applications feature has been available since version 5.3.

Summary

The Window-based Shared Desktops and Remote Applications feature supports window-based display of shared desktops and remote applications.

Feature Description

Shared desktops and remote applications can be displayed in windowed mode. Shared desktops support Windows terminals only and automatic adjustment of resolution. Remote applications support Windows and Linux terminals.

Application Scenario

Application Virtualization
●

1.3.7 Voice Input

Version Requirements

The Voice Input feature has been available since version 5.3.

Summary

Mobile terminals are integrated with iFLYTEK voice input software. When a user runs an application, the user can input information by voice, which improves user experience.

Feature Description

Mobile terminals are integrated with iFLYTEK voice input software. When a user runs an application, the user can input information by voice, which improves user experience.

Application Scenario

Application Virtualization
●

1.3.8 Native Gesture

Version Requirements

The Native Gesture feature has been available since version 5.3.

In FusionAccess 6.2, Windows Server 2016 is also supported.

Summary

Native gestures of Windows Server 2012 and Windows Server 2016 are supported. Users do not have to change their usage habits.

Windows Server 2012 and Windows Server 2016 native gestures include the following:

- Tapping
- Holding
- Sliding
- Zooming using two fingers
- Dragging
- Rotating
- Flipping from the right edge to the left
- Flipping from the left edge to the right
- Flipping from the top/bottom to the middle

Feature Description

Native gestures of Windows Server 2012 and Windows Server 2016 are supported. Users do not have to change their usage habits.

Windows Server 2012 and Windows Server 2016 native gestures include the following:

- Tapping
- Holding
- Sliding
- Zooming using two fingers
- Dragging
- Rotating
- Flipping from the right edge to the left

- Flipping from the left edge to the right

Application Scenario

Application Virtualization
●

1.3.9 Application Self-Service Maintenance

Version Requirements

The Application Self-service Maintenance feature has been available since version 6.0.

The FusionAccess 6.2 supports the multi-instance SBC application tray and the application tray configuration data can be saved.

Summary

The Application Self-service Maintenance feature allows users to deregister sessions on clients to quickly release server resources and improve user experience. The feature supports:

1. Application tray (Windows, Linux)

2. Application auto login

Feature Description

1. Application tray (Windows and Linux) is supported.

For tray applications, tray display windows, for example, QQ and eSpace, can be used normally.

The application tray supports multiple instances. Different application shortcuts on the desktop can be associated with different WI addresses to open applications.

2. Application auto login is supported.

Auto maintenance agents can remember the password. Users do not need to enter the password to log in each time.

Application Scenario

Application Virtualization
●

1.3.10 Local Application Experience

Version Requirements

The Local Application Experience feature has been available since version 6.0, incorporating three original features: "merging local application menu", "Local Application Desktop Shortcut", and "Local Application Taskbar Display".

Summary

Integrating the shortcuts of remote applications to the menu bar, shortcuts and local taskbar of local Windows desktop is supported, so that application operation experience similar to the local desktop is provided.

Feature Description

Remote applications can be seamlessly integrated on the local Windows start menu, which improves user experience.

Shortcuts of remote applications can be generated on the local Windows desktop, which improves user experience.

When remote applications are minimized, their icons can be displayed on the local Windows taskbar, which improves user experience.

Application Scenario

Application Virtualization
●

1.3.11 User Data Storage

Version Requirements

The User Data Storage feature has been available since version 5.3.

Summary

The User Data Storage feature supports storage of user profile roaming data of shared desktops and remote applications.

Feature Description

User profile roaming: User profile data of shared desktops and remote applications is stored on a third-party shared file server using the roaming user configuration and folder redirection functions of Windows OSs.

User data storage: User personal data is stored on a third-party storage system, such as NAS.

Application Scenario

Application Virtualization
●

1.3.12 Application Policy Adjustment

Version Requirements

The Application Policy Adjustment feature has been available since version 5.3.

Summary

The Application Policy Adjustment feature supports RDS policy configuration for shared desktops.

Feature Description

RDS policy configuration for shared desktops is supported. RDS policies include the following:

- Setting the user home directory
- Clearing sessions that are disconnected for a long time
- Clearing sessions that are not operated for a long time
- Deleting temporary folders after user deregistration
- Assigning an independent IP address to each session

Polices can be configured on the FusionAccess management system, including the idle time limit for disconnection and when to deregister after disconnection.

Application Scenario

Application Virtualization
●

1.3.13 Application Session Management

Version Requirements

The Application Session Management feature has been available since version 5.3.

Summary

The Application Session Management feature is provided to automatically disconnect or deregister sessions after users disconnect shared desktops and remote applications for a certain period. Time policies can be set.

Feature Description

Sessions are automatically disconnected or deregistered after users disconnect shared desktops and remote applications for a certain period. Time policies can be set.

Administrators can view the session duration.

Administrators can send message notifications to each session, thereby facilitating system O&M.

Application Scenario

Application Virtualization
●

1.4 Series of Clients

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

A series of clients include TCs, Windows PC SCs, Android multimedia converged terminals, ChromeOS clients, and iOS and Android mobile clients.

Benefits

This feature allows the FusionAccess system to be deployed in various scenarios.

1.4.1 TC

Version Requirements

The TC access has been available since version 1.0.

The CT5100 and CT6100 have been available since version 5.3.

The CT1000 has been available since version 6.0.

Version 6.1 supports the hard floating-point ARM TC.

Version 6.2 supports CT3200, ST5110, and ST6110.

Summary

TCs of various models differ from each other in performance, peripheral ports, and operation screens to meet the requirements of different scenarios, such as common OA, high security, and high-performance graphics processing.

Feature Description

TCs, designed based on industrial standards, use embedded processors of low power consumption, small local flash memory, and simplified OSs to provide higher reliability and security and lower power consumption than PCs.

TCs of different specifications and configurations satisfy the requirements of various scenarios.

- CT3200

  The CT3200 is the next generation of the CT3100. It completely replaces the CT3100 in functions. The CT3200's CPU is upgraded to the quad-core 1.8 GHz and its hardware specifications are the same as those of the CT3100.

  The CT3200 applies to common OA.

- CT5100

  The CT5100 supports the following features:

  - Uses the Intel Bay Trail platform.
  - Supports a total power consumption of less than 15 W.
  - Compatible with HDP virtualization applications and allows users to enjoy smooth OA experience as well as optimal cloud-based multimedia experience.
  - Adopts the DVI-I interface to support dual-screen display.

  The CT5100 applies to common OA, call centers, branch offices, and task-based scenarios such as the education industry.

- CT6100

  The CT6100 supports the following features:

  - Uses the Intel Bay Trail platform.
  - Supports a total power consumption of less than 15 W.
  - Provides one USB 3.0 port, five USB 2.0 ports, four serial ports, and one parallel port, which can connect to various types of devices.
  - Adopts the DVI-I interface to support dual-screen display. Two gigabit NICs meet requirements of connections with two networks.

  The CT6100 applies to OA with multiple peripherals, common OA, and high-performance graphics processing scenarios.

- ST5110

  The ST5110 uses the Intel Baytrail platform and has the same CPU as the CT5100. It uses 4 GB DDR3 memory and 16 GB SSD storage, twice those of CT5100. The ST5110 also supports Wi-Fi and its standard configuration is one 2.4 GHz NIC (802.11 b/g/n). It has eight USB ports, whereas CT5100 has only six USB ports. The ST5110 also supports the DP display interface, and the DP display interface supports 2K resolution.

  The ST5110 is fully compatible with the HDP, delivering smooth OA experience, and higher and faster cloud multimedia experience.

- The ST5110 applies to common OA, R&D, and business hall scenarios.

  The ST6110 uses the Intel Baytrail platform and has the same CPU as the CT6100. It uses 4 GB DDR3 memory and 16 GB SSD storage, twice those of CT6100. The ST6110 also supports Wi-Fi and its standard configuration is one 2.4 GHz NIC (802.11 b/g/n). The ST6110 also supports the DP display interface, and the DP display interface supports 2K resolution. It has one USB 3.0 port and seven USB 2.0 ports, whereas CT6100 only has six ports. It also has one parallel port and four serial ports, which can be used to

connect to multiple external devices. In addition, the ST6110's two gigabit NICs can meet the requirements of dual network connection.

The CT6110 applies to OA with multiple peripherals, common OA, and high-performance graphics.

The CT3100 (Linux), CT3000 (Linux), Sunniwell S-Box8V40 (Linux), CT2000 (Linux), and GI945 (Windows and Linux) are supported, which are used after the desktop cloud is upgraded for compatibility purpose.

The CT2000/3000, GI945, and Sunniwell S-Box8V40 can concurrently connect to a maximum of one VM, while the CT3200/CT3100, CT5000/5100, CT6000/6100, and ST5110/ST6110 can concurrently connect to two.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.4.2 Basic SC

Version Requirements

The Basic SC feature has been available since version 1.0.

Peripheral capabilities of Mac OS clients and SBC have been available since version 5.3.

Client installation and application on Windows 10 has been available since version 6.0. The function of original cloud access configuration tool is integrated into C/S clients as a sub-function.

The Chrome client is supported since version 6.2.

Summary

The FusionAccess Desktop Solution comes with the Windows SC software, which enables Windows users to easily access virtual desktops and remote applications. SCs can be installed on Mac OSs.

Feature Description

Windows clients can connect to the desktop cloud system from Internet Explorer, Mozilla Firefox, and Google Chrome browsers. Before connecting to the desktop cloud system for the first time, the system will prompt users to download and install an SC plug-in so that users can connect to the desktop cloud from clients running Windows OSs.

SCs can be installed on Windows 7 (32-bit/64-bit), Windows XP (32-bit), Windows 8.1 (32-bit/64-bit), Windows 10, and Linux (Red Hat 6.6/Ubuntu 14.04 64-bit).

SCs can be installed on Mac OSs of version 10.9 and later. After installation, users can log in to virtual desktops from a Safari browser. Only drive or folder redirection and clipboard redirection are supported.

C/S clients are supported. C/S clients integrate the cloud access configuration tool, login browser and software client program, and can flexibly configure WI addresses and automatically detect WI address access with disaster tolerance ability.

C/S clients can save user login password, realizing virtual desktop auto login.

Toolbar of the client supports quick screen switch among multiple VMs.

Chrome (version 59 or later) clients provide basic desktop capabilities, such as keyboard, mouse, display, audio, and clipboard redirection, as well as file association and dual-display. Chrome clients can be used to access VDI and SBC.

NOTE

1. Fingerprint authentication and MAC address binding are not supported when users log in to virtual desktops from Google Chrome or Safari.
2. The Linux OS supports only officially released standard versions rather than other tailored versions. OSs of third-party TCs need to go through the Huawei Ready authentication process to check the client compatibility.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.4.3 Mobile Client

Version Requirements

The Mobile Client feature has been available since version 5.2.

Version 6.1 supports multi-domain scenarios and the binding between mobile clients and users.

Summary

Android and iOS mobile clients are supported.

Feature Description

Users can access virtual desktops and virtual applications from Android (version 4.1.2 or later) and iOS (version 8.0 or later) mobile clients.

Mobile client login in multi-domain scenarios is supported.

The terminal MAC addresses bind users automatically upon users' first login to mobile terminals, thereby meeting the secure login requirements of enterprises. You must enable Wi-Fi when using this function for the first time.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.4.4 TCM

Version Requirements

The TCM feature has been available since version 1.0.

Summary

The thin client manager (TCM) implements remote centralized maintenance, configuration, deployment management, security management, asset management, and performance monitoring on TCs. It supports the remote batch operations of system restoration, system upgrade, and patch installation.

Feature Description

The TCM provides the following functions:

- Power control: TCs can be remotely powered on, powered off, registered, and waken up.
- System configuration: An intelligent TC configuration tool is provided to remotely configure TCs of different models, from different vendors, or running different OSs. End users do not need to perform any operations during this phase.
- Software distribution: Software can be distributed in batches. This feature enhances network security by eliminating incorrect software installation.
- System image management: helps users quickly install, recover, and back up OSs on clients. This function is primarily used for upgrading OSs on Windows TCs.
- Task management: Tasks, especially tedious, time-consuming operations, are performed based on preset policies and task dependency rules, achieving unattended operation.
- Message management: A tool is provided for administrators and TC users to communicate in real time.
- Log management: Activities of administrators and TCs are logged and archived, helping users locate faults.
- Performance monitoring: TCs' performance is monitored. The collected information helps trace TC running status and handle emergencies. In addition, reports are provided for users to know the TC performance.
- Agent upgrading: Users can distribute upgrade packages to clients and configure the TC Agent software to automatically install the packages.
- User management: User management covers user creation, resource allocation, account examination and approval, and role management.

NOTE

The TCM can be used only to manage the CT3000/3100/3200/5000/5100/6000/6100. A dedicated TC management system is provided for the Sunniwell S-Box8V40/ST5110/ST6110, which provides different functions from the TCM.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.4.5 Local Desktop Lock of Windows SCs

Version Requirements

The Local Desktop Lock of Windows SCs feature has been available since version 5.1.

In version 6.1, this function is integrated to the CS client. Local desktop lock and auto login can be used together. Users can manually stop their local PCs.

Summary

The Local Desktop Lock of Windows SCs feature allows users to access the desktop cloud from traditional Windows PCs.

Feature Description

Enterprise users are likely to access local PC resources after they connect to virtual desktops through Windows PCs. To ensure that users can easily differentiate between local PC and virtual desktop resources and quickly learn how to use virtual desktops, the Access Lock solution is deployed, which ensures that the experience of using virtual desktops is the same as that of using local desktops.

After the Access Lock solution is deployed, users cannot access the taskbar and Start menu of PCs after logging in to the PCs but directly view the WI login page.

The AccessLock function cannot be used with the LazyDesk function.

This feature supports the following client OSs.

Application Scenario	Supported OS
VM OS	Windows XP 32-bit Windows 7 32-bit/64-bit Windows 10 32-bit/64-bit
PC OS	Windows XP 32-bit Windows 7 32-bit/64-bit

Application Scenario

Windows Virtual Desktop
●

1.5 Virtual Desktop Service Management

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●		●

Introduction

The Virtual Desktop Operation Management feature is provided by the web-based FusionAccess system. Users can access the system using Internet Explorer or Mozilla Firefox without a local client.

Virtual desktop operation management includes the following:

- Virtual desktop provisioning

  Users can perform the following operations:
  - Registering VM images
  - Creating, assigning, unassigning, querying, and deleting VMs.
- Virtual desktop maintenance and management

  Users can perform the following operations:
  - Managing VM templates
  - Adjusting VM configurations
  - Restoring linked-clone VMs in one-click mode

Benefits

Customers can uniformly manage virtual desktop assets and rapidly provision and maintain virtual desktop resources. This feature increases operation efficiency and reduces IT costs.

1.5.1 Desktop Provisioning Management

Version Requirements

The Desktop Provisioning Management feature has been available since version 5.0.

Static multi-user VMs can be assigned to user groups and VMs can be queried by template.

Summary

The Desktop Provisioning Management feature is provided to implement the following functions:

- Flexible creation of virtual desktops
- Assignment of virtual desktops in multiple modes
- Query of virtual desktops
- Unassignment of virtual desktops

- Deletion of virtual desktops

Feature Description

Creating VMs

Users can select an appropriate VM template to create VMs based on service requirements. The VM type can be linked clone and full copy.

- **Creation of VMs in the immediate mode**

  Users can create VMs one by one or in batches. A maximum of 100 VMs can be created at a time.

- **Creation of VMs by creating a scheduled task**

  Users can create a scheduled task to create VMs one by one or in batches at a specified time.

- **Creation of VMs in a flexible mode**

  Users can flexibly specify a data store when creating VMs. In this way, high-IOPS VMs and low-IOPS are matched well to prevent overload of high-IOPS VMs.

  When creating VMs, users can also select a required VM naming rule, domain name, and NIC based on the data plan.

- **VM group management**

  Each VM must belong to a VM group. Specify or create a VM group when a VM is created.

  The following table describes the VM group parameters.

Parameter	Description
VM Group Name	Uniquely identifies a VM group.
VM Group Type	Indicates the type of a VM group. Value: • Linked clone • Full copy
VM Group Description	Provides supplementary information about a VM group.

- **VM naming rule**

  The VM naming rule is as follows: A VM name consists of two parts: a prefix and digits. A VM name cannot exceed 15 characters.

  The prefix contains digits, letters, and hyphen (-), starting with a letter or digit, but cannot contain only digits.

  The digits are represented by a number sign (#).

Assigning VMs

- **Domain user and user group**

In the FusionAccess Desktop Solution, users and user rights are managed based on Active Directory (AD) domains. Each domain user belongs to a user group. Users must log in to the AD server to configure or modify a domain user and user group. If the AD server is deployed on a VM, users can log in to the AD VM using VNC.

The multi-AD domain deployment mode (inter-domain mutual trust) is supported.

- **Management of desktop groups**

  Each virtual desktop belongs to a desktop group. Specify or create a desktop group when a virtual desktop is created.

  The following table describes the desktop group parameters:

Parameter	Description
Desktop Group Name	Uniquely identifies a desktop group.
Desktop Group Type	Indicates the type of a desktop group. It can be one of the following types: • Dedicated: The VM-user ratio is 1:1 or 1:N • Pooled: If the VM-user ratio is M:N, the pool is dynamic or static.
Desktop Group Description	Provides supplementary information about a desktop group.

Querying VM information

Users can query VM information, including the name, VM ID, VM specifications, VM group name, actual IP address, running status, login status, assignment status, assignment type, desktop group name, user (group), login user, site information, resource cluster, service type, description, creation time, local area, and template ID.

Users can click a VM to view more information, such as storage, NICs, and monitoring of the VM.

Unassigning VMs

Administrators can reclaim the VMs assigned to users. For security reasons, the reclaimed VMs must be deleted.

Deleting VMs

The operation of deleting a VM varies depending on whether the VM has been assigned to any user:

- If the VM has not been assigned to any user, delete it directly.
- If the VM has been assigned to a user, unassign the VM from the user and delete it.

Creating VMs using specified IP addresses

Administrators can specify IP addresses of VMs during VM creation. Because of security requirements and regulations, it is not allowed for VMs to obtain dynamic IP addresses from the DHCP server. In this case, administrators can specify IP addresses on the ITA and create VMs using the specified IP addresses.

After VMs are successfully created using specified IP addresses, the VMs can be assigned to users and work correctly.

NOTE

The Windows XP virtual desktop and full memory desktop cannot be provisioned when the VRM (KVM) platform is used.

Application Scenario

Windows Virtual Desktop
●

1.5.2 Desktop Maintenance and Management

Version Requirements

The Desktop Maintenance and Management feature has been available since version 5.0.

The following functions are added in version 5.1: one-lick automatic restoration of linked-clone VMs, safe deletion of VMs, and assignment/unassignment of VMs.

Summary

This feature provides the following functions: one-click automatic restoration of linked-clone VMs, safe deletion of VMs, and VM assignment and unassignment.

Feature Description

One-Click Automatic Restoration of VMs

The automatic OS restoration function is supported only by linked-clone VMs and PvD linked-clone VMs.

Safe Deletion of VMs

Safe deletion of VMs means that if a VM has sensitive or import data, the disk data will be completely deleted before the VM disk space (logical volume) is allocated to other users.

Modification of VM Configurations

The following VM configurations can be modified: VM service type, vCPU quantity, memory size, QoS configuration, and VM description.

VM Status Adjustment

Users can start/wake up, restart, hibernate, or shut down VMs.

Users can create a scheduled task to start/wake up, restart, hibernate, or shut down VMs periodically or at a specified time.

Application Scenario

Windows Virtual Desktop
●

1.5.3 Multi-AD Domain Deployment

Version Requirements

The Multi-AD Domain Deployment feature has been available since version 5.1.

Summary

The Huawei FusionAccess Desktop Solution supports the multi-AD domain deployment mode (inter-domain mutual trust). A certain number of users are managed in each AD domain. Multiple AD domains can be in the parent-child relationship or in a forest. The parent domain and child domain have a mutual trust relationship with each other, and inter-domain mutual trust must be established between domains in a forest.

Feature Description

The Huawei FusionAccess Desktop Solution supports the multi-AD domain deployment mode (inter-domain mutual trust). A certain number of users are managed in each AD domain. Multiple AD domains can be in the parent-child relationship or in a forest. The parent domain and child domain have a mutual trust relationship with each other, and inter-domain mutual trust must be established between domains in a forest.

Application Scenario

Windows Virtual Desktop
●

1.6 Virtual Desktop Maintenance Management

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

The System Operation and Maintenance feature is provided by FusionManager, and auxiliary functions are provided by FusionAccess.

The operation and maintenance (O&M) system provides a web-based user interface that can be accessed using Internet Explorer or Mozilla Firefox. A local client is not required.

The following O&M functions are provided:

- Configuration management
- Log management
- Alarm management
- System monitoring
- Resource statistics
- License management
- Clock synchronization
- Rights- and domain-based management
- Separation of roles
- Policy management

Benefits

This feature enables carriers to centrally maintain and monitor systems, improving the O&M efficiency.

1.6.1 Configuration Management

Version Requirements

The Configuration Management feature has been available since version 5.0.

Configuration wizard for first logging in to the system after the ITA installation is added in version 6.0.

Version 6.1 adds the LiteAD configuration page function.

Summary

The FusionAccess O&M System provides initial system configuration and O&M-based configuration functions, including initial configuration, time management configuration, and rights management configuration.

Feature Description

Configuration wizard for first logging in to the system after the ITA installation is supported. This function can automatically complete initial configuration steps such as virtual environment, domain, desktop components, and alarm component after users enter according to the wizard tips, which greatly simplifies data configuration process after the initial installation.

After the system is installed, users can adjust configurations on configuration management function page:

Initial Configuration

The following initial system data can be configured: IT adapter (ITA) database data, FusionCompute connection data, domain data of infrastructure servers, and configuration data of FusionAccess components.

A maximum of 16 sets of virtual desktop infrastructure (VDI) devices can be configured for one FusionAccess system.

Time Management Configuration

Time and time zone configuration covers:

Time synchronization configuration: includes configuration of primary and secondary domain controllers, query period, and IP address of the clock source.

Time zone configuration: Whether DST is supported can be specified.

Rights Management Configuration

- User management configuration

  Create user accounts for logging in to FusionAccess to query system information and maintain the system.

  The desktop management domain accounts are supported, enabling unified management, easy maintenance, and simple account management.
- Role management configuration

  Create a system administrator, and set management permissions of the system administrator.
- Area management configuration

  Configure virtual desktop management areas, and set desktop administrators of areas. Administrators who join an area have permissions to manage VMs in the area.
- Password policy configuration

  Set policies for system administrator's passwords and user lock conditions.

Configuration of Other Functions

- Tomcat configuration

  The Tomcat account must be the same as that configured on the AD and ITA servers. The Tomcat account is used to manage created VMs, for example, assigning or renaming VMs.
- Session timeout period configuration

  The login session timeout period can be set to 5 minutes to 2 days.
- Auditing rule configuration

  The system automatically enables the internal data verification function after the auditing rule is configured. Perform the audit in idle time because the audit occupies system resources.
- Auditing rule configuration

Domain Controller Management

- Domain user management

  Manage the user configurations of LiteAD, including creating, deleting, disabling, enabling, and unlocking users. In addition, users can be imported in a batch.
- Domain user group management

  Manage the user group configurations of LiteAD, including creating and deleting user groups, as well as adding users to user groups.
- DNS forwarder management

  LiteAD can be configured as the DNS forwarder that forwards DNS information to the upper-level DNS server for domain name resolution. A maximum of three DNS servers can be configured.
- Domain password policy

  Information about domain users, such as password strength, validity period, and lock threshold and time, can be configured.

  NOTE

Domain controller management configuration applies only to LiteAD scenarios. LiteAD supports only single domain and single site, and does not support SBC. Microsoft AD is recommended in SBC scenarios.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.6.2 Log Management

Version Requirements

The Log Management feature has been available since version 5.0.

Query of user login information is supported in version 5.1.

The security audit log upload function is supported in version 5.3.

Summary

Log management includes management of FusionManager and FusionAccess operation logs.

The system management module of FusionAccess provides the following functions: filtering and querying administrator operation logs of the FusionAccess system, and querying user login information.

The log management module of FusionManager provides the following functions: filtering and querying administrator operation logs of the FusionManager system, and querying user login information.

Feature Description

Collecting Operation and Login Logs of FusionManager

After logging in to the FusionManager system, administrators can view and query user login information and operation information in log management of the system module. The information includes the following: operation user, operation name, user IP address, operation time, component type, component name, level, operation result, and detailed information. If the operation failed, the failure cause is also recorded.

Logs can be exported or searched by type.

Collecting Operation and Login Logs of FusionAccess

After logging in to the FusionAccess system, administrators can view and query user login information and operation information from the operation logs of the system management module. The information includes the following: operation user, operation name, level, user IP address, start time, end time, operation result, and detailed information. If the operation failed, the failure cause is also recorded.

Logs can be exported or searched in batches by type. A maximum of 60,000 data records can be exported at a time.

Log association is supported. Logs about operations on VMs can be searched by log number, facilitating fault location.

Logs can be printed by level. Usable logs are provided for onsite engineers and customers to quickly locate faults.

Operation logs of system administrators and user login logs are uploaded to a third-party log audit system in FTP mode. The log system centrally audits and analyzes logs to meet audit requirements.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.6.3 Alarm Management

Version Requirements

The Alarm Management feature has been available since version 5.0.

Version 6.1 supports the alarm indicating that the certificate between components is about to expire. In addition, this version supports the function of reporting desktop cloud alarms by emails based on alarm levels and types. Desktop cloud alarms can be exported.

Version 6.2 supports alarms indicating that the third-party backup server is not connected.

Summary

The FusionManager alarm monitoring module supports management for the cloud platform, enabling O&M personnel to locate faults.

The FusionAccess alarm monitoring module supports alarm and status monitoring for the FusionAccess desktop system, enabling O&M personnel to locate faults.

Feature Description

FusionManager Fault Management

- Alarm information

  An alarm is generated when a fault occurs, reminding O&M personnel of the fault. The alarm information of FusionManager contains the following information: alarm name, object type, alarm object, alarm severity, component name, component type, start time, and clear time.
- Guidelines for handling alarms

  In the alarm GUI, O&M personnel can clear an alarm and locate the alarm to the physical topology of the component where the alarm is generated. In the alarm name column, O&M personnel can click an alarm to view the alarm causes and handling suggestions.
- Alarm threshold setting

  Alarm thresholds can be set for the downstream bandwidth of a physical server, CPU temperature, and hard disk usage. Alarm thresholds can also be set for the storage allocation rate, CPU allocation rate, and memory allocation rate of cloud resource pools.
- Alarms reported by mail

  After a mail server and the recipient mailbox are configured for alarm reporting, alarm information can be directly forwarded to the recipient. This enables O&M personnel to check and handle alarms in a timely manner.
- Alarm masking setting

  Information about the alarms to be masked, including the alarm ID, alarm name, component type, and operator information, can be set.
- Third-party component management

  Alarms generated by a third-party device or component can be reported to FusionManager for management. The SNMPv2 and SNMPv3 versions are supported.

- Alarm exporting

  Alarm information of the cloud platform can be exported for analysis.
- Alarm statistics

  Cloud platform alarms can be collected at the specified interval for statistical purpose.

FusionAccess Alarm Management

- Alarm information

  An alarm is generated when a fault occurs, reminding O&M personnel of the fault. The FusionAccess alarm information of FusionAccess contains the following information: alarm name, object type, alarm object, alarm severity, start time, clear time, and clear type.
- Guidelines for handling alarms

  O&M personnel can clear alarms in the alarm GUI. In the alarm name column, O&M personnel can click an alarm to view the alarm causes and handling suggestions.
- Alarms reported by mail configuration

  After a mail server and the recipient mailbox are configured for alarm reporting, alarm information can be directly forwarded to the recipient. This enables O&M personnel to check and handle alarms in a timely manner. Specific alarms can be reported by emails based on alarm levels and types.
- Alarm export

  Alarm information of the desktop cloud can be exported to a local computer in a unified manner for analysis and statistics. The certificate expiration alarm among components is supported and the expiration time is 30 days by default, which is configurable.

  Alarms indicating that the third-party backup server is not connected are supported.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.6.4 Desktop System Monitoring

Version Requirements

The Desktop System Monitoring feature has been available since version 5.1.

Original **System Monitoring** and **Desktop System Monitoring** are merged in version 6.0.

In version 6.2, the build version number of the Windows 10 VM can be displayed.

Summary

Integration monitoring on Cloud resources (computing resource, storage resource, and virtual resource) usage and current status is supported. Software and hardware resources of the system can be shown in diagrams.

The Desktop System Monitoring feature allows users to query login and VM information.

Desktop management component status is monitored.

The system prompts the last login address and login time after the VM terminal changes.

Feature Description

Monitoring of cloud resources in FusionAccess Desktop Solution is provided by FusionSphere management portal, including:

Monitoring clusters: TOP CPU usage cluster, TOP memory usage cluster, TOP CPU reservation cluster, TOP memory reservation cluster, TOP storage allocation cluster, and TOP storage usage cluster.

Monitoring server hosts, including server CPU usage, server memory usage, network inflow and outflow usage, disk IO read and write usage, disk space usage, and so on.

Monitoring VMs, including VM CPU usage, VM memory usage, network inflow and outflow usage, disk IO read and write usage, disk space usage, and so on.

In FusionAccess Desktop Solution, FusionAccess Management Portal (ITA) provides monitoring functions related to desktop applications, including:

The AccessAgent versions, VM specifications, VM IP addresses, VM OS types, running status, login status, login users, and creation time can be displayed in the VM list, and the OS type, OS version number, profile file path, CPU usage, memory usage, network latency, and login duration are displayed in VM details. In addition, VMs can be filtered based on multiple criteria.

The FusionAccess alarm monitoring module supports status monitoring for desktop system management components. Monitored components include AD/DNS/DHCP, databases, HDC, ITA, and Loggetter.

User VMs prompt the last login addresses and login time when users change terminals to log in to the desktop VMs.

Application Scenario

Windows Virtual Desktop
●

1.6.5 Resource Management

Version Requirements

The Resource Management feature has been available since version 5.0.

The CPU resource control and memory resource control functions are added in version 5.1.

Summary

The FusionManager resource management module manages physical resources and virtual resources for the cloud platform, which helps O&M personnel perform daily maintenance. Physical resources include computing devices, network devices, storage devices, and physical locations.

Feature Description

Computing Device Management

Server management discovers server configuration information and performs maintenance operations (such as power-on, power-off, and restart) on servers. In addition, the following server information can be monitored: CPU usage, memory usage, incoming and outgoing traffic, and disk I/O (write and read). The monitored performance data can be queried by week, month, year, or a scheduled time.

Network Device Management

Network device management discovers switch configuration information and displays switch port status information. The port status information includes the connection status, transmit rate, receive rate, packet loss rate, and error rate during packet transiting and receiving. In addition, firewalls and load balancers can also be managed.

Storage Device Management

Storage device management discovers storage devices and checks configuration information about storage devices. The configuration information includes storage device location, product model, status, management IP address, and number of disks. In addition, users can query the total capacity and available space of storage devices to determine whether storage expansion is required.

Physical Location Management

Physical location management manages and records the names and locations of equipment rooms and cabinets.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.6.6 VM Live Migration

Version Requirements

The VM Live Migration feature has been available since version 5.0.

Summary

VM live migration does not affect VM services, and users are unaware of the migration.

Feature Description

Before powering off a computing server for maintenance purposes, administrators must perform live VM migration to relocate the VMs on the server to another server. VM live migration does not affect VM services, and users are unaware of the migration.

VM live migration must be implemented within a resource cluster. The VM to be migrated must be in the **Running** state and the destination computing server must have sufficient available CPU and memory resources for the VM.

Application Scenario

Windows Virtual Desktop
●

1.6.7 License Management

Version Requirements

The License Management feature has been available since version 5.0.

The licensing mode, licensing by the number of users and the number of concurrent users, is supported in version 6.0.

Summary

The system supports management of licenses.

Feature Description

A license is an agreement made by and between Huawei and a customer on the scope of usage, functions, and time restrictions of the product that has been sold or purchased. A license is required for scenarios such as installation, upgrade, and expansion.

Administrators can view license information and upload license files on the license management system.

License management in the Huawei FusionAccess Desktop Solution consists of the cloud platform license and desktop access license. For the cloud platform license, the licensing mode, licensing by physical server CPU, is used.

Desktop cloud licenses include the Standard Edition, Advanced Edition, and SBC Standard Edition. Two licensing modes are supported: licensing by the number of users or the number of concurrent users. The Standard Edition provides the VDI function only. The Advanced Edition provides VDI, SBC, HDP Plus (120 Mbit/s HD video editing and 4K video editing), and Linux desktop functions. The SBC Standard Edition provides the SBC function only.

The licensing mode, licensing by the number of users and the number of concurrent users, is supported. Users can purchase two licensing modes at the same time: licensing by the number

of users and the number of concurrent users and only apply for one License file to activate it in the management system. For blending licensing mode, different types of users are required to deploy one set of HDC, each set of which should specify a control type: the number of users or the number of concurrent users.

If users purchase Standard Edition and Advanced Edition at the same time, they can only apply for one License file to activate them.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.6.8 Clock Synchronization

Version Requirements

The Clock Synchronization feature has been available since version 5.0.

Summary

The system supports clock synchronization, which implements time consistency between the clocks of the FusionAccess desktop system servers and VM clocks.

Feature Description

Clock synchronization is the prerequisites to ensure stable running of the FusionAccess desktop system. If the time of system clocks is not synchronized, management of the FusionAccess desktop system will be chaotic. Clock synchronization ensures time consistency between the clock of the FusionAccess desktop system and VM clocks.

The AD server and the IP address of the upper-layer clock source must be configured to ensure that the time of the AD server is synchronized with that of the upper-layer clock source.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.6.9 Desktop Protocol Policy Management

Version Requirements

The Desktop Protocol Policy Management feature has been available since version 5.1.

Virtual channel bandwidth and priority management are supported in version 5.3.

Parameter control for network adaptive flow control is supported in version 6.1.

Summary

The Desktop Protocol Policy Management feature allows administrators to customize desktop policies based on service rules and requirements.

Feature Description

On the FusionAccess GUI, administrators can customize desktop policies based on service rules and requirements and synchronize the desktop policies to the HDC. When user VMs register with the HDC, the HDC delivers the policies to VMs.

Administrators can customize policies about the USB, audio, flash, multimedia, client, GDI Display, smartcard, Toolkit Without An Interesting Name (TWAIN), printer, and others. Administrators can enable or disable the peripheral redirection function. Administrators can also set parameters for audio, display, and high-performance graphics to ensure best user experience in related scenarios.

Virtual channel bandwidth management: An absolute bandwidth limit or bandwidth percentage is set for each virtual channel of the desktop protocol to ensure user experience. Virtual channels that support bandwidth limit and percentage control are as follows: display, audio, multimedia redirection, flash, file redirection, clipboard, printer, parallel port, TWAIN, USB, and serial port.

Parameter control of network QoS adaptive policies, including network delay, dynamic frame rate, image lossy compression quality, and video quality, is supported.

After a desktop policy is formulated, the application object and scope of the policy must be specified. Desktop policies can apply to desktop groups, VMs, users, user groups, OUs, terminal IP addresses, and application groups.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.6.10 Desktop Access Control Policy Management

Version Requirements

The Desktop Access Control Policy Management feature has been available since version 5.3.

A TC can be bound to a VM in version 6.0.

The TC can be bound to a user automatically upon the user's first login in version 6.1.

Summary

Virtual desktop access can be controlled based on the client IP segment, specific client, and access time.

Feature Description

Access control based on the client IP segment: supports configuration for client IP segment access rights. Users are not allowed to log in from a non-specified IP segment. An IP segment contains IP addresses and subnet masks.

Access from specific clients can be configured. That is, TCs are bound with domain usernames.

Access control based on the access time: specifies users, user groups, terminal IP addresses, VMs, and desktop groups to access VMs and virtual applications in a specified period. Applications in the specified application resource pool can be accessed. This policy does not support DST. OUs of application objects do not support computer OUs.

Application objects of polices are as follows:

When domains are deployed, policies apply to users, user groups, OUs, VMs, terminal IP addresses, desktop groups, and application groups.

In this version, you can configure that a specific user can access the VM on a specific client. That is, the TC binds to a domain username. In addition, upon a user's first login to the VM, the system binds the client and the user automatically, implementing entry without the MAC address.

You can also configure that a specific client can access a specific virtual desktop. That is, the TC binds to a VM.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.6.11 Daylight Saving Time

Version Requirements

The Daylight Saving Time (DST) feature is added in version 5.0.

Summary

The FusionAccess system allows DST-based time adjustment for regions that use DST.

Feature Description

If Huawei FusionAccess Desktop is deployed in a city that supports DST, the DST time is (usually one hour) ahead of the standard time of the time zone. When DST ends, users need to switch the DST time to the local time on the VDI system, including the management system and user VMs. The DST feature provides the following functions:

After the time zone of a city is correctly set on the OS (Windows) of a user VM, a correct DST time is displayed on the OS after the user logs in to the VM if the OS supports DST switching. If the OS does not support DST switching, the DST switching time point needs to be manually configured.

The FusionAccess infrastructure server can correctly display the local DST time.

FusionAccess, FusionCompute, and FusionManager use the same clock source. When they switch to the DST time (the local time changes) at the same time, the system still runs properly.

During DST switching, the time on the unified portal and the log time use the local time, and time-related tasks are not affected.

Application Scenario

Windows Virtual Desktop
●

1.6.12 Support for Multiple Languages

Version Requirements

The Support for Multiple Languages has been available since version 5.0.

Summary

The FusionAccess system supports Chinese and English.

Feature Description

The FusionAccess system supports Chinese and English.

The WI login page of user VMs supports Chinese, English, and Arabic.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.6.13 Virtual Desktop Rights- and Domain-based Management

Version Requirements

The Virtual Desktop Rights- and Domain-based Management feature has been available since version 5.1.

Division of domain of resource statistics is supported in version 6.1.

Summary

Virtual desktop rights- and domain-based management: Multiple administrators can be created in the FusionAccess Operation Management System and are granted different operation and data access rights based on their roles and domains. Only the administrators granted corresponding rights can perform operations and view VM data.

Feature Description

Default System Administrators

The system defines the following types of roles by default:

- The system administrator has all the operation and data access rights to the system. The system administrator is responsible for routine system maintenance, and has permission to configure the portal system, perform operations on services, and manage users.
- The operation administrator has all or some operation and data access rights. The system administrator defines an operation administrator, and assigns operation and data access rights to the operation administrator. Usually, operation administrators do not have permission to manage users.
- The system viewer has permission to query service data, but does not have permission to perform operations on services, configure the system, or manage users.

Customized Administrator Rights

When the FusionAccess O&M system and the FusionManager O&M system are deployed on the same portal, administrator rights cannot be self-defined. When the FusionAccess O&M system is deployed independently, administrator rights can be self-defined.

If the default roles cannot meet management requirements, the super administrator can define roles and assign rights to the roles based on actual requirements. The role management, area management, and user management can be implemented by defining roles and rights. Administrators, for example, can be categorized as service administrators that manage services, administrators that manage personnel, and auditors that audit logs. The super administrator account can be reclaimed after these roles are created, separating the management of service, personnel, and auditing.

- Rights-based management

  The operations on the system can be defined. A role can be assigned any operation rights. An administrator can play more than one role and has all the operation rights assigned to these roles.
- Domain-based management

  The system supports domain-based VM management. That is, VMs can be allocated to a specified area or subarea so that the administrators who have the data rights of the area or subarea can manage these VMs.

  Domain-based management of status statistics, performance statistics, historical registration exception statistics, user online duration, and unused VM statistics items is supported.

Application Scenario

Windows Virtual Desktop
●

1.6.14 Separation of Roles

Version Requirements

The Separation of Roles feature has been available since version 5.1.

In version 6.0, operations performed in the high risk operating system by administrators can take effect only after being audited by safety officers.

Summary

The Separation of Roles feature separates operation rights of roles. Operation rights, such as service control, system configuration, log management, alarm management, and account role management rights, are separated. A role cannot have all the above rights. This enhances system account security.

Feature Description

In the separation of roles scenario, rights of the system administrator, security administrator, and security auditor are independent of each other and restrict each other. The system administrator is responsible for system routine O&M. The system administrator has permission to configure the system and manage services, alarms, and logs but does not have permission to manage rights. The security administrator is responsible for account management. The security administrator has permission to manage rights (such as accounts and roles), areas, and password policies but does not have permission to perform service operations. The security auditor is responsible for auditing operations of the system administrator and security administrator. The security auditor can only view alarms and logs. The security administrator and security auditor cannot be the same person.

In the separation of roles scenario, the system provides three roles by default: the system administrator, security administrator, and security auditor. Each role has a default account.

In non-separation of roles scenarios, relationships between ITA accounts, roles, and rights are the same as those in earlier versions.

Operations performed in high risk operating system by administrators may take effect after being audited by safety officers.

Application scenarios and constraints of the Separation of Roles feature are as follows:

- Two account management modes are available: separation of roles mode and common mode. Determine the mode when installing and configuring FusionAccess. The user management module can support only one mode at a time. The mode cannot be changed after installation.
- The authentication mode (separation of roles or common) must be determined when the FusionAccess Desktop Solution is installed and configured. Only one authentication mode can be deployed on a node at a time.
- When roles and accounts are created, the types of roles and accounts must match the account management mode.
- In Huawei FusionAccess Desktop Solution 5.1, the separation of roles mode must be deployed on FusionManager, FusionAccess, and FusionCompute at the same time. Otherwise, the mode cannot be used. If the common mode is deployed on FusionManager but the separation of roles mode is deployed on FusionAccess, users cannot access ITA from FusionManager because no corresponding roles and rights exist

on ITA. In this case, you need to set the separation of roles mode on FusionManager, and then FusionManager can associate with ITA.

- FusionAccess operation logs do not support separation of roles. All administrators can view and perform operations on logs.
- Sites that do not use the separation of roles mode cannot be upgraded to sites that use the separation of roles mode.
- If you want to replace the common mode with the separation of roles mode, you need to uninstall ITA and reinstall it.

Application Scenario

Windows Virtual Desktop
●

1.6.15 Desktop Session Management

Version Requirements

The Desktop Session Management feature has been available since version 5.2.

Support for screen lock, disconnection, and deregistration settings is added in version 5.3.

Summary

Desktop sessions can be managed, for example, disconnecting user connections and deregistering user VMs on the desktop management system.

Feature Description

Desktop sessions can be managed, for example, disconnecting user connections and deregistering user VMs on the desktop management system.

Screens are locked after the keyboard and mouse are in idle time for a certain period. Desktops are disconnected or deregistered after screens are locked for a certain period. This function is disabled by default. You can enable the function by setting ITA policies.

Application Scenario

Windows Virtual Desktop
●

1.6.16 Desktop Management for Any VMs

Version Requirements

The Desktop Management for Any VMs feature has been available since version 5.2.

VMs running on the OpenStack platform can be managed in version 5.3.

Version 6.2 supports wizard-based import and management of VMs provisioned by the FusionAccess OpenStack platform.

Summary

VMs that are not created by FusionAccess can be added to the desktop management system and used as virtual desktops.

Feature Description

VMs that are not created by FusionAccess can be added to the desktop management system and used as virtual desktops.

For example, VMs created using desktop cloud templates on FusionManager can be added to the desktop management system and allocated to specified users. These VMs can also be managed by FusionManager and use advanced features of FusionManager, such as the security group.

Power management for VMs running on the OpenStack platform is supported, including restarting or forcibly restarting, stopping, and starting VMs. Other functions are not supported currently.

Application Scenario

Windows Virtual Desktop
●

1.6.17 Device Archives

Version Requirements

The Device Archives feature has been available since version 5.2.

Summary

Device archives are maintained on the desktop cloud system.

Feature Description

Device archives are maintained on the desktop cloud system. Users can export information such as versions from the service maintenance tool.

Application Scenario

Windows Virtual Desktop
●

1.6.18 Flexible Configuration of Desktop Access Page

Version Requirements

The Flexible Configuration of Desktop Access Page feature has been available since version 5.2.

The image size and resolution can be adjusted within a certain range in version 6.1.

Summary

The administrator can change images on the WI or UNS login page.

Feature Description

By changing the images, the administrator can change the web page label icon, system logo, daily notice image, login image, and background image on the WI or UNS login page. The image format and file name must be the same as that of the system built-in image. The image size and resolution can be adjusted within a certain range.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.6.19 Unified GUI Management

Version Requirements

The Unified GUI Management feature has been available since 5.0.

Summary

The FusionManager system provides a unified graphical user interface (GUI) that integrates the FusionAccess Desktop Service Maintenance System, Virtualization Platform, and Hardware Management System.

Feature Description

FusionManager obtains data using interfaces provided by lower-layer components to achieve unified GUI management.

- Home page

  FusionManager collects statistics on the health status and resource utilization of the cloud platform and displays the statistical information.

- Resources

  FusionManager creates a unified model for virtual resource management and provides a GUI for virtual resource management. FusionManager obtains virtual resource data through the virtual resource manager (VRM) interface. FusionManager supports initial

configuration of resources and can manage the resources. Resources include hardware devices, virtual resources, virtual resource pools, and VM templates.

- Organization

  An organization is used to manage certain resources. Rights- and domain-based management is implemented for virtual resources by adding, modifying, and deleting organizations and managing organization members and roles.

- Monitoring

  Alarms and performance of the cloud platform are managed and monitored.

- Task

  System tasks are displayed, including the task type, object, status, creation time, start time, end time, and creator.

- Report

  Statistics on devices, virtual resources, and network resources are collected and displayed on reports. Historical reports and real-time reports are provided.

- System

  System management includes system configuration, rights management, and log management. On the system configuration page, you can configure the desktop cloud address. After the external IP address of the Desktop Cloud Service Management System is configured, unified GUI management can be implemented for the Huawei FusionAccess desktop system.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.7 Basic Virtual Desktop Security

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

The Basic Virtual Desktop Security mechanisms include client security, user access authentication, transmission security, virtual desktop isolation, virtual desktop antivirus, and management system security.

The security mechanisms ensure the information security of the FusionAccess desktop system.

Benefits

This feature provides a desktop cloud-based IT system that has minimal security risks.

1.7.1 Client Security

Version Requirements

The Client Security feature has been available since version 5.0.

Summary

The clients support the Secure Sockets Layer (SSL) authentication mechanism. Unauthorized access is not allowed.

Feature Description

After the SSL authentication mechanism is enabled, import the SSL certificate to the client. Otherwise, the access request will be denied.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.7.2 Client Access Control Policies

Version Requirements

The Client Access Control Policies feature has been available since version 5.2.

Summary

IP segment access rights of clients can be configured. Users are not allowed to log in from a non-specified IP segment. An IP segment contains IP addresses and subnet masks.

Feature Description

IP segment access rights of clients can be configured on FusionAccess. Users are not allowed to log in from a non-specified IP segment. During settings, you need to enter valid IP addresses and subnet masks. You can enter multiple IP segments. The access control policies apply to desktop groups, VMs, and users.

Application Scenario

Windows Virtual Desktop
●

1.7.3 User Access Authentication

Version Requirements

The User Access Authentication feature has been available since version 5.0.

Management components use the Linux OS in version 6.0.

Version 6.2 supports the interconnection with the customer's existing Windows Server 2016 AD.

Summary

Client users log in to the FusionAccess desktop system through AD domain authentication. Client users can also log in to the FusionAccess desktop system through fingerprint, USB key, and dynamic password authentication.

Windows desktop management system components adopt AD domain authentication. The Linux component of the management system can be logged in by using non-root accounts (user **root** is disabled in remote login), and security of the user account and password must be ensured.

The FusionManager O&M system adopts authentication based on the AD domain or management system username plus password. The FusionAccess O&M system adopts authentication based on system username plus password.

Feature Description

End Users Logging In to the FusionAccess Desktop System

The AD domain authentication is implemented on end users for logging in to the FusionAccess desktop system. Users can enter the FusionAccess desktop system and access the desktop group and virtual desktop list only after passing the authentication of the AD system. The AD authentication uses single sign-on (SSO). Once logged in to the virtual desktop, users do not need to enter the username and password for the subsequent login.

Administrator Logging In to a Management System

The administrator can log in to a management system using one of the following authentication modes:

- Authentication based on the AD domain username and password: The Windows OS of a FusionAccess management component uses this authentication mode. The FusionManager O&M system can also use this authentication mode.
- Authentication based on the management system username and password: The FusionManager O&M system and FusionAccess O&M system use this authentication mode.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.7.4 Transmission Security

Version Requirements

The Transmission Security feature has been available since version 5.0.

Summary

To ensure information transmission security, the FusionAccess desktop system uses the SSL-based encryption and authentication mechanism for transmitting information from clients to servers and between internal components.

Feature Description

The SSL protocol is used to ensure secure data transfer over the Internet. The SSL protocol uses the public key technology to protect the security of the communication between users and servers.

Transmission security covers the following:

- Authentication data transferred over the Internet when end users log in to virtual desktops from the WI
- Protocol data transferred over the Internet when end users log in to virtual desktops using HDP
- Data transferred between the servers and the clients over the Internet when administrators use web management systems
- Data transferred over the Internet when components in the FusionAccess desktop system communicate with each other

NOTE

The Secure Sockets Layer virtual private network (SVN) device is required or vAG software security gateway needs to be deployed for client users to log in to virtual desktops using the SSL.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.7.5 Virtual Desktop Isolation

Version Requirements

The Virtual Desktop Isolation feature has been available since version 5.0.

Summary

Each virtual desktop user has logically independent VMs. Each VM has independent virtual CPUs (vCPUs), virtual memory, and virtual network resources. That is, VMs are isolated from each other. Users can access only the VMs that are assigned to them.

Feature Description

Virtual desktops are isolated as follows:

- Physical resources are isolated from virtual resources.

  The Hypervisor ensures that each VM obtains independent physical resources. The Hypervisor also ensures that the crash of one VM does not affect the Hypervisor and other VMs.
- VMs are isolated from each other.

  The Hypervisor isolates VMs running on the same physical machine to prevent data theft and malicious attacks. VMs isolation includes following aspects:
  - vCPU scheduling is used to isolate the OS from applications.
  - Virtual memory is isolated from each other.
  - Internal networks are isolated.
  - The I/O operations of hard disks are isolated.

Application Scenario

Windows Virtual Desktop
●

1.7.6 Virtual Desktop Antivirus Security

Version Requirements

The Virtual Desktop Antivirus Security feature has been available since version 5.0.

Summary

User VMs are protected against viruses by deploying antivirus software on user VMs or through antivirus virtualization.

Feature Description

- Commercial antivirus software is installed on user VMs to ensure VM security.

To learn the compatibility of antivirus software, carry out a POC test, or see the FusionAccess Desktop compatibility list.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.7.7 Management System Security

Version Requirements

The Management System Security feature has been available since version 5.0.

In version 6.2, the weak password dictionary can be used to log in to the ITA and the new and old passwords must be different in two characters.

Summary

In the FusionAccess Desktop Solution, security measures are taken on management nodes to ensure security of all management nodes.

Feature Description

Security Hardening for the Web Management System

The security of the FusionAccess O&M system and the FusionManager O&M system must be hardened.

Web management system security hardening is used to fix common and serious web vulnerabilities, thereby protecting the web system from hackers.

Management System OS Hardening

The Windows Server OS and SUSE Linux OS for the FusionAccess infrastructure servers and the SUSE Linux OS for the cloud platform management nodes must be hardened.

The following measures can be taken to harden the security of the Windows server OS:

- Set important key values of the system registry.
- Sets the services that can run on the Windows OS.
- Set the communication ports for systems.
- Set file sharing permissions.
- Set system auditing rules.
- Manage system accounts.
- Update system security patches.

The following measures can be taken to harden the security of the SUSE Linux OS:

- Stop unnecessary services.
- Reduce codes.
- Harden the secrete shell (SSH) service.
- Control access permission on files and directories.
- Restrict system access permission.
- Manage user passwords.
- Record operation logs.
- Detect system abnormality.

Antivirus Protection on Management Nodes

Antivirus software is deployed on nodes or VMs to protect components of the FusionAccess Desktop Solution from virus attacks.

- Infrastructure VM

  Trend Micro antivirus software is deployed on Windows Server VMs to protect infrastructure VMs from viruses.
- Management node

  The management node runs the reinforced Linux OS.

  The main hardening measures are: eliminating unnecessary codes, stopping unnecessary services, and controlling file and directory permission.
- Computing node and storage node

  The computing node and storage node run the reinforced Linux OS.

  The main hardening measures are: eliminating unnecessary codes, stopping unnecessary services, and controlling file and directory permission.

  The computing nodes and storage nodes are in the closed network, protecting them against virus attacks.

Database Hardening

Security hardening measures are taken on management system databases to improve database security. The following measures are taken to harden database security:

- Use the latest mainstream database version and has the latest security patches installed.
- Ensure that the password complexity meets security requirements, and do not use the default accounts.
- Use non-default ports as the database service ports.
- Use an independent OS account to run the database.
- Control the access permission on sensitive files.
- Clearly define the rights of every account, and ensure that each account has minimum rights only for performing its tasks.
- Set an independent password for databases that provide special functions.
- Enable the audit function if the database provides the security log audit function.

Log Auditing

Operation logs record all the operations of the administrator, such as login or logout, adding or deleting accounts, and changing account properties (including password).

An operation log includes information, such as the username, operation time, and operation result, and cannot be modified or deleted for the sake of security auditing.

Rights- and Domain-based Management

- Virtual desktop rights- and domain-based management

Operation permissions and management scopes of administrators are precisely controlled. Operation permissions of the super administrator are reclaimed. Different administrators are given different permissions and assigned different management scopes to implement rights- and domain-based management.

- Cloud platform rights- and domain-based management

  Operation permissions of administrators are precisely controlled. Operation permissions of the super administrator are reclaimed. Different administrators are given different permissions to implement rights-based management.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.7.8 Management System Certificate Authentication

Version Requirements

The Management System Certificate Authentication feature has been available since version 5.0.

Summary

The certificate authentication mechanism is used between OSs of management components, and communication between management components is encrypted by using certificates, ensuring authentication and communication security for the desktop cloud management system.

Feature Description

To ensure secure communication between desktop cloud components (including the WI, HDC, License, and ITA), before communication starts, two-way SSL-based Hypertext Transfer Protocol Secure (HTTPS) certificate authentication is implemented for each component, and an encrypted transmission channel is created between components. After each component is installed during FusionAccess deployment, each component comes with a certificate by default. This certificate is used for server and client certificate authentication.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.7.9 Management System Certificate One-click Replacement

Version Requirements

The Management System Certificate One-click Replacement feature has been available since version 5.0.

The V1 and V3 certificates can be created since version 6.2.

Summary

Security certificates can be automatically generated by using a tool, and certificates of all management components can be replaced in one-click mode.

Feature Description

If customers want to replace certificates of management components, they can use their own Certificate Authority (CA) system to issue certificates that can be used for client and server authentication, and manually replace component certificates by following the steps provided in the maintenance guide. Alternatively, they can use the certificate replacement tool provided by FusionAccess to generate new certificates which automatically substitute for original certificates.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.7.10 User Data Security

Version Requirements

The User Data Security feature has been available since version 5.0.

Summary

When a VM is deleted, all user data is deleted to prevent data theft or malicious use.

Feature Description

The User Data Security feature, also called VM disk data clearing, is provided to clear disk data of a VM during VM deletion before the disk space (logical volume) is assigned to another user, so that the new user cannot restore sensitive or important data of the original user. This prevents user data leakage.

This feature is developed to address security issues on disk space reuse in the cloud scenario. It complies with the 5220.22-M standard of United States Department of Defense (DoD), and is implemented based on the Clear level (that is, overwrite each bit with 0). It prevents original disk data from being restored using software. Therefore, if a physical disk in the data center is going to be scrapped, it is recommended that the disk be processed using a professional data destroy tool, degaussed, or physically destroyed.

To completely delete data from IP SAN-based big logical unit number (LUN) block storage or local disk block storage of servers, all volume space is overwritten with 0.

To completely delete data from FusionStorage and virtualized storage, the topmost 10 MB data instead of all data in the volume is overwritten with 0. This ensures that the original user data cannot be restored from the VM after it is allocated to another user.

NOTE

VMs that are safely deleted cannot be provisioned when the VRM (KVM) platform is used.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.7.11 System Data Security

Version Requirements

The System Data Security feature has been available since version 5.0.

Summary

Passwords and keys are encrypted and stored. The transmission of sensitive data (such as domain passwords) is encrypted.

Feature Description

Sensitive data is determined based on application scenarios of products. Sensitive data mainly refers to passwords, keys, and identity authentication information of users in the FusionAccess desktop system.

Passwords and keys stored in local files or databases must be encrypted. Non-reversible passwords are encrypted using SHA256, and reversible passwords are encrypted using AES256.

The following passwords are available:

- Password for logging in to the ITA portal
- Account for connecting the ITA to a database
- Account for connecting the ITA to an HDC database
- Domain administrator account
- Tomcat account
- Account for connecting the HDC to a database
- Account for connecting the WI to a database
- Account for connecting the license server to a database

Data transmission between FusionAccess Desktop infrastructure components is encrypted to ensure system data security. The following measures are taken:

- When the Huawei Desktop Agent (HDA) obtains the password of a domain account from the HDC, the password is encrypted for transmission.
- HTTPS-based transmission of the domain account password between the TC and the WI is encrypted.
- Transmission of sensitive data (such as passwords) between the WI and the HDC is encrypted.
- Plain text passwords are encrypted before they are stored in the HDC memory. The plain text passwords are used for obtaining usernames and passwords by login tickets.
- The AD domain authentication is implemented for users to log in to the FusionAccess desktop system by entering passwords. The AD domain authentication is implemented for users to log in to desktop management components.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.7.12 Secure Internet Access Desktop

Version Requirements

The Secure Internet Access Desktop feature has been available since version 5.3.

Summary

In secure OA scenarios, virtual desktops are isolated from local clients. Data files can be transmitted only from virtual desktops to clients but not allowed to be transmitted from clients to virtual desktops.

Feature Description

If users need to access the Internet, they can log in to the Internet access desktops (full memory desktops and SBC sharing desktops) from SCs. The Internet access desktops have permission to access the Internet. Users can query information and download data on the Internet access desktops.

The administrator delivers the same policies to all users. The policies specify that when users log in to the Internet access desktops from terminals (such as PCs, laptops, and VMs), users are not allowed to transmit terminal data to the Internet access desktops, which prevents information security risks. The Huawei FusionAccess Desktop system adopts HDP to transmit files from virtual desktops to local terminals. The administrator configures the same policies for all users to allow users to transmit files downloaded on the Internet access desktops to local terminals.

After Internet access desktops are disconnected, Internet access desktops are restarted based on power management policies, clear temporary user information, and restore to the initial state, which prevents intrusion of phishing websites through Trojan horses.

Application Scenario

Windows Virtual Desktop
●

1.7.13 Management System Ukey Login Authentication

Version Requirements

The Management System Ukey Login Authentication feature has been available since version 6.0.

Summary

Administrators can use Ukey for identity authentication when they log in to ITA Portal.

Feature Description

1. Ukey Login function for administrators should be interconnected with digital certificate identity authentication system of the third-party security vender. At present, interconnection with Koal identity authentication system has been completed.

2. If interconnection with other security venders is required, these security venders should adapt to the interfaces provided by Huawei.

Application Scenario

Windows Virtual Desktop
●

1.7.14 Desktop Watermark

Version Requirements

The Desktop Watermark feature has been available since version 6.0.

The color can be adjusted by entering RGB values in version 6.1.

The number of watermarks at fixed positions can be set in version 6.2.

Summary

On the desktop cloud, the administrator can configure the desktop watermark function to prevent users from photographing the virtual desktop.

Feature Description

On the desktop cloud, the administrator can configure the desktop watermark function to prevent users from photographing the virtual desktop.

Watermark Display supports two modes: fixed position and dynamic position:

- Fixed position mode: A single watermark is displayed in diagonal position from bottom left to top right.
- Dynamic position mode: A single watermark is displayed in horizontal position, which changes every 2 seconds on the screen randomly.

The watermark content supports custom text content, displaying **Login Username + Date** by default with max length of 64 bytes.

The color can be adjusted by entering RGB values in version 6.1.

The opacity of the watermark can be set.

Users can set a maximum of seven watermarks at fixed locations.

Application Scenario

Windows Virtual Desktop
●

1.8 Client Resource Redirection

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

The Client Resource Redirection feature allows desktop cloud users to use peripherals connecting to the peripheral ports of clients on VMs, and administrators to control device redirection based on policies. In this way, users can flexibly use client resources on VMs, and administrators can control peripherals for security purpose.

After tests in R&D labs, proof of concept (POC) tests, and verification in project delivery, a peripheral and software compatibility list for the Huawei FusionAccess Desktop Solution has been published and will be regularly updated at http://3ms.huawei.com.

Compatibility tests are required for the peripheral or software that is not covered in the compatibility list.

Benefits

This feature helps enterprises and users to access diversified peripherals and control local resources on virtual desktops, enhancing the network security and flexibility.

1.8.1 QoS Policies

Version Requirements

The QoS Policies feature has been available since version 5.1.

The display and video quality can be automatically adjusted when the QoS reaches the threshold in version 6.1.

Summary

The desktop transmission process can be controlled based on the QoS policies. Users can set policies to enhance user experience and control resource consumption.

Feature Description

Two solutions are available. One is enhanced user experience and the other is resource consumption control.

User experience enhancement is achieved by multi-stream policies, media redirection, and adaptive display and video quality.

Resource consumption control is achieved by bandwidth control.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.8.2 USB Port Redirection

Version Requirements

The USB Port Redirection feature has been available since version 5.0.

USB 3.0 ports, file transfer tool and SBC scenario have been available since version 6.0.

Summary

The USB Port Redirection feature allows the USB ports on a client to be associated with a virtual desktop. This allows users to connect to USB devices from the virtual desktop.

Feature Description

The USB Port Redirection feature allows the virtual desktop to connect to client USB devices through HDP.

USB Peripheral Bus Redirection

The USB protocol bus data packets are forwarded, so that the USB devices (USB2.0) connected to the USB ports of a client can be detected by the virtual desktop. USB devices

include the USB flash drive, USB hard disks, USB key, external USB CD-ROM drive, USB camera, USB printer, and USB scanner (excluding the USB keyboard and mouse). USB devices must comply with protocols of USB 2.0 or earlier and can be used on PCs. For details about USB types and models, see the USB device compatibility list.

USB Redirection Policy Management

Flexible policy control can be implemented for the USB redirection function to control the redirection of USB devices or grant users only the read permission on USB devices.

The system administrator configures policies on the management system for the server and saves the configuration in the database. When a user logs in to a VM, the management system delivers the configuration to the VM. Then the USB redirection module reads the configuration data, notifies the client, parses the data, and applies the configuration. The configuration delivery mode and dimension are specified by the administrator on the management system.

USB redirection policies of servers

Option	Value	Default Value
USB Redirection Enable	Yes/No	No
Image Device Redirection Enable	Yes/No	Yes
Video Device Redirection Enable	Yes/No	Yes
USB Printer Redirection Enable	Yes/No	Yes
USB Storage Device Redirection Enable	Yes/No	No
Other USB Device Redirection Enable	Yes/No	No
Customized USB Policies	N/A	N/A

Servers support policy control for user-defined devices. User-defined devices refer to devices with a user-defined ID or type. If USB devices that are not listed in 0 or USB devices of a specific model need to be controlled, users need to define the control policies by themselves.

Users can click a button on the toolbar on the client browser to display a popup window (provided by Windows and Linux clients) and configure policies in the window. In the popup window, all USB devices connected to the client are displayed, and users can disconnect and connect each device in the window.

This feature supports the following client OSs.

Application Scenario	Supported OS
VM OS	Windows XP 32-bit Windows7 32-bit/64-bit Windows10 32-bit/64-bit
TC OS	CT3000 and CT5000 (WES7 32-bit or Linux) CT6000 (WES7 32-bit or Linux) Sunniwell S-Box8V40

SC OS	Windows XP 32-bit Windows7 32-bit/64-bit Windows10 32-bit/64-bit

- For the compatible USB devices, see the USB device compatibility list. Compatibility of USB devices that are not listed in the compatibility list is not ensured. The compatibility list has been put on http://w3.huawei.com. The compatibility list will be updated when necessary.
  - USB devices must comply with the USB2.0 protocol. USB3.0 devices support USB devices on USB3.0 port mapping to VMs. By default, Microsoft and other given USB3.0 drivers are supported. Third-party USB 3.0 drivers may be configured manually for Windows clients.
  - A built-in file transfer tool is provided in desktop agent. By using it, secure high-speed transmission between a client and a VM can be achieved through a file transfer channel dedicated to HDP protocol.
  - USB port mapping on SBC scenario is added.
- Visit http://support.huawei.com/onlinetool/datums/fusioncloud/comptool/index.jsp to obtain the Huawei FusionAccess Desktop software and peripheral compatibility lists.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.8.3 Camera Redirection

Version Requirements

The Camera Redirection feature has been available since version 5.1.

The SBC scenario has been available since version 6.0.

Cameras in VMs are supported in version 6.1.

Summary

The Camera Redirection feature allows USB cameras to be redirected to servers with compressed videos.

Feature Description

Cameras that can be locally detected can be redirected to servers through the compression channel. Compared with direct camera redirection through buses, compressed videos occupy less bandwidth. The compression channel supports only cameras for which the driver does not need to be installed or has been installed on the client.

In the USB camera compression scenario, clients must support cameras free of drivers (a universal driver is used), or dedicated drivers for cameras are installed on TCs.

The camera mapping is supported in SBC scenario. Third-party camera software on the server must support virtual cameras with DirectShow interfaces.

Only the CT6100/ST6110 Windows TC supports the function of opening two cameras at the same time.

Visit http://support.huawei.com/onlinetool/datums/fusioncloud/comptool/index.jsp to obtain the Huawei FusionAccess Desktop software and peripheral compatibility lists.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.8.4 COM Port Redirection

Version Requirements

The COM Port Redirection feature has been available since version 5.1.

Summary

The COM ports on a client can be associated with a virtual desktop. This allows users to connect to COM devices from the virtual desktop.

Feature Description

The COM ports on a client can be associated with a virtual desktop. This allows users to connect to COM devices from the virtual desktop. COM port redirection can be controlled by a switch. The function of automatically connecting to COM devices can be set.

Visit http://support.huawei.com/onlinetool/datums/fusioncloud/comptool/index.jsp to obtain the Huawei FusionAccess Desktop software and peripheral compatibility lists.

Application Scenario

Windows Virtual Desktop
●

1.8.5 Parallel Port Redirection

Version Requirements

The Parallel Port Redirection feature has been available since version 5.3.

Summary

The parallel ports on a client can be associated with a virtual desktop. This allows users to connect to parallel port devices from virtual desktops.

Feature Description

The parallel ports on a client can be associated with a virtual desktop. This allows users to connect to parallel port devices from virtual desktops. Only Windows clients support this feature.

Visit http://support.huawei.com/onlinetool/datums/fusioncloud/comptool/index.jsp to obtain the Huawei FusionAccess Desktop software and peripheral compatibility lists.

Application Scenario

Windows Virtual Desktop
●

1.8.6 Drive or File Redirection

Version Requirements

The Drive or File Redirection feature has been available since version 5.1.

Linux TCs and Mac OS terminals and SBC are supported in version 5.3.

Summary

Drives installed on a client can be associated with a virtual desktop. This allows users to use drives from the virtual desktop. Read-only redirection is supported.

Feature Description

Drives installed on a client can be associated with a virtual desktop. This allows users to use drives from the virtual desktop. Read-only redirection is supported.

In the OA scenario, users can use local drives installed on a client, DVD-ROM drives, removable drives, and network drives on VMs. Users can access directories and files of drives.

This feature uses a data transmission channel that is at a lower level than that of channels used for transmitting display, keyboard, and mouse data. This feature provides good user experience when users access files of redirected drives.

Application Scenario	Supported OS
VM OS	Windows XP 32-bit Windows7 32-bit/64-bit Windows 8.1 32-bit/64-bit Windows Server 2008 R2 Windows 10 32-bit/64-bit Windows Server 2016
TC OS	CT3200 (Linux) CT5100/CT5110 (Linux, Windows) CT6100/CT6110 (Linux, Windows)
SC OS	Windows XP 32-bit Windows 7 32-bit/64-bit Windows 8.1 32-bit/64-bit Windows 10 32-bit/64-bit Mac OS 10.9 and later

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.8.7 Printer Redirection

Version Requirements

The Printer Redirection feature has been available since version 5.1.

SBC has been available since version 5.3.

In version 6.0:

1. x86 Linux clients have been available, and local printer mapping is supported.

2. A position-based network printing is supported. Administrators can configure the nearest network printer from their offices as default printers.

3. Printer redirection data compression is supported.

4. A local default printer can be automatically mapped as a default printer of a VM.

Summary

The printers connected to a client can be associated with a virtual desktop. This allows users to use printers from the virtual desktop and set papers, colors, and single and dual sides for printing.

Feature Description

After users log in to virtual desktops from clients, they can use the printers that are connected to clients on virtual desktops. This is similar to that client printers are mapped to virtual desktops.

A position-based network printing is supported. Neighboring network printers can be dynamically matched and added according to policy conditions.

Printer redirection data compression is supported.

A local default printer can be automatically mapped as a default printer of a VM. This feature supports the following client OSs.

Application Scenario	Supported OS
VM OS	Windows XP 32-bit, Windows 7 32-bit/64-bit, Windows 8.1 32-bit/64-bit, Windows Server 2008 R2, Windows10 32-bit/64-bit, and Windows Server 2016
TC OS	CT3200 (Linux) CT5100/CT5110 (Linux, Windows) CT6100/CT6110 (Linux, Windows)
SC OS	Windows XP 32-bit Windows 7 32-bit/64-bit Windows 8.1 32-bit/64-bit Windows 10 32-bit/64-bit

Compatibility of the following printers is tested. Perform a compatibility test for other printers to check whether the printers can be used on virtual desktops.

Terminal Type	Compatible Printer
Windows TC	Printers of the PCL or ESC RAW format
Windows SC	Printers of the PCL or ESC RAW format

Windows TCs support USB and parallel port printers. For information about supported printer models, visit http://support.huawei.com/onlinetool/datums/fusioncloud/comptool/index.jsp to see the peripheral compatibility list.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.8.8 TWAIN Redirection

Version Requirements

The TWAIN Redirection feature has been available since version 5.1.

Summary

The TWAIN Redirection feature allows TWAIN devices connected to a client to be associated with a virtual desktop. This allows users to use TWAIN devices from virtual desktops. The compression level can be controlled on the virtual desktop.

Feature Description

TWAIN is an open protocol that regulates devices such as scanners, digital cameras, and digital audio and image databases. TWAIN-based software applications can directly obtain data from TWAIN-based devices.

The FusionAccess Desktop Solution 5.1 supports direct mapping of TWAIN devices to virtual desktops.

Four lossless compression levels are supported: none, low, medium, and high. This setting saves bandwidth.

This feature supports the following client OSs.

Table 1-1 Supported client OSs

Application Scenario	Supported OS
VM OS	Windows XP 32-bit, Windows 7 32-bit/64-bit, Windows 8.1 32-bit/64-bit, Windows Server 2008 R2, Windows 10 32-bit/64-bit, Windows Server 2016
TC OS	CT3200 (Linux) CT5100/CT5110 (Linux, Windows) CT6100/CT6110 (Linux, Windows)
SC OS	Windows XP 32-bit Windows7 32-bit Windows 10 32-bit/64-bit

To use this feature, TWAIN device drivers must be installed on Windows TCs/SCs. Few TWAIN drivers are available for Linux OSs, so you can install the Huawei TWAIN universal

driver on Linux TCs to support driver-free cameras, such as the Liangtian high-speed document scanner. Refer to the POC test results for the compatibility of the driver.

Visit http://support.huawei.com/onlinetool/datums/fusioncloud/comptool/index.jsp to obtain the Huawei FusionAccess Desktop software and peripheral compatibility lists.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.8.9 Clipboard Redirection

Version Requirements

The Clipboard Redirection feature has been available since version 5.1.

Linux TCs and Mac OS clients are supported in version 5.3.

SBC is supported in version 5.3.

Summary

Clipboard redirection allows the clipboard on a client to be associated with a virtual desktop. This allows data to be transferred between a client and a virtual desktop by using the clipboard.

Feature Description

Clipboard redirection allows the clipboard on a client to be associated with a virtual desktop. This allows data to be transferred between a client and a virtual desktop by using the clipboard.

The Windows client supports clipboard redirection of TEXT, BITMAP, RICH TEXT, METAFILEPICT, and BIFF8 files (the file redirection switch must be opened), as well as bi-directional clipboard control, or unilateral control from TC to VM or from VM to TC.

Bidirectional file copy between a client and a virtual desktop is supported. Unidirectional file copy from a client to a virtual desktop or from a virtual desktop to a client can be implemented by policies. TEXT, UNICODETEXT, METAFILEPICT, DIB, BITMAP, and BIFF8 files can be copied between a client and a virtual desktop. In Linux and Mac OS client, only the plain text format is supported. Special formats, such as the image and file formats are not supported. Rick texts are converted to plain texts. File clipboard redirection is not supported. For plain texts, bi-directional clipboard control, or unilateral control from TC to VM or from VM to TC is supported.

Application Scenario	Supported OS
VM OS	Windows XP 32-bit Windows 7 32-bit/64-bit Windows 8.1 32-bit/64-bit Windows Server 2008 R2 Windows 10 32-bit/64-bit Windows Server 2016
TC OS	CT3200 (Linux) CT5100/CT5110 (Linux, Windows) CT6100/CT6110 (Linux, Windows)
SC OS	Windows XP 32-bit Windows 7 32-bit/64-bit Windows 8.1 32-bit/64-bit Windows 10 32-bit/64-bit Mac OS 10.9 and later

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.8.10 Shadowing Redirection

Version Requirements

The Shadowing Redirection feature has been available since version 5.1.

Summary

The Shadowing Redirection feature allows administrators to remotely connect to user VMs and solve problems on user VMs. The user and administrator connect to the same VM and operate the VM together.

Feature Description

After the remote assistance function of the Windows OS is enabled, administrators can remotely control users' virtual desktops to rectify faults for users.

Application Scenario

Windows Virtual Desktop
●

1.8.11 Monitor Redirection

Version Requirements

The Monitor Redirection feature has been available since version 5.1.

SBC has been available since version 5.3.

Summary

The HDP can be used to deliver the OS GUI of VMs to the monitors connected to terminals and supports multi-screen display.

Feature Description

Administrators can specify whether virtual desktops support multi-screen display on ITA. Users can specify whether to support multi-screen display using the client toolbar. Single-screen display is configured for ITA and clients by default. The multi-screen display function is enabled only when the multi-screen display function is configured on both ITA and clients.

Maximum resolution of 3840 x 2160 is supported for single-screen display.

A maximum of four monitors are supported.

The CT5100/ST5110 and CT6100/ST6110 supports dual-screen horizontally extended display. In the dual-screen display scenario, a single monitor supports a maximum resolution of 2560 x 1440. In the quad-screen scenario, a single monitor supports a maximum resolution of 1920 x 1200. The network bandwidth between terminals and VMs multiples based on the number of monitors.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.8.12 Smartcard Redirection (PC/SC)

Version Requirements

The Smartcard Redirection (PC/SC) feature has been available since version 5.1.

Summary

Smartcards connected to TCs can be mapped to virtual desktops.

Feature Description

The PC/SC standard is formulated by the PC/SC team formed by Microsoft and other famous smartcard manufacturers.

The PC/SC standard provides a standard user interface (API) based on the Windows platform and an environment for integrating PCs and smartcards.

To use this feature, smartcard drivers compliant with the PC/SC 1.0 standard need to be installed on TCs/SCs and VMs. Smartcard redirection through USB buses must be disabled.

This feature supports the following client OSs.

Application Scenario	Supported OS
VM OS	Windows XP 32-bit Windows 7 32-bit/64-bit Windows 8.1 32-bit/64-bit Windows Server 2008 R2 Windows 10 32-bit/64-bit Windows Server 2016
TC OS	CT3200 (Linux) CT5100/ST5110 (Linux, Windows) CT6100/ST6110 (Linux, Windows)
SC OS	Windows XP 32-bit Windows 7 32-bit/64-bit Windows 8.1 32-bit/64-bit Windows 10 32-bit/64-bit

Theoretically, smartcards in compliant with the PC/SC 1.0 standard are supported. Perform a compatibility test to verify the compatibility of specific devices. If Linux TCs are used, ensure that smartcards carry Linux drivers that support the PC/SC protocol. Compatibility of smartcards in the following table has been verified.

Terminal Type	Compatible Smartcard
Windows TC	SafeNet eToken PRO 72k New ePass3000 (Huawei customized version)
Windows SC	SafeNet eToken PRO 72k New ePass3000 (Huawei customized version)
Linux TC	SafeNet eToken PRO 72k

Application Scenario

Windows Virtual Desktop
●

1.8.13 HID Redirection

Version Requirements

The HID Redirection feature has been available since version 5.3.

Summary

Human interface device (HID) redirection is supported.

Feature Description

HID devices directly interact with humans, such as the keyboard, mouse, joysticks, and ID card readers. HID devices may not provide a man-machine interface. Devices that comply with HID specifications can be considered as HID devices. Only Windows TCs and SCs support HID redirection.

Application Scenario

Windows Virtual Desktop
●

1.8.14 Unified Printing

Version Requirements

The Unified Printing feature has been available since version 6.0.

Summary

Desktop Cloud integrates a third-party network printing solution and provides desktop VM unified printing function, so that clients and desktop user VMs are not required to install drivers.

Feature Description

Desktop Cloud integrates a third-party network printing solution and provides the unified printing function of desktop VMs, so that driver installation is not required by clients and desktop user VMs.

The network printing software that has obtained Huawei ready authentication includes UniPrint.

Application Scenario

Windows Virtual Desktop
●

1.9 Multimedia Support

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

The FusionAccess desktop system supports 480p, 720p, and 1080p video and high-quality audio. Users can have enjoyable audio and video experience in the Huawei FusionAccess desktop system. Compared with the common office automation (OA) feature, the Multimedia Support feature has higher requirements for CPUs, memory resources, and network bandwidth of VMs and clients.

Benefits

This feature provides users with smooth video and audio playing experience over the FusionAccess desktop system.

1.9.1 Image Display GDI

Version Requirements

The Image Display GDI feature has been available since version 5.0.

SBC has been available since version 5.3.

Users can manually set the resolution of a VM in version 6.2.

Summary

The FusionAccess desktop system supports highly efficient image encoding and decoding. Lossless compression is used for non-natural images, repeated image data is not transmitted, and the display frame rate is auto-adaptive. These technologies are used to smoothly display high-definition images with less bandwidth.

Feature Description

The Graphics Device Interface (GDI) is an important part of the Windows Application Programming Interface (API).

When a user logs in to a virtual desktop, the system automatically starts the HDP client, sets up a display transmission channel, and enables the display redirection service. The entire virtual desktop in 32-bit true color is transmitted to the client through HDP.

The HDP protocol adopts highly efficient image encoding and decoding technologies to provide high-definition, smooth images for virtual desktop users with less bandwidth.

According to the image effect tested in the Huawei library, HDP can provide better display effect for characters and characters plus images than protocols used by other vendors. The peak signal to noise ratio (PSNR) shows that HDP can provide near-lossless display effect.

PSNR is an objective method for evaluating image quality. PSNR is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Usually, compressed images will change a little from original images. PSNR is used to measure the image quality provided by an image processing program. PSNR is the logarithmic value of the mean squared error (MSE) between the original and compressed images relative to (2^n-1)^2 (the square of the maximum signal value, and *n* indicates the number of bits of a sample value). PSNR is in the unit of dB.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.9.2 Virtual Desktop Display Policies

Version Requirements

The Virtual Desktop Display Policies feature has been available since version 5.1.

SBC has been available since version 5.3.

Summary

Various desktop display policies can be set to meet desktop display requirements in different scenarios and provide high user experience of virtual desktops.

Feature Description

Virtual desktop display is key experience for using virtual desktops. The Huawei FusionAccess Desktop Solution supports various desktop display policies to ensure high user experience in different scenarios.

Display policy grade

Grade 1: This grade provides poorest display quality but requires lowest bandwidth, and therefore is applicable to a network with a bandwidth of lower than 1 Mbit/s.

Grade 2: This grade provides poorer display quality but requires lower bandwidth, and therefore is applicable to a network with a bandwidth ranging from 1 Mbit/s to 2 Mbit/s.

Grade 3: This grade provides poorer display quality but requires lower bandwidth, and therefore is applicable to a network with a bandwidth ranging from 2 Mbit/s to 5 Mbit/s.

Grade 4 (recommended): This grade balances display quality and bandwidth requirements, and is applicable to a network with a bandwidth of 20 Mbit/s.

Grade 5: This grade provides best display quality but requires highest bandwidth, and therefore is applicable to a network with a bandwidth of 25 Mbit/s or higher.

Graphics card cache (MB): indicates the device cache capacity. The value ranges from 0 to 64. This policy affects the bandwidth in some scenarios. The higher the value, the lower the bandwidth.

Bandwidth (kbit/s): limits the peak bandwidth of a user. The value ranges from 32 to 25000.

Frame rate (fps): specifies the desktop image update frequency in common OA scenarios. The value ranges from 1 to 60. The higher the frame rate, the smoother the desktop operations, but the higher the requirements on bandwidth and TC configuration. Recommended value: 15 fps to 25 fps.

Video frame rate (fps): The value ranges from 1 to 60. The higher the frame rate, the smoother the video playback, but the higher the requirements on bandwidth and TC configuration. Recommended value: 25 fps to 30 fps.

Advanced settings, such as the video bandwidth and image compression mode, can also be configured.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.9.3 Video Support

Version Requirements

The Video Support feature has been available since version 5.0.

SBC has been available since version 5.3.

Summary

The FusionAccess desktop system supports standard-definition (480p) and high-definition (720p/1080p) videos of common formats.

Feature Description

In the FusionAccess desktop system, videos can be played and viewed in server rendering mode. The FusionAccess desktop system supports standard-definition (480p) and high-definition (720p/1080p) videos of common formats. The number of concurrently played videos is determined by server capabilities and video quality.

Server decoding

- 1080p videos are supported, and 5 Mbit/s to 15 Mbit/s bandwidth is provided for a single user. A computing server (two 2640 CPUs) supports a maximum of seven concurrent users in the case of 1080p videos. High requirements are put on VMs. VMs must run on the Windows 7 OS and are configured with four CPUs and 4 GB memory capacity.
- 720p videos are supported, and 5 Mbit/s to 15 Mbit/s bandwidth is provided for a single user. A computing server (two 2640 CPUs) supports a maximum of 14 concurrent users in the case of 720p videos. VMs run on the Windows 7 OS and are configured with two CPUs and 2 GB memory capacity.

- 480p videos are supported, and 3 Mbit/s to 8 Mbit/s bandwidth is provided for a single user. A computing server (two 2640 CPUs) supports a maximum of 28 concurrent users in the case of 480p videos. VMs run on the Windows 7 OS and are configured with two CPUs and 2 GB memory capacity.

Client decoding

The Client decoding supports the video resolution of 1080p in full screen. File formats and TCs have specific requirements. For details, see the description about the multimedia redirection feature.

If the number of concurrent users exceeds the preceding specifications, screen freezing may occur due to CPU resource preemption and IOPS storms.

Video playing quality is related to VM configuration of servers, TCs, network conditions, video quality, and players. The number of virtual desktops that play videos concurrently supported by servers of other types is determined by the SPEC value of servers. Determine system configuration based on application scenarios.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.9.4 Audio Support

Version Requirements

The Audio Support feature has been available since version 5.0.

SBC has been available since version 5.3.

Summary

With the audio redirection function, the audio data of VMs can be transmitted to clients for playing, and the audio data of clients can be transmitted to VMs.

Users can play music and have VoIP calls on VMs.

Feature Description

Administrators can modify audio redirection policies. Administrators configure policies for servers on the management system and deliver the configuration to a VM. The configuration takes effect when a user reconnects to the VM.

Virtual desktops support stereo mixing, that is, mixing of input and output sounds of a VM. When the stereo mixing function is enabled, the volume of mixed sound can be adjusted by dragging a slider on the stereo mixing interface.

Table 1-2 lists some audio redirection polices of servers.

Table 1-2 Audio redirection polices of servers

Option	Value	Default Value
Audio Redirection Enabled or Not	Yes/No	Yes
Play Volume	Do Not Set Volume 10 to 100, set by a step of 5	Do Not Set Volume
Play Volume Ratio	Do Not Set Volume Ratio Low Medium High	Do Not Set Volume Ratio
Record Volume	Do Not Set Volume 10 to 100, set by a step of 5	100
Record Volume Ratio	Do Not Set Volume Ratio Low Medium High	Do Not Set Volume Ratio

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.9.5 Audio Scenario Automatic Detection

Version Requirements

The Audio Scenario Automatic Detection feature has been available since version 5.0.

Summary

The audio encoding and decoding algorithms are selected based on scenarios to provide best user experience in a specific scenario.

Feature Description

Encoding and decoding algorithms are selected based on scenarios. In the broadcasting scenario, the algorithm is used, and buffer is expanded. In the voice call scenario, the other algorithm is used, and latency is shortened.

Encoding and decoding algorithms are switched in auto-adaptive mode to provide best user experience in a specific scenario.

Application Scenario

Windows Virtual Desktop
●

1.9.6 Multimedia Redirection

Version Requirements

The Multimedia Redirection feature has been available since version 5.0.

Video redirection with video accelerator is supported in version 6.1.

In version 6.2, the Huawei video accelerator supports display ratio adjustment based on the original view ratio, improving the usability of file association.

Summary

In the FusionAccess desktop system, videos can be played and viewed in multimedia redirection mode. The FusionAccess desktop system supports standard-definition (480p) and high-definition (720p/1080p) videos of AVI, WMV, MPG, and MP4 formats.

Feature Description

Common video redirection:

The cloud video acceleration function is used to fragment the source video file and download the fragments to the clients. Then the video file is locally decoded and played on the clients. MediaPlayer player redirection and redirection using the Huawei video accelerator are supported.1. MediaPlayer player: Supports 1080p full-screen playback. The file format can be only AVI, MP4, WMV, and MPG. TCs support only CT5100/CT6100 (Windows).

2. Huawei video accelerator: TCs that support full-screen 4K video playback are supported. PCs and TCs that support 4K hard decoding and 4K output are required. Centerm C51 and 90B0Z TCs are recommended. 1080p video playback require CT5100/ST5110 (Windows) and CT6100/ST6110 (Windows). 720p/480p video playback require CT5100/ST5110 (Windows and Linux), CT6100/ST6110 (Windows and Linux. Video files in MP4, FLY, WMV, MKV, AVI, RMVB, and MOV format are supported) and CT3200 (only MP4 and FLV video files in H.264 encoding format are supported).

Application Scenario

Windows Virtual Desktop
●

1.9.7 Flash Redirection

Version Requirements

The Flash Redirection feature has been optimized in version 5.1.

Summary

In the desktop cloud, flash videos can be played and viewed in flash redirection mode, improving multimedia experience.

Feature Description

A flash video source file is fragmented, downloaded to a client, and decoded on the client for playback.

Servers in proxy or non-proxy mode are supported.

The FusionAccess management system allows users to specify whether to enable flash redirection, whether to enable server proxy, the minimum width and height (picture elements) of flash, and the list of video websites that support redirection.

Constraints:

- Client requirements
  - Only CT6100/ST6110 Windows TCs and Windows 7 32-bit SCs are supported.
  - A flash player plug-in (Adobe Flash Player Plug-in) must be installed on clients, and the plug-in version must be 10.1 or later.
- VM requirements
  - VM OSs must be Windows 7 (32-bit/64-bit) or Windows XP 32-bit.
  - An Adobe Flash Player ActiveX plug-in is installed on VMs, and the plug-in version must be 10.1 or later.
  - Internet Explorer 8, Internet Explorer 9, or Internet Explorer 10 is installed on VMs.

Application Scenario

Windows Virtual Desktop
●

1.9.8 4K Resolution

Version Requirements

The 4K Resolution feature has been available since version 6.0.

Summary

The 4K resolution (3840x2160) display is supported.

Users can play local 4K video in user VMs through Huawei video accelerator.

Feature Description

The 4K resolution (3840x2160) display is supported.

Users can play local 4K video in user VMs through Huawei video accelerator, which needs to be configured on a high-performance terminal.

Specifications are as follows:

1. Supporting 4K (3840x2160) resolution, and requiring a 4K resolution display and a TC (Centerm C51 and STAR 90B0Z are recommended.)

2. Only Windows 7 and Windows 10 32-bit and 64-bit OS are supported at present.

3. For 4k video playback, only 3840x2160 resolution video is supported for local playback when using the video accelerator provided by Huawei, and network 4K video playback is not supported.

4. PCs or TC terminals (Centerm C51 and STAR 90B0Z are recommended) that support 4K hardware decoding are required. The minimum configuration of a terminal that ensures user experience is as follows:

GPU model: Intel(R) HD Graphics 5500 (Intel CPU with built-in integrated graphics card)

CPU model: i3-5010U 2.1 GHz

Memory size: 8 GB

5. 8 U 8 GB is recommended for VMs. When using 4K HD video playback, bandwidth depends on 4K video bit rate. Available bandwidth between a VM and a terminal (TC) is not less than 100 MB.

Application Scenario

Windows Virtual Desktop
●

1.9.9 Duplicate Display

Version Requirements

The Duplicate Display feature has been available since version 6.2.

Summary

The screen of a VM can be displayed on the client of another VM through the desktop cloud client. The common application scenario of this function is the smart city command center, which delivers the display screen of employees on the working island to the command big screen.

Feature Description

Specifications are as follows:

1. Clients support only Windows OSs.

2. The source and destination TCs of duplicate screen must have the same model.

3. Only duplicate screen in VDI scenarios is supported. The SBC does not support this feature.

4. The single display supports a maximum resolution of 4K.

5. A maximum of two monitors are supported and only one monitor supports 4K resolution.

Application Scenario

Windows Virtual Desktop
●

1.10 Carrier-class VoIP

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●		●

Introduction

The green call center solution integrates the FusionAccess Desktop with the IP call center (IPCC). To ensure voice quality, the requirements on specifications, such as end-to-end latency, the packet loss rate, and jitter must be met. Therefore, Huawei has optimized the hardware, virtual platform, and application software of the desktop system. Interworking with the OpenEye provided by the Huawei IPCC solution, the FusionAccess desktop system provides carrier-class voice over IP (VoIP) experience.

The Huawei FusionAccess desktop system is compatible with mainstream IP-based call center software, such as CosmoCall Universe and Avaya.

Benefits

Provides a call center system based on virtual desktop clouds, which features high reliability, centralized maintenance, and pleasant workplaces.

1.10.1 TC-based SoftClient

Version Requirements

The TC-based SoftClient solution has been available since version 5.1.

Summary

This solution is oriented to the FusionAccess Desktop IPCC, and provides high-quality and low-latency communication services.

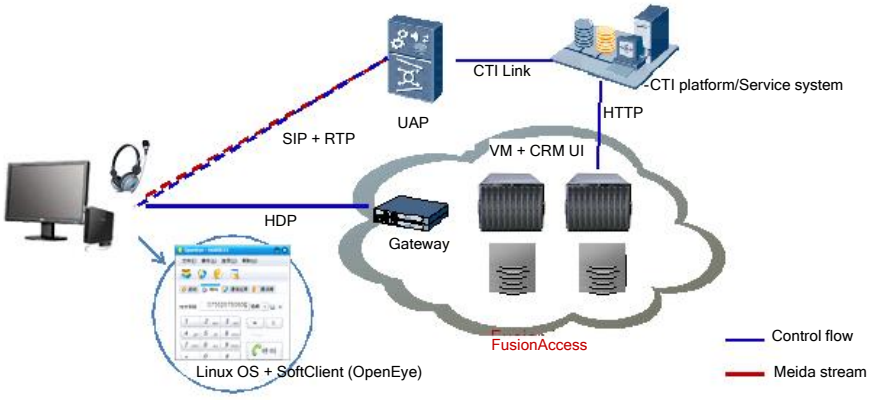
Feature Description

FusionAccess Desktop VMs provide agents in customer service centers with virtual desktops on which Windows and agent software are installed. Agent software includes Internet Explorer and Customer Relationship Management (CRM) add-ins. TCs where the OpenEye is

installed function as Session Initiation Protocol (SIP) user equipment (UE) to communicate with the universal access point (UAP) by using SIP and RTP. TCs connect to agent desktops and process keyboard, mouse, and display information by using HDP. This enables agents to remotely access their desktops and process services with consistent experience as if they were using local desktops.

Figure 1-1 shows the TC-based SoftClient solution.

Figure 1-1 TC-based SoftClient solution



Huawei OpenEye clients support Linux TCs. The TC-based SoftClient solution is preferred. This solution provides voice quality that meets general VoIP quality requirements. The perceptual evaluation of speech quality (PESQ) is greater than 3, and the one-way delay (OWD) is smaller than 400 ms.

Each agent uses about 400 kbit/s bandwidth. In this solution, voice SCs are deployed on TCs, voice transmission and call processing modes are the same as traditional modes, and the voice quality is high. In this solution, SCs are deployed on TCs, and agent software is deployed on VMs. Agents initiate or answer calls through the call center. Signaling and media streams are exchanged between the call center access platform and SCs.

If non-Huawei agent software is used, the TC of the WES 7 version and the TC-based SoftClient solution are used. Voice quality meets general VoIP quality requirements in theory. During project implementation, POC tests are required.

Visit http://support.huawei.com/support/ to learn matched OpenEye and TC versions from **Software Center** > **Version Software** > **Application and Software** > **Service and Software Public** > **OpenEye** > **OpenEye V300R001C60** > **OpenEye V300R001C60 Version Mapping**.

NOTE

This solution supports Huawei OpenEye VoIP client software. Scenarios supported by other voice client software need to be verified by tests.

Application Scenario

Windows Virtual Desktop
●

1.10.2 SoftClient-split Architecture

Version Requirements

The SoftClient-split Architecture feature has been available since version 5.1.

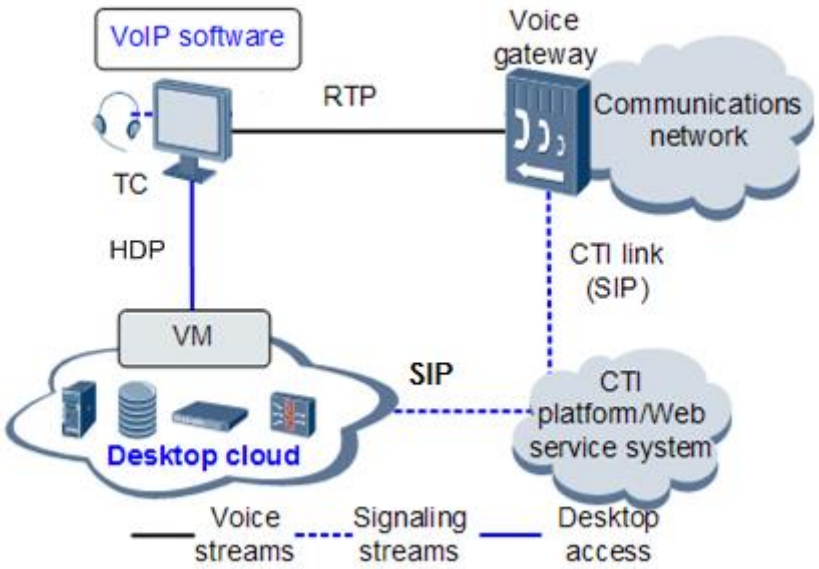
Summary

The SoftClient-split architecture based on OpenEye is provided. It is an optimized solution for the desktop cloud IP call centers (IPCCs) and features excellent voice quality and low latency.

Feature Description

The client software of the IPCC is divided into the control module and voice module. The voice module is installed on the TC, and the control module is installed on the VM, as shown in Figure 1-2.

Figure 1-2 SoftClient-split architecture solution



The flow of a VoIP call from a call center agent to a client is as follows:

Agent > TC > VoIP client software (OpenEye) > voice gateway and communications network > fixed-line or mobile phone > client

If the Huawei OpenEye is used and background service system versions match the OpenEye version, the SoftClient-split architecture solution is preferred to improve agent experience and voice quality. The perceptual evaluation of speech quality (PESQ) is greater than 3, and the OWD is smaller than 400 ms.

Voice transmission does not require second codec conversion from the VM to the TC. Therefore, the voice quality is ensured. Each agent uses about 200 kbit/s bandwidth.

Dedicated versions of Huawei OpenEye, TC software, and CSP software are provided for the SoftClient-split architecture solution.

Visit http://support.huawei.com/support/ to learn matched OpenEye and TC versions from **Software Center** > **Version Software** > **Application and Software** > **Service and Software Public** > **OpenEye** > **OpenEye V300R001C60** > **OpenEye V300R001C60 Version Mapping**.

NOTE

This solution supports Huawei OpenEye VoIP client software. Scenarios supported by other voice client software need to be verified by tests.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

1.10.3 VM-based SoftClient

Version Requirements

The VM-based SoftClient feature has been available since version 5.0.

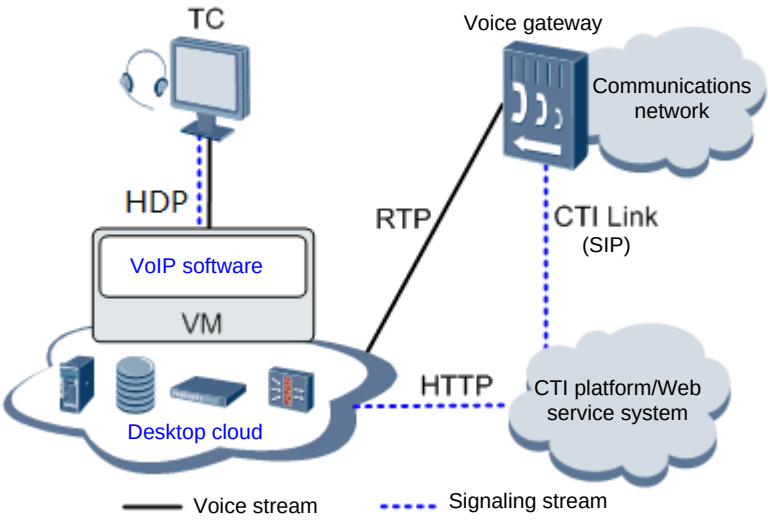
Summary

The VM-based SoftClient solution is a universal IP-based call center solution, and compatible with mainstream IP-based call center software. Compared with TC-based SoftClient and SoftClient-split Architecture solutions, the VM-based SoftClient solution provides long latency and cannot meet professional voice requirements. A POC test must be performed to determine its application scenarios, which is not recommended.

Feature Description

Install the VoIP software on the VM, as shown in Figure 1-3.

Figure 1-3 VM-based SoftClient solution



The flow of a VoIP call from a call center agent to a client is as follows:

Agent > TC >VM > VoIP client software > voice gateway and communication network > fixed-line or mobile phone > client

In the VM-based SoftClient solution, virtual desktops redirect voice signals using HDP, which increases complexity in signal transmission and processing. The voice transmission protocol and path differ from those in traditional mode. The voice quality is poor, and the delay is long. Since the bandwidth for redirecting voice signals over HDP is added, the access bandwidth of virtual desktops increases.

To improve voice quality, the virtual desktop access network on the TC side must meet the following requirements:

- Delay < 10 ms
- Jitter < 5 ms
- Packet loss rate < 0.1%

Since video codec is performed on VMs, the VMs must have high specifications.

If non-Huawei call center software is to be used, it is recommended that POC tests be performed to check whether the software is compatible with the Huawei FusionAccess Desktop Solution.

Compared with the SoftClient-split Architecture solution, the VM-based SoftClient solution provides long latency. Perform a POC test to check whether the VM-based SoftClient solution can be put in commercial use.

Application Scenario

Windows Virtual Desktop
●

1.10.4 Separation of Skype Audios and Videos

Version Requirements

The separation of Skype audios and videos has been available since version 6.1.

Summary

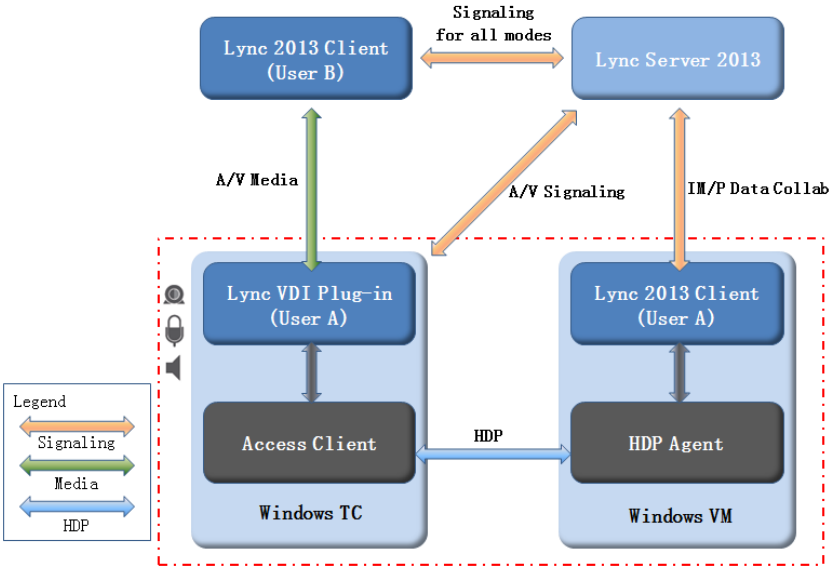
The function provides optimization support for deploying the Microsoft Skype for Business enterprise (called Lync before) communication application solution in VDI environment. It is based on the VDI Plug-in of Skype for Business and downloads audios and videos to TC/PC terminals for processing, thereby providing audio and video qualities and reducing VM pressures.

Feature Description

Principle of Skype audio and video separation: In VDI scenarios, Skype for business is divided into three parts: Server, Client, and VDI Plug-in. The Client is installed in the VM to

provide software operations. VDI Plug-in is installed in the TC/PC to provide audio and video decoding, as shown in the following figure.

Figure 1-4 Skype audio and video separation architecture



1. Supported servers include Lync Server 2013 and Skype for Business 2015 (Lync was changed to Skype for Business after Microsoft acquired Skype). You need to enable the EnableMediaRedirection function on the Server.

2. Skype software requirements:

(1) Servers support Lync Server 2013 and Skype for Business Server 2015.

(2) Clients support Lync 2013 and Skype for Business 2015.

Note: Lync 2013 is contained in Microsoft Office 2013 and Skype for Business 2015 is contained in Microsoft Office 2015. Microsoft Office 2016 is not supported (the VDI plug-in does not match with the Lync client).

3. Supported OSs: Windows 7 32-bit and 64-bit, Windows 10 32-bit and 64-bit, Windows 2008 R2 SP1 64-bit, and Windows 2012 R2 64-bit

4. Terminal requirements:

(1) Microsoft Lync VDI 2013 plugin (32-bit) must be installed on terminals.

(2) Only Windows TCs (WES7 SP1 32bit) are supported. Users need to customize 4 GB memory and 16 GB storage for CT5100 and CT6100. The ST5110/ST6110 (4 GB memory and 16 GB storage by default) is recommended.

(3) SC-based terminals running on Windows 7 SP1 32-bit and 64-bit, and Windows 10 32-bit and 64-bit are supported.

The following functions of Microsoft VDI Plug-in 2013 plug-in cannot be used in this version:

- Multi-party video conferencing
- SBC scenarios
- The Office 2013 of a PC must be 32-bit when a 32-bit VDI Plug-in 2013 is installed on the PC.

- For other restrictions, see the following website: https://support.office.com/en-us/article/FAQs-for-Lync-in-a-Virtual-Desktop-Infrastructure-VDI-environment-763ebe41-24ba-44fa-895b-8e76e00833d4#__toc336603640

Application Scenario

Windows Virtual Desktop
●

1.10.5 Audio and Video Bypass

Version Requirements

The audio and video bypass function has been available since version 6.1.

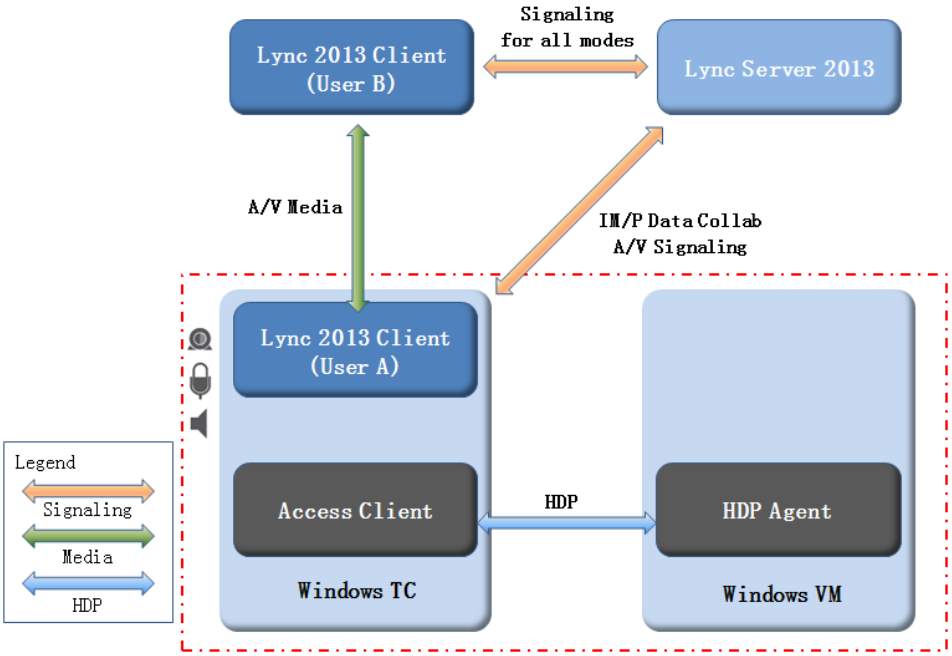
Summary

The function provides optimization support for deploying the communication application solution in VDI environment. Enterprise communication software is installed and enabled on a local TC/ PC to map the application operation page to a VM, thereby improving audio and video qualities without compromising user experience of enterprise communication software.

Feature Description

Principle of the audio and video bypass solution: When the enterprise communication software is installed and run on a TC/PC terminal, the HDP Client obtains the operation interface of the software and maps the interface to a VM through the HDP protocol. Therefore, from the perspective of end users, the software is running in the VM, thereby improving audio and video qualities without compromising user experience of enterprise communication software, as shown in the following figure.

Figure 1-5 Audio and video bypass solution architecture



1. Supported virtual desktop OSs include Windows 7 32-bit/64-bit and Windows10 32-bit/64-bit.

2. Only Windows terminals are supported. TC terminals only support WES7 SP1 32-bit. PC terminals only support Windows 7 SP1 32-bit/64-bit and Windows 10 32-bit/64-bit.

3. 4 GB memory and 16 GB storage must be configured for a TC terminal.

4. SBC scenarios are not supported.

5. The communication software can use only the input method of local TCs/PCs.

6. The communication software cannot directly access files on the virtual desktop.

Application Scenario

Windows Virtual Desktop
●

1.11 Mobile Office

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

Users can connect to background virtual applications or desktops over wireless networks (3G/4G network or Wi-Fi) to implement mobile office.

Benefits

With the rapid development of enterprise IT systems and updates of intelligent terminals, enterprises require employees to access software systems from mobile devices to handle services anytime and anywhere. The Mobile Office feature allows employees to work without restrictions of time and space

1.11.1 SBC Mobile Office

Version Requirements

The SBC Mobile Office feature has been available since version 5.1.

Summary

The SBC Mobile Office feature allows users to access application virtualization systems through a wireless network, such as Wi-Fi, 3G, and LTE.

Feature Description

Some traditional B/S and C/S service system software cannot run on iOS and Android mobile terminals, due to differences and restrictions of iOS and Android mobile terminals. The FusionAccess application virtualization platform access solution can solve the problem. For example, web applications compatible with Internet Explorer cannot be migrated to PADs. The compatibility problems between ActiveX, Flash, Internet Explorer, and PADs must be solved by delivering Internet Explorer kernels to PADs. Compatibility problems between Microsoft Office software and PADs must also be solved. Many enterprises have developed Office plug-ins and Office document encryption tools. These advanced Office functions are not supported by iOS and Android applications. In addition, PADs' performance cannot meet requirements of large-scale complex computing. These functions and applications can be implemented by application virtualization on servers.

iOS (8.0 or later) and Android (4.1.2 or later) mobile clients are supported.

FusionAccess can integrate with AnyOffice to publish clients through AnyOffice.

User experience of mobile office is related to wireless network quality. You are not advised to use the SBC Mobile Office feature when the wireless network is of poor quality.

Application Scenario

Application Virtualization
●

1.11.2 VDI Mobile Office

Version Requirements

The VDI Mobile Office feature has been available since version 5.1.

Summary

The feature allows users to access virtual desktops from mobile devices through a wireless network, such as WiFi, 3G, and LTE.

Feature Description

Some traditional B/S and C/S service system software cannot run on mobile terminals, due to differences and restrictions of mobile devices' OSs. The FusionAccess mobile virtual desktop access solution can solve the problem.

Mobile terminals' performance cannot meet requirements of large-scale computing, which can be implemented by virtual desktops on servers. Mobile access to virtual desktops provides enjoyable user experience in using virtual desktops.

This feature supports Android (version 4.1.2 and later) and iOS (version 8.0 and later) mobile clients.

User experience of mobile office is related to wireless network quality. You are not advised to use the VDI Mobile Office feature when the wireless network is of poor quality.

Application Scenario

Windows Virtual Desktop
●

1.11.3 Touchscreen Optimization

Version Requirements

The Touchscreen Optimization feature has been available since version 5.1.

Windows 10 tablet mode, Windows 10 original gestures, and enhanced SBC client experience are supported in version 6.1.

Summary

The Huawei FusionAccess application virtualization solution performs optimization on touchscreen-based mobile terminals to improve user experience.

Feature Description

The Huawei FusionAccess application virtualization solution performs optimization on touchscreen-based mobile terminals. This solution supports an intelligent floating customized toolbar. The toolbar provides functions like the keyboard, magnifier, touch mode change,

horizontal or vertical screen lock, and camera. The sequence of tool buttons can be adjusted, and the toolbar location can be changed.

The keyboard is automatically displayed when users enter information in the text box. The text box can be detected, and a customized keyboard is displayed. The keyboard disappears when users click an area out of the text box.

Intelligent scroll is supported. The input area is automatically adjusted to the screen center (not shaded by the keyboard), facilitating inputting.

Mobile clients, for example tablets and mobile phones, can be used to access the Windows 10 desktops, which are in tablet mode by default.

You can perform operations by native single-finger and multi-finger gestures of Windows 10 in this version. Single-finger gestures include click, double-click, right-click, drag, and roll. Multi-finger gestures include zoom in and zoom out.

Application Scenario

Application Virtualization
●

1.12 HD Graphics and Omnimedia Editing

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●		●

Introduction

The FusionAccess desktop system provides several mechanisms to support high-performance 2D/3D graphics processing and is compatible with mainstream 2D/3D graphics software.

Benefits

The implementation of this feature helps fully utilize features of the FusionAccess desktop system, such as high information security, and centralized maintenance.

1.12.1 GPU Passthrough

Version Requirements

The GPU Passthrough feature has been available since version 5.1.

In version 6.0:

GPU graphics cards Q2000, Q4000, K2000, and K4000 are out of production. The K2200 and K4200 replace K2000 and K4000 respectively.

The mainboard capabilities of V3 servers are improved to support more graphics cards.

The Windows 10 OS is supported.

Version 6.1 supports the Tesla M60 graphics card and GPU pool.

In version 6.2, the VRM (KVM) platform supports the P40/P4/M60 GPU.

Summary

The GPU Passthrough feature allows users to use graphics cards of physical machines or GPU passthrough VMs to implement high-performance graphics processing and access GPUs remotely through Remote Desktop Protocol (RDP). In GPU passthrough mode, GPUs (physical graphics cards) on the Computing Node Agent (CNA) are bound to user VMs, and users log in to VMs to use high-performance graphics applications.

The GPU Passthrough feature applies to high-performance graphics design and 120 Mbit/s HD video editing and 4K video editing scenarios.

Feature Description

In GPU passthrough mode, GPUs (physical graphics cards) on the CNA are bound to user VMs, and users log in to VMs to use high-performance graphics applications.

The GPU Passthrough feature applies to scenarios that require high GPU performance.

The VRM+XEN platform supports only E9000 + IPSAN, FusionCube 9000 appliance, and RH2288H V3 + IPSAN. Each server supports only one Tesla M60.

The VRM + KVM platform supports P40/P4/M60 GPU cards. P4/P40 graphics cards only support the RH2288H V5 server.

Supported graphics software includes Pro/E, Allegro, Altium Designer, and PADS. It is recommended that the effect of graphics software and large game software be verified in POC tests.

GPU pool is supported. In GPU pool scenarios, GPU cards must be mounted to an exclusive cluster and GPU graphics cards must share a same type in a same cluster.

For details about the specifications and restrictions, see the HD graphics write paper of FusionAccess desktop solution.

Application Scenario

Windows Virtual Desktop
●

1.12.2 HDP Plus

Version Requirements

The HDP Plus feature has been available since version 5.2.

4K video editing is supported in version 6.1.

The HDP Plus feature is supported only in Advanced Edition.

Summary

HDP Plus is a user experience improvement feature provided by Huawei FusionAccess Desktop Solution. It is used to improve experience and dual-screen display quality for GPU-based 120 Mbit/s HD video editing and 4K video editing.

Feature Description

HDP adopts intelligent video detection algorithms to detect the video area of real-time desktop transmission and uses the specific highly efficient compression algorithm for videos. This enables smooth video playback and reduces required bandwidth. HDP adopts intelligent image detection algorithms. It uses the lossless compression algorithm for texts and the lossy compression algorithm for natural images. This reduces required bandwidth while ensuring user experience.

The GPU passthrough technology removes mirror drivers from VMs to reduce GPU performance consumption of mirror drivers. The hardware snapshot function and compression interfaces provided by NVIDIA GRID SDK are used on VMs to release CPU pressure and improve VM performance. With the preceding technologies, Huawei first launched the ultra-HD video editing solution with a bit rate of 120 Mbit/s and 4K video editing for the media industry.

Dual-screen display for 120 Mbit/s HD video editing is supported.

TCs cannot meet the requirements of 4K display output and hardware decoding, so you must use PCs as the clients. PC specifications are as follows.

Type	Intel Core Graphics Card	Independent NVIDIA Graphics Card
GPU	Intel HD Graphics 4600 or later	GeForce GTX 650 or later
CPU	Intel Core i7 4770 or later	i5series with 3.0 GHz or more dominant frequency
Memory	6 GB	6 GB
Monitor	4K monitor	4K monitor

Application Scenario

Windows Virtual Desktop
●

1.12.3 GPU Hardware Virtualization

Version Requirements

The GPU Hardware Virtualization feature has been available since version 5.2.

Windows 10 is supported in version 6.0.

Version 6.1 supports the Tesla M60 graphics card and GPU pool.

Version 6.2 supports the Tesla M60 and Pascal P40 graphics card and GPU pool.

Summary

Hardware virtualization capability (VGX) is provided based on NVIDIA Tesla M60 and Pascal P40 GPUs.

The GPU Hardware Virtualization feature applies to graphics editing and 25 Mbit/s standard-definition video editing scenarios.

Feature Description

Graphics desktop VMs used for GPU hardware virtualization provide GPU graphics acceleration capabilities. Graphics software can use GPUs to implement hardware rendering. GPUs put rendered bitmaps into the video buffer and deliver contents in the buffer to terminals in real time. Virtual desktop display technology is embedded in Huawei VMs. Each vGPU VM sends rendering instructions and control commands to physical GPUs through an independent input channel. After rendering is complete, the driver sends desktop frame data to the VM. The desktop frame data is sent by RDP to the client for decoding and display.

A single server in GPU hardware virtualization supports a large number of users, achieving a balance between GPU performance, user density, and cost-effectiveness.

The following hardware forms support GPU hardware virtualization: server + IP SAN or FusionCube 9,000. Servers that support GPU hardware virtualization include the E9000 (CH220 V3) and RH2288H V3. Each E9000 CH220 V3 blade or RH2288H V3 supports one Tesla M60 GPU. One physical card can be virtualized into two pGPUs or 32 vGPUs. In the GPU hardware virtualization scenario, one graphics card is configured on each server for optimal performance.

In GPU pool scenarios, GPU cards must be mounted to an exclusive cluster and vGPUs must share a same type in a same cluster. User experience provided by the GPU Hardware Virtualization feature needs to be verified in POC tests.

The VRM + KVM platform supports P40/M60 GPU cards. P40 graphics cards only support the RH2288H V5 server.

User experience provided by the GPU Hardware Virtualization feature needs to be verified in POC tests.

Application Scenario

Windows Virtual Desktop
●

1.12.4 Graphics Workstation Management

Version Requirements

The Graphics workstation management feature has been available since version 6.2.

Summary

Customers' existing graphics workstations can be reused. The graphics workstations are centrally placed at a secure and controllable area and are allocated and managed using the desktop management system. Customers can use the HDP to log in to the workstations that have been taken over. This not only protects enterprises' current investments, but also allows customers to flexibly reuse resources.

Feature Description

Specifications are as follows:

1. Only NVIDIA Quadro M5000 and NVIDIA Quadro K2000 are supported. If you want to use other graphics cards in the workstation, a PoC test is required.

2. Only graphics workstations with the PS/2 interface are supported.

3. Workstations support Windows 7 and Windows10 only.

4. Only terminals CT6100 and ST6110 running the Windows OS are supported.

5. Workstations do not support the WI self-maintenance console.

6. Operations, such as remote startup, forcible shutdown and restart, and scheduled task management, cannot be performed on the workstations.

7. The HDP and RGS protocols cannot be used for preemption and login.

8. Cameras are not supported.

9. The graphics workstations can connect to two local monitors at most.

Application Scenario

Windows Virtual Desktop
●

1.13 Resource Reuse

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●		●

Introduction

The Resource Reuse feature is provided to fully use available resources to meet requirements of different services. Computing resources in a cluster are monitored, and free resources are released and used by different services in different time periods based on policies. This leverages resources and lowers investment costs.

Benefits

This feature improves resource utilization and reduces investment costs.

1.13.1 Memory Overcommitment

Version Requirements

The Memory Overcommitment feature has been available since version 5.2.

Summary

Most VMs use only a small portion of the physical memory that is allocated to them. Memory overcommitment allows a VM to use more memory space than the memory available on the physical host. The Memory Overcommitment feature improves memory utilization.

Feature Description

The Memory Overcommitment feature allows the unused memory of some VMs to be dynamically allocated to other VMs that require memory resources.

Technologies, such as memory ballooning, memory sharing, and memory swapping, are used based on memory overcommitment policies to release unused memory resources for other VMs and balance memory overcommitment among VMs in real time.

With optimized intelligent memory overcommitment policies, the system dynamically allocates memory resources based on the Guest OS load detected. This feature increases the memory overcommitment rate to 50% without affecting user experience.

The purpose of memory overcommitment is to:

Improve memory utilization: Hypervisor is used to reclaim free memory from light-loaded VMs and allocate memory resources to heavy-loaded VMs.

Improve the consolidation ratio: This feature enables VMs to consume less host memory. As a result, more VMs with high performance can be created on the hosts. This increases the VM density.

Advantage: This feature allows VMs to use more memory space than the memory available on the physical host, while user experience is not affected.

Application Scenario

Windows Virtual Desktop
●

1.13.2 Full Memory Virtual Desktop

Version Requirements

The Full Memory Virtual Desktop feature has been available since version 5.2.

Summary

Memory data deduplication compression and memory overcommitment technologies are used to store all system disk data of desktop VMs in memory so that read and write operations on disks of desktop VMs are converted to in-memory operations. This provides user experience higher than that of local PCs.

Feature Description

Memory data deduplication compression and memory overcommitment technologies are used to store all system disk data of desktop VMs in memory so that read and write operations on disks of desktop VMs are converted to in-memory operations. This provides user experience higher than that of local PCs.

- Linked clone VMs are supported. Personalized system disk data is not supported.
- This feature applies to scenarios without personalized requirements, such as schools, training institutions, and hotels. After the server is restarted, personalized data on the system disk is lost.
- The shutdown restoration capability is provided.

NOTE

The full memory desktop is not supported when the VRM (KVM) platform is used.

Application Scenario

Windows Virtual Desktop
●

1.13.3 Linked Clone

Version Requirements

The Linked Clone feature has been available since version 5.2.

Summary

A linked clone is a copy of a parent VM. The linked clone shares the virtual disks (the system volume) of the parent VM, which reduces VM creation time and disk space. In addition, it allows multiple VMs to use the same software installed within the parent VM. Modifications on the linked clones bring no impact on the parent VM. The linked clone desktop pool

provides unified software update and system recovery functions. This greatly reduces maintenance costs and improves desktop maintenance efficiency.

Feature Description

This feature enables users to perform the following operations:

- Prepare a linked-clone VM template.

  Define a template for creating linked clone VMs, create a common VM, install the software required by the linked clone desktop on the VM, and convert the VM into a VM template.

- Create linked clone VMs.

  Select a template and create linked clone VMs using the template.

- Delete a linked clone VM.

  Select a linked clone VM and delete it. If the linked clone VM to be deleted is the last one on the data storage device, also delete the base disk of the linked clone VM. After the base disk is deleted, the VM template still exists.

- Update a VM template.

  Before the template associates with a VM and after the template is used to create a linked clone VM and update operations are performed on the VM, administrators can convert the VM into a template. The new template has a new ID and does not overwrite the old template.

  When a template has associated VMs, you can clone the template to a new template and convert it to a VM. Then, the new VM can be converted to a template after all upgrade operations are performed.

- Apply an updated template to linked clone VMs.

  Update linked clone VMs by applying an updated template to the VMs. Updates take effect on all linked clone VMs after template replacement.

NOTE

The NL-SAS/SATA cannot be used as the system disk for linked clone VMs. The SmartTier function must be disabled for SAN storage.

Application Scenario

Windows Virtual Desktop
●

1.13.4 Storage Thin Provisioning

Version Requirements

The Storage Thin Provisioning feature has been available since version 5.2.

Summary

Storage Thin Provisioning allows flexible on-demand allocation of storage space, which improves storage utilization.

Difference between storage thin provisioning and traditional storage provisioning (thick provisioning):

Storage thick provisioning: A large amount of storage space is reserved for future usage. The space may be kept unused for a long time, which lowers the storage utilization.

Storage thin provisioning: Virtual storage space greater than the available physical storage space is achieved using the virtualization technology. The system allocates physical storage space only when data is written into the virtual storage. The virtual storage space that has no data does not occupy physical storage resources.

Feature Description

Storage Thin Provisioning is implemented based on the virtual disk level. It enables the administrator to allocate virtual disk files in the Common or Thin Provisioning mode. For a virtual disk in Thin Provisioning mode, the virtual storage management system allocates storage space for data stored on the virtual disk. However, the system only provides storage space required for storing data and does not provide storage space that has been allocated but is not used. As data stored on a virtual disk increases, the provided space increases. When all allocated space is provided, the Thin-Provisioning disk is the same as a Common disk.

Feature Dependency

Storage Thin Provisioning is independent of the OS and hardware. The Storage Thin Provisioning function is supported if the virtual image management system is available.

Capacity Monitoring

The data storage capacity alarm function is supported. An alarm threshold can be configured so that an alarm will be reported when the storage space occupied by data exceeds the threshold.

Space Reclaiming

Monitoring and reclaiming virtual disk space is supported. When a virtual disk is used for a period of time and the allocated space is large while the used space is small, the allocated and provided but unused space can be reclaimed. Currently, virtual disk space can be reclaimed in the NTFS format.

Application Scenario

Windows Virtual Desktop
●

1.13.5 iCache

Version Requirements

The Intelligent Cache (iCache) feature has been available since version 5.0.

Summary

With the iCache technology, storage resources shared by users can be dynamically detected and cached in the memory in the linked clone scenario based on IP SAN storage virtualization. This significantly improves the read performance, especially when VMs are started in batches, accelerating the startup of user virtual desktops.

Feature Description

Key data of the linked clone VM base disk is saved in the read cache to increase the disk-read speed and I/O performance of linked clone VMs. The iCache feature in FusionAccess Desktop Solution 5.0 supports the following two scenarios:

- Local server storage is used as the base disk and delta disk, and server memory is used as read cache.

  In this scenario, the linked clone base disk and delta disks are stored in the local disk of the physical server, and the cache image is stored in the memory of the physical server.

  This feature accelerates VM startup and improves user experience. It reduces the IOPS impact on the local storage of the server during VM startup, and lowers local storage costs by reducing the read IOPS.
- External shared storage is used as the base disk and delta disks, and the server memory functions as the read cache.

  In this scenario, the linked clone base disk and delta disks are stored in the external shared storage, and the cache image is stored in the memory of the physical server.

  This feature accelerates VM startup and improves user experience. It reduces the IOPS impact on shared storage during VM startup, eases the read IOPS pressure on some shared storage but cannot reduce the write IOPS. In addition, it supports live migration of VMs.

  When FusionStorage serves as storage resource pools, iCache is not supported, because FusionStorage can provide large-capacity cache.

NOTE

Linked clone iCache is not supported when the VRM (KVM) platform is used.

Application Scenario

Windows Virtual Desktop
●

1.13.6 Dynamic VM Scheduling and Reuse

Version Requirements

The Dynamic VM Scheduling and Reuse feature has been available since version 5.0.

Summary

Dynamic VM Scheduling includes load balancing and dynamic energy saving.

Elastic resource reuse allows services to use system resources of the cloud computing platform at different time periods, which maximizes the usage of cloud platform resources. In most scenarios, resource reuse must work with dynamic VM scheduling.

Feature Description

Load Balancing Scheduling

VM load balancing can be implemented only within a cluster that has at least two computing servers.

The load balancing policy defines scheduling thresholds and the period when the policy takes effect. In the effective period, if the CPU load of a computing server exceeds the scheduling threshold, the system will migrate some VMs to other computing servers with low CPU load. This ensures CPU load balancing between computing servers.

Dynamic Energy Saving Scheduling

VM dynamic energy saving can be implemented in the same cluster that has at least three computing servers.

Users can set the percentage of reserved resources and the effective period of policies when configuring dynamic energy saving scheduling policies. The effective period must be at least 2 hours. In the effective period, if the remaining CPU rate of computing servers exceeds the reservation ratio, the system automatically centralizes the VMs running on those light-loaded computing servers to one or several servers and powers off the other servers to save energy.

Elastic Resource Reuse

Elastic resource reuse allows services to use system resources of the cloud computing platform at different time periods, which maximizes the usage of cloud platform resources. Users use virtual desktops for work in daytime and release the computing resources at night. The system can use the released resources for other service tasks (such as image rendering and supercomputing) and release the resources after the service tasks are done. The resources can be used by users again for work in daytime. In this way, resource utilization is improved.

The FusionAccess Desktop Solution achieves elastic resource reuse in different application scenarios by configuring different scheduled tasks (such as startup, shutdown, hibernation, and waking) to implement automatic scheduling of VDI service resources.

Application Scenario

Windows Virtual Desktop
●

2 Features of Experience Improvement

2.1 Efficient Desktop Maintenance

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

Efficient desktop maintenance includes batch automatic desktop management, unified HDA software upgrade, resource statistics, user resource monitoring, desktop user experience optimization tool, and system deployment and planning tool. These functions help administrators manage the system efficiently.

Benefits

This feature provides high operation and management (O&M) efficiency, reduces misoperations, and lowers O&M administration cost.

2.1.1 Batch Automatic Desktop Management

Version Requirements

The Batch Automatic Desktop Management feature has been available since version 5.0.

Linked clone upgrade and VM restoration tasks can be forcibly stopped in version 6.1.

The tasks in the task center can be forcibly terminated, and the VM name can be displayed in the task query result in version 6.2.

Summary

Virtual desktop task management implements unattended management of VMs and supports the following batch operations:

- Create VMs.
- Start or stop VMs.
- Restart VMs.
- Wake up VMs.
- Hibernate VMs.

Feature Description

Task Type

Create, start, restart, shut down, wake up, or hibernate VMs in batches.

Implementation Mode

- Immediately
- Scheduled: Tasks are implemented at a specified time that is accurate to seconds.
- Periodically: Tasks are implemented periodically. After the start time, end time, and interval (accurate to seconds) of a periodic task are specified, the system automatically calculates the specific time to start the task and the number of times the task will be performed. Alternatively, users can specify the start time and set the end mode of a task to **Manual**. In addition, users can set a repeated task in the advanced setting, and specify the implementation interval and duration of the task.

Task Schedule Policy

Task schedule policies supported by the system include policies for starting, shutting down, or restarting VMs. Users can select a policy as required.

Task Management

Tasks can be suspended, restored, or deleted. Linked clone upgrade and VM restoration tasks can be forcibly stopped.

Task Querying

The following task information can be queried: task name, task type, task creation time, task triggering time, task start time, task end time, task status, and task implementation records.

Application Scenario

Windows Virtual Desktop
●

2.1.2 Unified Management System Upgrade

Version Requirements

The Unified Management System Upgrade feature has been available since version 5.3.

The ITA and LiteAD component upgrading has been available since version 6.0.

Summary

A unified management system upgrade tool is provided so that the administrator can run the tool on a PC or laptop to remotely upgrade management systems in batches.

Feature Description

A unified management system upgrade tool is provided so that the administrator can run the tool on a PC or laptop to remotely upgrade management systems in batches without the need of logging in to the hosts or VMs where management software runs.

FusionManager, FusionCompute, and FusionAccess management components support this feature.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

2.1.3 Unified AccessAgent Software Upgrade

Version Requirements

The Unified HDA Software Upgrade feature has been available since version 5.0.

Silent upgrade through the PV driver was introduced in version 5.0.

Upgrade by updating the base disk of linked clone VMs is supported in version 5.0.

The HDA software can be upgraded by using AUS or offline in version 6.1.

Version 6.2 supports the overwrite upgrade when the AUS is upgraded to the HDA. During the upgrade, whether the key services are installed and whether the installation is abnormal are checked.

Summary

The FusionAccess desktop system provides the HDA automatic upgrade function, which enables administrators to centrally manage software.

Feature Description

The HDA automatic upgrade supports the following upgrade modes:

Silent Upgrade Using the PV Driver

This upgrade mode applies to the VMs that have PV drivers installed. The PV drivers automatically upgrade the HDA.

Upgrade Using the AD Group Policy

The group policy on the AD is used to implement HDA upgrade.

Upgrade Using the Third-party Software Push Function

The third-party software push function is used to implement HDA upgrade.

Upgrade by Updating the Base Disk of Linked Clone VMs

The HDA software of linked clone VMs can be upgraded by updating the base disk.

Upgrade Using AUS

Three upgrade modes are supported: The administrator forcibly updates the software; the administrator notifies the upgrade; and users upgrade the software in self-service mode.

Forcible upgrade: The administrator selects a VM to upgrade the software without affecting users.

Upgrade notification: The administrator selects a VM and notifies users for upgrade. Users can select upgrade policies, for example, upgrade immediately or later.

Self-service update: In this mode, the system delivers upgrade operations to all VMs and notifies users for upgrade. Users can select upgrade policies, for example, upgrade immediately or later.

Offline Upgrade

The administrator sends a notification to users to download offline upgrade packages in a specified URL and perform one-click script upgrade for HAD.

NOTE

- If the AD group policy is used for the upgrade, the AD is required to send the group policy.
- Related software must be installed if the third-party software push function is used.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

2.1.4 Unified AccessClient Upgrade

Version Requirements

The Unified AccessClient Update feature has been available since version 5.0.

Summary

The FusionAccess desktop system supports automatic upgrade of AccessClient software, enabling administrators to manage software in a centralized manner.

Feature Description

The thin client manager (TCM) that is used for the Huawei FusionAccess Desktop Solution automatically upgrades AccessClient software installed on TCs.

Users can upgrade AccessClient software installed on TCs through the WI.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

2.1.5 Resource Statistics

Version Requirements

The Resource Statistics feature has been available since version 5.2.

Online user statistics can be collected based on desktop groups in version 6.1. User login statistics information contains login WI addresses.

In version 6.2, statistics on unused VM status are added. VMs can be sorted by VM idle time.

Summary

This feature supports query of VM information and user information. The VM information includes performance statistics and historical registration exception statistics. The user information includes the number of online users, usage time, login information, and unused VMs.

Feature Description

Status Statistics

Statistics on VM running status, login status, and assignment status are collected. Statistics information can be viewed based on VM groups, desktop groups, application groups and desktops.

Performance Statistics

Performance statistics of a specified time range are displayed in two parts:

A bar chart: displays the Top 10 users whose CPU usage and memory usage exceed 80%. (The vertical coordinate shows the Top 10 VMs.)

A list: displays performance data of all users on different pages. By default, users are sorted out in descending order based on the times when the CPU usage and memory usage equal or exceed 80%. The following items are displayed: site name, VM ID, username, sample quantity, average CPU usage, times when the CPU usage equals to or exceeds 80%, average memory usage, times when the memory usage equals to or exceeds 80%, average NETIN, average NETOUT, average DRWB, and average DRWN.

Historical Registration Exception Statistics

By default, information about HDC registration exceptions in the last 15 days is displayed based on users. The displayed information includes the site name, VM ID, username, and days. Query by site, VM ID, user, or time range is supported. Fuzzy query is also supported. The maximum time range is 180 days.

Online User Statistics

The online user statistics are displayed in two parts:

A line chart: displays the number of online users. The horizontal coordinate indicates the time, and the vertical coordinate indicates the number of users. By default, the number of online users on the current day is displayed.

A list: displays the number of online users on the current day.

Statistics in the latest 180 days can be queried. Statistics collection based on desktop groups is supported.

Statistics on Usage Time of Users

By default, statistics on usage time of users in the latest 15 days are displayed. The start time and end time in the latest 15 days are also displayed. For example, if the end time is the current day, the start time is 15 days before. The statistics including the following items are displayed in ascending order based on the usage time: VM ID, user, Desktop ID, and days (the time duration).

The value of **Days** represents the total usage time within the specified time range. If a user uses multiple VMs, the value for the user is the sum of the usage time of the VMs. Statistics collection based on desktop groups is supported.

Statistics on Unused VMs

Statistics on unused VMs in 180 days are displayed on different pages. The displayed information includes the VM name, VM ID, desktop group name, and belonged user (group). Statistics collection based on desktop groups is supported.

User Login Statistics

User login statistics in the latest 180 days are displayed. The displayed information includes the VM name, login user, desktop group name, terminal information (including the terminal name, IP address, MAC address, and system type), connection start time, connection created time, connection end time, connection failure cause, and login WI address.

Statistics on vAG Information

The vAG information is displayed, including incoming traffic, outgoing traffic, CPU usage, memory usage, number of online users, TCP packet retransmission ratio.

User connection statistics

The login user connection information in the vAG is displayed, including user login accounts, incoming traffic, outgoing traffic, historical maximum outgoing traffic, TC IP addresses, and RTT round trip delay.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

2.1.6 User Resource Monitoring

Version Requirements

The User Resource Monitoring feature has been available since version 5.1.

Summary

The User Resource Monitoring feature is provided to monitor VM information, including the internal CPU, memory, and network resource usage. In addition, the following VM information can be queried: VM status, user login information, and VMs that are not logged in to for a long time.

Feature Description

Monitoring of Internal VM Resources

Internal resource usage of VMs can be monitored using the FusionManager O&M system.

Items that can be monitored

Monitored Item	Content
Static information:	VM name
	VM ID
	IP addresses and MAC addresses of VMs
	Applications of VMs, VM type
Dynamic information	CPU usage
	Memory usage
	Incoming network traffic volume Outgoing network traffic volume
	VM status

VM Assignment Statistics

The following VM assignment statistics can be viewed on the FusionAccess O&M system.

- Number of all types of VMs that have been assigned, including the single-user mode, the static pooled mode, and the dynamic pooled mode
- Number of VMs that have not been assigned
- Number of VMs that cannot be assigned
- Number of VMs that are being processed

VM Login Statistics

The following VM login statistics can be viewed on the FusionAccess O&M system.

- Number of VMs that are ready to be logged in
- Number of VMs that have not been registered with the HDC
- Number of VMs that are connected to user terminals
- Number of VMs that are disconnected
- Number of VMs whose status is unknown

VM Running Statistics

The following VM running statistics can be viewed on the FusionAccess O&M system.

- Number of VMs that are running
- Number of VMs that are shut down
- Number of VMs that are hibernating
- Number of VMs in other status

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

2.1.7 O&M Management Tool Set (vTools)

Version Requirements

The O&M Management Tool Set has been available since version 5.0.

The O&M Management Tool Set is enhanced in version 5.3.

Summary

With years of desktop cloud maintenance experience, Huawei launched a desktop maintenance tool set to improve desktop cloud O&M efficiency. The tool set includes the AD checking tool, WI dialing test tool, WI image replacement tool, and information analysis tool, and provides third-party tool links and the online search function.

Feature Description

AD checking tool: checks AD (including the customer's AD) fulfillment, such as rights, during desktop cloud deployment.

WI dialing test tool: simulates a user to log in to a VM through the WI and sends the test results to administrators. This tool substitutes for manual routine inspection.

WI image replacement tool: replaces WI background images and logos.

Information analysis tool: analyzes the software and peripheral compatibility and collects statistics on performance data based on information collected by the information collection tool. System planning information collection tools are supported, including the presales information collection tool and information analysis tool. The tools can check the compatibility of desktop application software and peripherals in advance. The information collection tool can be used to collect configuration, software, and peripheral information about computers. The information analysis tool and compatibility maintenance tool can provide reports of software-hardware compatibility based on the compatibility list.

Third-party tool link: navigates users to third-party tools.

Online search: enables users to search for required information in the cloud computing maintenance forum by entering keywords.

Application Scenario

Windows Virtual Desktop
●

2.1.8 VIP Desktop

Version Requirements

The VIP Desktop feature has been available since version 5.3.

Summary

CPU and memory resources are guaranteed and monitored in real time for VIP desktops to provide better desktop experience for VIP users. VIP desktop status and resources (including VM status, CPU usage, memory usage, and system disk usage) are monitored, and statistics are collected on the performance. Administrators are notified by email when exceptions occur.

Feature Description

CPU and memory resources are guaranteed and monitored in real time for VIP desktops to provide better desktop experience for VIP users. VIP desktop status and resources (including VM status, CPU usage, memory usage, and system disk usage) are monitored, and statistics are collected on the performance. Administrators are notified by email when exceptions occur.

Application Scenario

Windows Virtual Desktop
●

2.1.9 Message Notification

Version Requirements

The Message Notification feature has been available since version 5.3.

Version 6.2 supports message notification when a user logs in to the virtual desktop again after the VM is disconnected.

Summary

Administrators can send real-time text notifications to user VMs.

Feature Description

Administrators can send real-time text notifications to user VMs, facilitating O&M management.

Application Scenario

Windows Virtual Desktop
●

2.1.10 Log Collection Tool

Version Requirements

The Log Collection Tool has been available since version 5.3.

The APS Log Collection feature has been available since version 6.0.

Summary

Logs of FusionAccess components can be collected remotely through FusionCare, which achieves one-click package and log collection.

Feature Description

Logs of FusionAccess components can be collected remotely through FusionCare, which achieves one-click package and log collection.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

2.1.11 Health Check Tool

Version Requirements

The Health Check Tool has been available since version 5.3.

Summary

The health check tool is provided to automatically check the system health.

Feature Description

The health check tool checks the system health and exports reports about the check results. O&M personnel can learn the system status and potential risks from the reports and work out solutions.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

2.1.12 Template Creation Tool

Version Requirements

The Template Creation Tool feature has been available since version 6.0.

Templates can be created based on user VMs in version 6.2.

Summary

The template creation tool is provided. Desktop cloud user VM templates can be created based on wizards. Operations such as desktop agent installation, system optimization, and parameter configuration are automatically completed.

Feature Description

The template creation tool is provided. Desktop cloud user VM templates can be created based on wizards. Operations such as desktop agent installation, system optimization, and parameter configuration are automatically completed.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

2.1.13 LazyDesk

Version Requirements

The LazyDesk feature has been available since version 6.0.

In version 6.2, users can press the shortcut key to exit the Lazydesk mode and return to the TC interface.

Summary

The Desktop Cloud enables users to directly use their virtual desktops after powering on TCs, providing users with similar experience when they use PCs.

Feature Description

The Desktop Cloud enables users to directly use their virtual desktops after powering on TCs, providing users with similar experience when they use PCs.

The main functions include:

1. Clients can be automatically started after TCs are powered on by presetting the login username and password.

2. Virtual desktops can bind TCs.

3. TC start menu, control panel and all applications can be hidden, and only cloud client login screen is displayed.

4. The setting menu of a cloud client and the toolbar of a client can be hidden. The desktop operating system is displayed in full screen after login.

This feature is applicable to call centers, cloud classrooms, multimedia classrooms, libraries, meeting rooms, and other scenarios that require simple login and efficient use.

Specifications are as follows:

1. Hiding function of TC start menu, control panel and all applications is only applicable to Huawei TCs, including CT3200, CT5100/CT5110, and CT6100/ST6110.

2. Hiding setting menu of cloud client and toolbar of client can be achieved by modifying the configuration files of the client. For setting of batch TCs, it is advised to pack the modified configuration files and login addresses of the cloud clients into patch files, and batch deliver the patch files to terminals by using TCM for taking effect.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

2.1.14 VM Rebuilding

Version Requirements

The VM Rebuilding feature has been available since version 6.2.

Summary

For a full copy VM, after the VM template is updated, you can use the VM rebuilding function to update the full copy VM. This feature can be used for VM fault recovery and VM OS upgrade, for example, from Windows 7 to Windows 10.

Feature Description

The restrictions on the VM reconstruction feature are as follows:

1. After a VM is rebuilt, the computer name and IP address remain unchanged, but personalized programs and data in the system disk will be lost. The personal application management and personal data management features must be configured together with this feature.

2. VM rebuilding only rebuilds the system volume in the template. The data volume is not rebuilt.

3. When multiple VMs are recreated in batches, the VMs must be created using the same template and use the same allocation type.

4. During VM rebuilding, determine whether to retain the system disk of the original VM as the data disk.

5. Hosting VMs, Linux VMs, and APS VMs do not support rebuilding.

Application Scenario

Windows Virtual Desktop
●

2.2 Desktop System High Reliability

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

The desktop management system adopts high reliability design to ensure high reliability during running of the FusionAccess desktop system.

The FusionAccess desktop system adopts multi-path and multi-plane designs to improve system reliability in terms of architecture.

Benefits

The FusionAccess desktop system is reliable, shortening service downtime and narrowing impact scope when a fault occurs.

2.2.1 Automatic Backup and Quick Recovery of Configuration Data

Version Requirements

The Automatic Backup and Quick Recovery of Configuration Data feature has been available since version 5.0.

Summary

The FusionAccess desktop system supports automatic backup of configuration data. Therefore, configuration data can be restored quickly in the case of data corruption or loss.

Feature Description

Automatic Backup and Quick Recovery of Configuration Data includes:

Backup and Recovery of Configuration Data for the Desktop Management System

Data and configuration of the desktop management system are automatically backed up to the Backup Server (the backup server). If FusionAccess configuration data is damaged or lost, the backup data can be used to quickly restore the FusionAccess system and services.

Backup and Recovery of Configuration Data for the Cloud Platform

The cloud platform adopts the active/standby mechanism to ensure reliability of management nodes. The configuration data of the management system is also backed up to a backup server, so that data can be quickly restored from the backup data in the case of data damage or loss.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

2.2.2 Desktop Reconnection

Version Requirements

The Desktop Reconnection feature has been available since version 5.0.

Summary

Virtual desktops are automatically reconnected within a specified time period at a specified interval after being disconnected unexpectedly.

Feature Description

The Desktop Reconnection feature applies to the following scenarios:

- Virtual desktop connection through a gateway

  When a gateway exists, the HDP client knows only the address ticket of the destination VM. When the desktop is reconnected, the gateway establishes a connection with the destination VM based on the address ticket saved by the HDP client.
- Virtual desktop connection without a gateway

  When no gateway exists, the HDP client knows the IP address of the destination VM. When the desktop is reconnected, the HDP client directly establishes a connection with the destination VM to recover the session.
- Preempted login during automatic reconnection

  During an automatic reconnection, a user logs in to the virtual desktop from another place. A message is displayed indicating that the desktop is preempted.

  The session persistence duration can be set from 0 second to 180 seconds.

  The automatic reconnection interval can be set from 1 second to 50 seconds.

Application Scenario

Windows Virtual Desktop
●

2.2.3 Port Negotiation for Desktop Connections

Version Requirements

The Port Negotiation for Desktop Connections feature has been available since version 5.0.

Summary

When a port conflicts with desktop agent software, the standby port is automatically used for desktop connection.

Feature Description

When desktop pre-connection starts, the main desktop connection program asks the communication module to implement pre-connection. The communication is listened. If a port fails to be enabled, standby ports (28510 to 28511) will be enabled for desktop connection. The number of the successfully enabled port is sent to the main program MainService, and then the MainService sends the port number to the desktop agent. The desktop agent sends the available port to the HDC.

If a gateway is used, the gateway obtains the IP address and port number of a VM from the HDC with an address ticket. If no gateway is used, the HDC sends the IP address and port number of the VM to the WI, and the WI sends them to the client.

Application Scenario

Windows Virtual Desktop
●

2.2.4 Desktop Agent Software Protection

Version Requirements

The Desktop Agent Software Protection feature has been available since version 5.0.

SBC has been available since version 5.3.

Summary

The desktop agent software can be protected from being deleted and killed by mistake. The desktop agent software recovers automatically after being killed by mistake.

Feature Description

After a VM starts, the HdpProtector process is started, which is used to protect the following applications: communication module, MainService, display, mouse and keyboard, audio, USB, HdpMonitor, Westone Gina, and HwGina. If a user logs in to the VM at the time, control codes are sent to make each application work again. If no user logs in to the VM, no control code is sent to make each application work again.

The HdpMonitor process protects the HdpProtector process. The HdpProtector and HdpMonitor processes protect each other.

The HdpProtector or HdpMonitor process checks whether the process protected by it exists every 2 seconds. If a process is killed by mistake, it will be automatically recovered.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

2.2.5 Networking Reliability

Version Requirements

The Networking Reliability feature has been available since version 5.0.

Summary

The FusionAccess desktop system adopts multi-path and multi-plane designs to improve system reliability in terms of architecture.

Feature Description

Full Redundancy of Network Paths

The FusionAccess desktop system uses different redundancy technologies on different network layers to ensure reliability of network connections.

On servers, multiple NICs are bound together to prevent service interruption due to faults on a single NIC.

At the access, convergence, and core layers, switches are stacked or added to clusters to ensure network path redundancy.

Multiple Network Planes

The FusionAccess desktop system uses three planes for communication: management plane, storage plane, and service plane.

These planes are separated by virtual local area networks (VLANs). The fault of one plane does not affect the other planes. For example, when the management plane is temporarily faulty, the service plane can still provide services for cloud terminal users.

In addition, the system supports priority settings based on VLANs. By setting the highest priority for internal management and control packets, the administrator and users can manage and control the system at any time.

Multiple Storage Paths

Multiple data storage paths are provided between servers and the storage system to increase data transfer bandwidth, improve data transfer reliability, and reduce storage fault risks. This design provides the following functions:

- Failover

  If a path is faulty or disconnected, the system automatically switches over services from the faulty path to an available path. This prevents service interruption caused by a single point of failure.
- Failback

  After the faulty path is restored, the system automatically switches over services to this path.
- Input/output (I/O) load balancing

  This function is used to evenly distribute network load on multiple storage paths and to increase data transfer bandwidth.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

2.2.6 High Reliability of Desktop Management Nodes

Version Requirements

The High Reliability of Desktop Management Nodes feature has been available since version 5.0.

Automatic monitoring of memory, CPU, and hard disk status of management nodes has been available since version 5.1.

Version 6.1 supports the LiteAD data consistency check and alarm.

Summary

Management nodes are deployed in active/standby mode. If a management node VM fails, the VM can be automatically recovered. Memory, CPU, and hard disk status of management nodes can be monitored automatically.

Feature Description

Management nodes are deployed in active/standby mode. When the active node is faulty, services can be automatically switched over to the standby node without affecting desktop services.

If a management node VM fails, the VM can be automatically recovered by restart.

Memory, CPU, and hard disk status of management nodes can be monitored automatically. An alarm is generated when exceptions occur. For example, hard disk space is insufficient.

AD data synchronization status detection and data inconsistency alarms of LiteAD are supported. The system can check the consistency between two LiteAD DHCP servers and report alarms.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

2.3 Self-Service Maintenance Management

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

User experience improvement covers self-service interface update, self-service power management, self-service maintenance, network status detection, desktop manager vDesk, and other functions.

Benefits

This feature improves user experience.

2.3.1 Self-Service Interface Update

Version Requirements

The Self-Service Interface Update feature has been available since version 5.0.

Summary

Users can set the language, background picture, and resolution on the displayed VM list page.

Feature Description

When a user uses a TC or SC to log in to a VM, the user can set the following options on the displayed VM list page:

- Language

  Two languages are available: simplified Chinese and English. After the preferred language is selected, the language displayed on the login page automatically changes.

- Background picture

  A variety of background pictures are available.

- Resolution

  When a user logs in to a virtual desktop, the system automatically sets the user VM resolution to the client resolution, ensuring that the virtual desktop can be displayed in full screen. Common resolutions are supported.

  HDP supports a maximum resolution of 3840 x 2560 for a single monitor.

  Considering desktop access bandwidth and user experience, the resolution higher than 1680 x 1050 is not recommended.

  The administrator can customize user login interfaces to allow additional information to be presented to users.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

2.3.2 Self-Service Power Management

Version Requirements

The Self-Service Power Management feature has been available since version 5.0.

Support for dynamic pooled desktops is added in version 5.3.

Summary

Users can implement power management for virtual desktops on the WI by using the automatic hibernation, restart, and forcible restart functions.

Feature Description

After logging in to the WI by entering a domain username and password, users can manage VMs (including static pooled and dynamic pooled desktops) power on the WI. Users can disable or enable the automatic shutdown, restart, or hibernation function.

Application Scenario

Windows Virtual Desktop
●

2.3.3 Self-Service Maintenance

Version Requirements

The Self-Service Maintenance feature has been available since version 5.1.

Summary

Users can use the Self-Service Maintenance feature to rectify faults when they fail to log in to VMs.

Feature Description

If the local network cannot be connected or the HDA does not function properly due to application software errors or human-induced mistakes, users fail to log in to the virtual desktop.

When this failure occurs, users can click the self-service maintenance system on the login portal. With the Self-Service Maintenance function, users can enter the virtual desktop system and rectify the fault. After the fault is rectified, users can log in to the virtual desktop through the portal.

Self-Service Maintenance helps reduce the workload of the administrator.

In FusionAccess Desktop Solution, this feature enables users to log in to the virtual desktop system using the VNC protocol, which reduces costs for deploying self-service maintenance channels.

GPU passthrough VMs do not support the default self-service maintenance channel.

Application Scenario

Windows Virtual Desktop
●

2.3.4 Visualized VM Startup Process

Version Requirements

The Visualized VM Startup Process feature has been available since version 5.0.

Summary

When users log in to stopped VMs, they can see the complete VM startup process.

Feature Description

If users log in to stopped VMs, because the virtual desktop agent is not started up, a message is displayed on the login page asking users to wait and try again later. By deploying the security gateway, Huawei FusionAccess can connect to VMs at the virtualization layer using VNC.

In the scenario of logging in to stopped VMs, the desktop login system automatically detects the scenario and starts the VNC client program to connect VMs. Therefore, users can see the complete VM startup process.

Application Scenario

Windows Virtual Desktop
●

2.3.5 Network Status Detection

Version Requirements

The Network Status Detection feature has been available since version 5.0.

Summary

Clients provide network status indicators. When user experience is not good, users can determine whether the network is faulty by observing indicators.

Feature Description

Clients are integrated with the network status detection function. The network status detection function can be used to determine the network status by checking the transmission delay of the HDP-based network between the client and the VM.

Table 2-1 describes the network status.

Table 2-1 Network status

Network Quality	Network Status Indicator on the Client	Round-trip Delay (RTD) Between the Client and the VM	User Experience
Excellent	Green	< 100 ms	Good
Good	Yellow	100 ms < Delay < 250 ms	Acceptable
Poor	Red	> 250 ms	Unacceptable

The network status detection function allows users to check whether poor user experience is caused by deteriorated network quality and locate faults on the network between the client and the VM.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

2.3.6 Login Information Display

Version Requirements

The Login Information Display Feature has been available since version 5.3.

Summary

When a user logs in to a VM, the user can view the last login information about the VM, including the terminal IP address and login time.

Feature Description

When a user logs in to a VM, the user can view the last login information about the VM, including the terminal IP address and login time.

Application Scenario

Windows Virtual Desktop
●

2.3.7 Desktop Connection Diagnosis and Recovery

Version Requirements

The Desktop Connection Diagnosis and Recovery feature has been available since version 5.0.

Summary

The one-click diagnosis and repair mechanism for desktop connections is provided. The following items are checked to rectify connection faults:

- NIC status
- Desktop agents
- IP addresses
- System clock
- Desktop protocol service status
- VM registration status
- Adding VMs to domains

Feature Description

The Huawei FusionAccess Desktop Solution provides the one-click diagnosis and repair mechanism to check necessary conditions for virtual desktop connection and rectify faults in one-click mode. Diagnosis items include the following:

- Whether the desktop agent is installed
- Whether the NIC is enabled

- Whether IP addresses are normal
- Whether VMs are added to the domain
- Whether the system clock is synchronized
- Whether the desktop protocol service is running
- Whether VMs are registered

The Huawei one-click diagnosis tool is installed during VM template creation and deployed on virtual desktops by default. The installation path is **All Programs\Huawei FusionAccess\FusionAccess Diagnostics**. Users can enable the diagnosis tool by clicking this application.

Application Scenario

Windows Virtual Desktop
●

2.3.8 Desktop Manager vDesk

Version Requirements

The Desktop Manager vDesk has been available since version 5.1.

The check items of the connection repair tool are enhanced and can be executed on VMs with user rights in version 6.2.

Summary

With years of experience in desktop experience optimization, Huawei provides a series of experience optimization tools, including the one-click desktop experience optimization tool, one-click connection restoration tool, and one-click log or information collection tool.

Feature Description

One-click desktop experience optimization tool: checks VM experience-related indicators and optimizes VM experience by one click. This tool provides the following functions:

- System acceleration: Checks VM performance indicators and optimizes the performance.
- Display optimization: Checks display performance indicators of VMs and optimizes the performance.
- Performance statistics: Provides information about network traffic, CPUs, and memory to help administrators learn the network, CPU, and memory status in real time.

One-click connection restoration tool: checks a VM that fails to be connected and restores recoverable options.

One-click log or information collection tool: The log collection tool is used to collect VM logs by one click for fault locating. The information collection tool is used to collect data of VM software, peripherals, and performance.

A variety of desktop cloud applications and peripherals exist. In addition, a large number of user terminals exist, and different users have different usage habits. Therefore, administrators

cannot provide complete and correct application, peripheral, and terminal information. Besides, it is difficult for administrators to manually collect application information. All these make requirement analysis incorrect. To ensure correct presales analysis, the presales information collection tool is provided to completely collect application, peripheral, and terminal information and improve information correctness and integrity. An analysis tool is also developed to provide simple analysis reports and improve correctness and convenience of presales assessment.

Peripheral assistant: The peripheral assistant can configure the current peripheral policy, locate and analyze peripheral faults, and provide links for peripheral compatibility query.

Application Scenario

Windows Virtual Desktop
●

2.3.9 Display Auto Energy-Saving

Version Requirements

The Display Auto Energy-Saving feature has been available since version 6.0.

Summary

In the desktop cloud, users can set policies to enable displays to be automatically sleep based on the using status of VMs, to save energy.

Feature Description

On PCs, displays can be automatically sleep when PCs are idle for a while by setting power management policies for saving energy. In desktop cloud scenario, display is connected to the terminal which it accesses. Power management policies can be only set by using terminal near-ends or TC management software. Huawei FusionAccess Desktop Solution supports a power management policy that is set through ITA Portal to control login terminal, so that display auto energy-saving is implemented.

Constraints are as follows:

1. Only Windows guest OS is supported. Linux VM is not supported at present.

2. Windows TCs and PCs are supported. Associated Linux TC CT3200, CT5100/ST5110, and CT6100/ST6110 are supported.

Application Scenario

Windows Virtual Desktop
●

2.3.10 Linked Shutdown

Version Requirements

The Linked Shutdown feature has been available since version 6.2.

Summary

When a user shuts down a VM, the TC automatically shuts down, simplifying TC management.

Feature Description

After a traditional PC is shut down, the monitor automatically shuts down. Huawei desktop solution enable users to set a policy that the TC terminal can be automatically shut down when a user powers off the VM. This simplifies TC power management and is applicable to cloud classrooms.

The TC is shut down when the VM is shut down but is not restarted or deregistered when the VM is restarted or deregistered.

In multi-instance scenarios, after linked shutdown is enabled, shutting down a VM shuts down the TC.

This function is disabled by default and needs to be enabled. You can use the TCM to push the configuration.

Constraints:

1. The linked shutdown function is not supported when Mac OS terminals are connected.

Application Scenario

Windows Virtual Desktop
●

2.4 Branch Office

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●		●

Introduction

The Branch Office feature supports desktop cloud services for branch offices of enterprises by deploying TCs remotely.

Benefits

This feature enables enterprises with multiple branches to centrally manage and maintain scattered virtual desktops, and centrally provision desktop services.

2.4.1 Branch Office Remote Module

Version Requirements

The Branch Office Remote Module feature has been available since version 5.0.

Summary

This feature provides a networking mode in which the service system is deployed locally at branch offices. This reduces network delay and ensures service bandwidth for branch offices, improving user experience for branch office and lowering quality requirements on the network between branch offices and the headquarters.

Feature Description

This feature achieves centralized O&M of scattered virtual desktops, including management and monitoring of hardware and virtual resources, centralized management of alarms and operation logs, SSO management, and TC management.

This feature achieves centralized provisioning of desktop services for branch offices.

With this feature, services and maintenance on a single branch office will not be affected even when the network between the branch offices and headquarters is disconnected.

A maximum of 20,000 VMs can be centrally managed. A maximum of 256 branch offices are supported, and each supports a maximum of 500 VMs. A branch office does not support a sub-branch office. The network between the headquarters and branch offices must have a bandwidth of 2 Mbit/s or higher. Only one VM of branch offices can be logged in at a time in the VNC mode through a management portal, because VNC login occupies 1.5–2 Mbit/s bandwidth.

The Branch Office feature supports the standard deployment mode, but does not support the appliance deployment mode. VM migration across different branch offices is not supported.

FusionManager cascading is not supported.

Application Scenario

Windows Virtual Desktop
●

3 High Security

3.1 Enhanced User Access Security

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

The Enhanced User Access Security package provides a series of access security hardening functions that include AD domain authentication, dynamic password login authentication, USB key login authentication, and fingerprint login authentication.

Benefits

This feature prevents unauthorized access and improves information security.

3.1.1 AD Domain Username and Password Authentication (Password)

Version Requirements

The AD Domain Authentication (Password) feature has been available since version 5.0.

SBC has been available since version 5.3.

In version 6.0, ITA supports domain account authentication login.

LiteAD is supported in version 6.1.

In version 6.2, users can configure that a password never expires in LiteAD configuration.

Summary

When a user logs in to a VM or virtual application or ITA management page, the user enters the Windows AD or LinuxAD domain username and password for authentication.

Feature Description

When a user enters a correct AD domain username and password on the WI, the user can log in to the WI and view the VM list or application list. After clicking a VM from the VM list, the user can log in to the virtual desktop. After clicking an application from the application list, the user can remotely use the application.

Desktop administrator can use domain account to log in to FusionAccess management system (ITA).

LiteAD can only be applied to application scenarios where a site has fewer than 300 desktops and only supports single domain and single site.

NOTE

Only Windows AD domain or LiteAD domain authentication is supported. Support for other domain authentication must be confirmed by performing interoperability tests.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

3.1.2 USB Key Authentication

Version Requirements

The USB Key Authentication feature has been available since version 5.1.

Windows 10 is supported in version 6.1.

UNS/WI supports multiple certificates in version 6.2.

Summary

The USB key authentication is implemented for users to log in to the FusionAccess desktop system. Windows terminals support smartcard SSO and non-SSO. Linux terminals support SSO only.

Feature Description

This feature allows a user to log in to the WI and VM by using a USB key or smartcard other than using a domain account.

When a user wants to access the WI from a TC browser, the user must insert the USB key into the physical USB port of the TC or insert the smartcard into a card reader first, and enters the personal identification number (PIN) of the USB key or the smartcard on the WI login page. If the PIN is correct, the user can log in to the WI and view the VM list. When the user clicks a VM to log in, in the smartcard non-SSO login scenario, the PIN text box is displayed on the VM login page. After entering the correct PIN, the user can log in to the VM OS. In the smartcard SSO login scenario, the desktop cloud management system records the PIN for logging in to the WI and enters the PIN on the VM login page for the user. Then the user can directly log in to the VM OS without entering the PIN again. USB key/smartcard authentication belongs to the two-factor authentication mode. To log in to VMs, users must

have the physical USB key or smartcard and know the PIN of the USB key or smartcard. The USB key or smartcard provides the function of locking the USB key after a user enters a wrong PIN for N times, which improves security for virtual desktop access.

The USB key is used by confidential institutions that require high security, such as governments, military, institutes, and banks.

The USB key applies when the user and VM have one-to-one, one-to-many, many-to-one, or many-to-many relationships. The USB key authentication mode is supported as long as the USB key driver is installed on the VM and TC for detecting the USB key.

The USB key login authentication feature has the following restrictions:

- This feature supports Windows 7 (32-bit/64-bit), Windows XP (32-bit), and Windows 10 (32-bit/64-bit) OSs for virtual desktops.
- This feature supports the following client OSs.
  - PC OS: Windows OSs (on which the USB key driver can be used) configured with Internet Explorer 8 or later
  - TC OS: Windows Embedded Standard (WES) and Linux OSs of the CT5100/ST5110 and CT6100/ST6110

NOTE

WES TCs support SSO and non-SSO, while Linux TCs support SSO only.

- In FusionAccess Desktop Solution 5.1, compatibility of USB keys Feitian ePass3000 and SafeNet eToken PRO 72k is verified. The Feitian ePass3000 has been verified by the National Information Network and often purchased by governmental enterprises. It is verified that Feitian ePass3000 and SafeNet eToken PRO 72k can be used on WES TCs for logging in to virtual desktops. Whether the USB keys provided by other vendors can be used on virtual desktops is not verified.
- VNC does not support USB mapping, and FusionCompute does not support remote USB mapping to VMs. If connection failures occur and users cannot log in to VMs by using the VNC self-maintenance function, contact the system administrator.

Application Scenario

Windows Virtual Desktop
●

3.1.3 Dynamic Password Login Authentication

Version Requirements

The Dynamic Password Login Authentication feature has been available since version 5.1.

Summary

Two-factor authentication, that is, AD domain plus dynamic password, is implemented for users to log in to virtual desktops.

Feature Description

Based on basic virtual desktop security, this feature provides high-security desktops for security-sensitive enterprises and organizations such as government agencies and military organizations. In addition to domain username and password, the dynamic password, another

authentication factor, is added when users log in to virtual desktops. This is a typical two-factor authentication mode. The dynamic password can be used only for once and cannot be predicted, so the dynamic password can be used to prevent password thefts and replay attacks.

Universal hardware or software dynamic password tokens are supported. When users log in to the WI, they must enter the domain username, password, and dynamic password on the WI login page. Users can log in to the WI only after the domain password and dynamic password pass authentication.

Short message service (SMS) dynamic passwords are also supported. SMS dynamic passwords are received through mobile phones. The administrator registers a user's account and mobile phone number on the dynamic password authentication server first. To log in to the WI, the user must enter the domain password. After the domain password passes authentication, the WI sends the domain account information to the dynamic password authentication server. The dynamic password authentication server generates a dynamic password and sends the password to the user's mobile phone through an SMS gateway. The user enters the dynamic password on the WI login page within the specified time period for login authentication. After authentication is successful, the user can view the VM list on the WI.

Only the two-factor authentication, domain password + dynamic password, is supported. Authentication based only on the dynamic password is not supported.

The dynamic password authentication servers that have been jointly commissioned are Shanghai DynamiCode and Feitian servers.

Both WI and UNS support dynamic password authentication.

Application Scenario

Windows Virtual Desktop
●

3.1.4 Desktop Isolation on a Terminal

Version Requirements

The Desktop Isolation on a Terminal feature has been available since version 5.3.

Summary

With two physical NICs and the dual-screen display feature provided by TCs, virtual desktops provisioned over different physical networks can be displayed on a TC while ensuring physical isolation between each other.

Feature Description

- TCs provide two gigabit NICs and support dual-screen display through the DVI-I interface. The external network is physically isolated from the private network.
- Customized security-hardened Linux OSs do not allow users to install software without permission so that screenshot capture software or Trojan horse software cannot host on the Linux OSs.

- The TC system is read-only and supports restoration upon restart. All temporary files are deleted after system shutdown.
- By using the security control mechanism of the desktop protocol, TCs can receive VM display information only, but users cannot upload or download any files using TCs. This prevents viruses.
- When a user exists from a virtual desktop, the desktop displayed on the TC also exists. All memory data is cleared, and no display image is retained.
- The CT6100 and CT6110 provide two physical NICs to support this feature.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

3.1.5 Interconnection with Third-Party Identity Authentication Systems

Version Requirements

The Interconnection with Third-Party Digital Certificate Authentication Systems feature has been available since version 5.0.

The identity authentication customization capability has been available since version 6.0..

Summary

The feature allows the desktop cloud authentication system to be integrated with USB key identity authentication systems of third-party security vendors (such as Westone and Xingtang). After a user inserts a USB key and enters the PIN to log in to an identity authentication gateway of a security vendor, the user can log in to the WI and VM without entering the PIN again. To ensure VM access security, only the USB key can be used to access VMs.

Huawei provides APIs for users to customize identity authentication. Integrators can redevelop the APIs to interconnect with third-party non-AD authentication systems, such as the LDAP authentication server, fingerprint authentication server, and digital certificate authentication server.

Feature Description

Third-party digital certificate authentication system is supported.

The FusionAccess desktop system can interconnect with identity authentication systems of third-party security vendors in two modes:

- The security gateway entering the password for users

  The digital certificate authentication system and AD authentication mode are used together for authenticating desktop cloud logins but presents only USB key login mode to users. The AD domain authentication mode is used in VDIs, and the unified user management platform of security vendors translates between the user certificate and

domain username/password. SSO is implemented for WI and VM logins. That is, users need to enter the PIN only for once when logging in to the WI and VM.

The identity authentication gateway is deployed in front of the load balancer or access gateway. The gateway client intercepts the WI login request and sends the request to the identity authentication gateway (an encrypted channel is established between the gateway client and the identity authentication gateway). The identity authentication gateway processes the request (for example, enters the domain password for the user) and sends the login request to the WI for authenticating the AD domain username and password. When a user logs in to a VM, the USB key is mapped to the VM. Windows OS login is implemented by the host and auditing software secure login modules. The Huawei FusionAccess desktop system sends related information to secure login modules, and security software authenticates the VM login.

- Ticket

  The digital certificate authentication system and AD authentication mode are used together for authenticating desktop cloud logins but presents only USB key login mode (including tickets) to users. The AD domain authentication mode is used in VDIs, and the ticket is used to translate between the user certificate and domain username/password. The identity authentication system generates a ticket after the USB key authentication is successful. The ticket is used for WI and VM logins.

NOTE

- This feature supports Westone (supports the mode in which the gateway enters the password for users) and Xingtang (supports two modes) systems only. Adaption may need to be performed for integration with other identity authentication systems on Huawei products or on third-party identity authentication systems.
- Only the USB redirection mode is supported for mapping the USB key to VMs. In this mode, the USB key is exclusively occupied. After the USB key is redirected to a VM, the USB key cannot be detected on the TC, which is equivalent to that the USB key is removed from the TC.
- Security vendors do not provide USB key drivers for Linux OSs. In Huawei FusionAccess Desktop Solution 5.1, WES 7 TCs are supported.
- When third-party digital certificate authentication systems are integrated, a VM cannot be shared by multiple users.
- VNC does not support USB mapping, and FusionCompute does not support remote USB mapping to VMs. If connection faults occur, users cannot log in to VMs by using the VNC self-maintenance function. In this case, contact the system administrator.
- The identity authentication customization capability is provided.
- For the identity authentication customization capability of Huawei FusionAccess Desktop Solution, integrators can redevelop it based on the API provided by Huawei to implement the interaction with third-party non-AD authentication system, such as LDAP authentication server, fingerprint authentication server, and digital certificate authentication server.
- Plug-ins and desktop portal (WI) northbound API customization modes are supported. Huawei only provides interfaces, and does not provide customization and development.

Application Scenario

Windows Virtual Desktop
●

3.1.6 Fingerprint Login Authentication

Version Requirements

The Fingerprint Login Authentication feature has been available since version 5.1.

Biocome pressure-sensitive fingerprint scanner can be used to log in to a desktop in version 6.1.

Summary

This function is applicable to virtual desktop login authentication and applications authentication.

Feature Description

Fingerprint authentication can greatly improve user access security. This function is applicable to virtual desktop login authentication and applications authentication.

- Fingerprint authentication

  A fingerprint scanner is used for authenticating VM logins. Users do not need to enter the domain username and password, simplifying the login process.

  Before using the fingerprint for login, users need to register or modify their fingerprints on the WI login page. Users' fingerprint information is encrypted and saved on TCs.

- Two-factor (domain and fingerprint) authentication

  In this authentication mode, a user's identity is verified by two factors: domain account and fingerprint. When a user attempts to log in to a VM, the user is required to enter the domain account information: username and password. If the username and password are correct, the user must swipe the finger against the fingerprint reader. The user can access the VM only when the fingerprints match. The two-factor authentication improves desktop security.

- On-click authentication by pressing on the fingerprint scanner

  A fingerprint scanner is used for authenticating VM logins. Users do not need to enter the domain account and password, thereby simplifying the login process and improving usability.

  Before using the fingerprint for login, users need to register or modify their fingerprints on the WI login portal. Users' fingerprint information is encrypted and saved on centralized fingerprint servers.

  On-click authentication by pressing on the fingerprint scanner and domain account and password authentication can coexist.

  UNS and SBC scenarios are not supported.

  Only the Biocome fingerprint scanner BFK3000B can be used. Fingerprint scanners and fingerprint authentication servers must be purchased from Biocome. Software like fingerprint plug-ins and login modules must be obtained from Biocome.

  TCs matching the pressure-sensitive fingerprint scanner are CT5100 and CT6100 WES.

- Two-factor (domain and fingerprint) authentication

  In this authentication mode, a user's identity is verified by two factors: domain account and fingerprint. When a user attempts to log in to a VM, the user is required to enter the domain account information: username and password. If the username and password are correct, the user must swipe the finger against the fingerprint reader. The user can access

the VM only when the fingerprints match. The two-factor authentication improves desktop security.

- Application system authentication

  When the fingerprint authentication is used for application system authentication, the desktop management system maps the fingerprint device to the virtual desktop system. Install the required fingerprint driver and software on the virtual desktop system. The management of fingerprint reader and the binding of application programs are performed by the software of the virtual desktop system. The fingerprint encryption data is stored in the user virtual desktop system.

NOTE

- Certified fingerprint scanners include Biocome TCR4, TCR4K, and TCR4KC. Other fingerprint scanners need to be verified by performing a test.
- The fingerprint login mode does not apply to VMs in the dynamic resource pool, because fingerprint data needs to be stored in VMs but VMs in the dynamic resource pool are allocated randomly for users during login. VMs connected in non-WI mode do not support fingerprint authentication.
- Currently, two-factor (domain and fingerprint) authentication is supported by Windows XP 32-bit.

Application Scenario

Windows Virtual Desktop
●

3.1.7 Verification Code Login Authentication

Version Requirements

The Verification Code Login Authentication feature has been available since version 6.2.

Summary

In scenarios where malicious login attacks may occur during Internet access, users can configure the WI to force the user to enter the verification code during login to improve security.

Feature Description

Users can enable the verification code login function for the WI cluster by configuring policies on the WI.

The verification code is valid when the TC, SC, and Android/iOS mobile clients access the desktop system.

Application Scenario

Windows Virtual Desktop
●

3.1.8 Restricted TC Access

Version Requirements

The Restricted TC Access feature has been available since version 5.1.

You do not need to enter the MAC address in version 6.1.

Summary

Binding between TCs and user accounts is supported. Some TCs can be accessed only using specified accounts. Users can only log in to the FusionAccess desktop system using the TCs bound with the account.

Feature Description

The system supports binding between TCs and users, and binding between users and VMs. This allows users to access specified VMs by using specified TCs. This function meets the enterprise requirements for information security, preventing unauthorized access to sensitive information.

Upon a user's first login, the system automatically binds the MAC address of a TC with the login username. The administrator can manually unbind the relationship and bind the TC MAC address with the user again.

NOTE

- Windows TCs and Linux TCs support this function.
- TCs produced by Huawei support this function.

Application Scenario

Windows Virtual Desktop
●

3.1.9 Unidirectional TC Authentication

Version Requirements

The Unidirectional TC Authentication feature has been available since version 5.2.

Summary

In scenarios with high system security requirements, root certificates must be installed on TCs before connecting to user VMs.

You need to configure this feature on FusionAccess and import related certificates to vAGs and TCs. Unidirectional authentication is implemented to prevent unauthorized TCs from connecting to the desktop cloud.

Feature Description

In scenarios with high system security requirements, root certificates must be installed on TCs before connecting to user VMs.

You need to configure this feature on FusionAccess and import related certificates to vAGs and TCs. Unidirectional authentication is implemented to prevent unauthorized TCs from connecting to the desktop cloud.

Application Scenario

Windows Virtual Desktop
●

3.1.10 Bidirectional TC Authentication

Version Requirements

The Bidirectional TC Authentication feature has been available since version 5.2.

Summary

In scenarios with high system security requirements, client certificates must be installed on TCs before logging in to the WI.

To ensure security for the WI server and TCs, you need to import a server certificate to the WI server for TC authentication and import client certificates to TCs for WI server authentication.

Feature Description

In scenarios with high system security requirements, client certificates must be installed on TCs before logging in to the WI.

To ensure security for the WI server and TCs, you need to import a server certificate to the WI server for TC authentication and import client certificates to TCs for WI server authentication.

Application Scenario

Windows Virtual Desktop
●

3.2 Load Balancer and Security Gateway

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

The Load Balancer and Security Gateway feature helps improve user experience and desktop connection reliability and security.

Benefits

This feature helps provide reliable desktop clouds.

3.2.1 Desktop Access Load Balancing

Version Requirements

The Desktop Access Load Balancing feature has been available since version 5.0.

Summary

A hardware load balancer (HLB) uses multiple servers to share traffic and improve service reliability. The HLB products SVN, F5, and NetScaler are supported.

Feature Description

A large-capacity FusionAccess desktop system requires multiple sets of WIs to quickly respond to users' login requests and improve user experience and system reliability. The load balancing technology is used to shield information of multiple sets of WIs from end users and balance traffic among WIs.

Load balancing provides the following advantages:

- Addresses of multiple sets of WIs are shielded from users, and users can log in to the WI using one address.
- Multiple sets of WIs work in load balancing mode, improving system reliability.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

3.2.2 Hardware Security Gateway

Version Requirements

The Hardware Security Gateway feature has been available since version 5.1.

The F5 can serve as the hardware security gateway in version 6.2.

Summary

Security access gateways encrypt HDP data flows, improving FusionAccess desktop system security. The hardware security gateway SVN is supported.

Feature Description

HDP Data Flow Encryption

After the security access gateway is deployed, HDP data flows sent by users for accessing the FusionAccess desktop system are SSL-encrypted to improve system security.

Network Isolation

After the security access gateway is deployed, the access client connects to the virtual IP address of the access gateway, so the IP address of the virtual desktop is not exposed to the access client. In this manner, the IP address segment of the virtual desktop is isolated from the IP address segment of the access client, improving security for virtual desktop data.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

3.2.3 Software-based Load Balancing

Version Requirements

The Software-based Load Balancing feature has been available since version 5.1.

Summary

The virtual load balancing (vLB) software of the Huawei FusionAccess Desktop Solution supports desktop access load balancing. This saves user investment.

Feature Description

A large-capacity FusionAccess desktop system requires multiple sets of WIs to quickly respond to users' login requests and improve user experience and system reliability. The load balancing technology is used to shield information of multiple sets of WIs from end users and balance traffic among WIs.

Load balancing provides the following advantages:

- Addresses of multiple sets of WIs are shielded from users, and users can log in to the WI using one address.
- Multiple sets of WIs work in load balancing mode, improving system reliability.
- The vLB software of the Huawei FusionAccess Desktop Solution supports desktop access load balancing. This saves user investment.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

3.2.4 Software-based Security Gateway

Version Requirements

The Software-based Security Gateway feature has been available since version 5.1.

Version 6.2 supports vAG distributed cluster deployment and provides large-scale networking capabilities.

Summary

The virtual access gateway (VAG) software of the Huawei FusionAccess Desktop Solution supports desktop security gateways, saving user investment. It supports vAG distributed cluster deployment and provides large-scale networking capabilities.

Feature Description

HDP Data Flow Encryption

After the security access gateway is deployed, HDP data flows sent by users for accessing the FusionAccess desktop system are SSL-encrypted to improve system security.

Network Isolation

After the security access gateway is deployed, the access client connects to the virtual IP address of the access gateway, so the IP address of the virtual desktop is not exposed to the access client. In this manner, the IP address segment of the virtual desktop is isolated from the IP address segment of the access client, improving security for virtual desktop data.

The VAG software of the Huawei FusionAccess Desktop Solution supports desktop security gateways, saving user investment. The software applies to small-sized sites that have fewer than 600 VMs.

Policy and Performance Monitoring

Policy control based on user access addresses is supported.

Basic performance monitoring and gateway statistics are supported.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

4 Backup and DR

4.1 Virtual Desktop Backup

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●		●

Introduction

The online backup system for virtual desktops applies when individuals want to back up their important files Mission-critical data can be backed up either manually or by running scheduled tasks. If data of a virtual desktop is lost, for instance, due to disk damage or accidental deletion, the data can be restored from the backup system.

The objectives of online backup are as follows:

- Data integrity protection: minimizes data loss.
- Rapid system recovery: minimizes service downtime.

Benefits

This feature restores data immediately if a disaster occurs and reduces the financial loss caused by unexpected data loss.

4.1.1 NAS Backup

Version Requirements

The NAS Backup feature has been available since version 5.0.

Summary

Two NAS backup schemes are available: NAS backup server scheme and NAS high-available disk scheme.

Feature Description

Virtual desktop users can back up data using either of the following methods:

Backing Up Data to NAS Servers

- Data backup process

  FusionAccess client users manually or run scheduled tasks to back up important files from their virtual desktops to NAS servers by sharing hard disks over a network.

  Backup methods are as follows:

  - Users manually copy files or directories from their virtual desktops to shared directories on NAS servers.
  - Users run scheduled tasks to copy files or directories from their virtual desktops to shared directories on NAS servers.
  - Users trigger the backup and restoration mechanism provided in Windows OSs that run on their virtual desktops to regularly back up files and directories from their virtual desktops to shared directories on NAS servers.

- Data restoration process

  Restoration methods correspond to backup methods.

  - If users have backed up data manually by running scheduled tasks, they have to copy the backup files from the shared directories on NAS servers to their virtual desktops.
  - If users have backed up data by using the backup and restoration mechanism provided in Windows OSs, they have to trigger the restoration function to restore data.

Backing Up Data to NAS High-Available Disks

Configure an active NAS server and a standby one. Allocate personal directories on the active server and map them to virtual desktops as high-available network disks.

The active and standby NAS servers synchronize data between each other in real time. If the active NAS server fails, data is handed over to the standby server to prevent data loss.

- Data backup process

  VM users store important data on NAS high-available disks.

  The active NAS server regularly synchronizes data to the standby NAS server for backup.

- Data restoration process

  If the active NAS server fails, the administrator switches the standby server to the active role so that users can continue to access NAS high-available disks from their virtual desktops.

NOTE

Additional NAS storage devices must be configured.

Application Scenario

Windows Virtual Desktop
●

4.1.2 VM Backup

Version Requirements

The VM Backup feature has been available since version 5.0.

Version 6.0 is matched with FusionSphere 5.1 version, in which, eBackup VM backup solution is imported.

Summary

The eBackup VM backup solution is supported.

Feature Description

Desktop cloud VM backup function depends on the VM backup capacity of Huawei FusionShpere virtual platform.

Huawei FusionShpere 5.1 and later versions all provide the eBackup VM backup solution, in which Huawei eBackup backup server needs to be deployed and CBT (Changed Block Tracking) and snapshot of FusionCompute are used to back up VM data. eBackup, together with FusionCompute, can back up specified VMs or specified volume objects in the VMs based on specified backup policies. When a VM becomes faulty or its data is lost, the VM can be restored using the backup data. The destination end of data backup can be SAN or NAS storage.

For details about specifications and constraints of eBackup backup solution, see *FusionSphere 5.1 Technical White Paper on Backup (Server Virtualization)*.

NOTE

In the desktop cloud scenario, disable the periodic password update policy for the VM that uses eBackup for backup in AD because the backup VM cannot perform password updating after the password is updated, which makes the restored VM offline and users cannot log in to it.

Application Scenario

Windows Virtual Desktop
●

4.2 Virtual Desktop DR

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

DR is the ability to recover from a disaster. To implement DR, two or more IT systems with the same functions are deployed at different locations. The IT systems monitor the health status of each other. If one IT system is unavailable due to an unexpected event such as a fire or earthquake, the services can switch over to the IT system at a different location.

The DR objectives are as follows:

Data integrity is protected, and service data loss is minimized, which is measured by recovery point objective (RPO).

The system is quickly restored, and service interruption time is minimized, which is measured by recovery time objective (RTO).

Benefits

The service system reliability is improved, avoiding service interruption or long-term interruption.

4.2.1 GSLB Service DR

Version Requirements

The GSLB Service DR feature has been available since version 5.0.

Summary

The global server load balance (GSLB) mode is adopted to provide DR capability for desktop cloud services. This feature applies to scenarios without individual data, such as call centers and customer service centers.

Feature Description

In standard desktop scenarios (without individual data), such as call centers and customer service centers, two desktop cloud systems are constructed in different locations and work in active/standby mode. Users can access both systems. That is, the virtual desktop of a user exists in both desktop cloud systems. If the local system encounters an unexpected disaster, services will switch over to the system located in another place through GSLB. After VMs are started from the remote system, they continue with service provisioning.

F5 or NetScaler is supported. Related GSLB licenses must be configured.

When the faulty site is recovered, services are automatically switched back to the site when users log in to virtual desktops.

Application Scenario

Windows Virtual Desktop
●

4.2.2 TC Autonomous DR

Version Requirements

The TC Autonomous DR feature has been available since version 5.2.

Summary

TCs detect the service status of the production site and DR site in real time. When the production site is faulty, TCs automatically connect to the DR site, and desktop VMs in the DR site continue to provision services.

Feature Description

TCs detect the status of the production site and DR site. When the production site is faulty, TCs automatically connect to the functional DR site. If data disks require DR, the NAS remote replication function must be enabled. DR capability is not provided for programs and data on the user system disk. In TC autonomous DR mode, GSLB is not required.

Application Scenario

Windows Virtual Desktop
●

4.2.3 UltraVR DR

Version Requirements

The UltraVR DR feature has been available since version 5.3.

This feature is commercially used under control.

Summary

The UltraVR-based array replication function is used to implement VM DR. This DR mode ensures consistency between DR VMs in the DR site and user VMs in the production site.

Feature Description

UltraVR replicates VM data in the production site to the DR site using the asynchronous remote replication function of Huawei storage. UltraVR replicates VM specifications and manages DR plans. When a disaster occurs, a DR switchover is automatically implemented based on the DR plan. RPO is the data replication cycle between storage systems. RTO is the system switchover time and VM startup time.

For details about specifications and restrictions of the UltraVR platform, see the *Huawei FusionSphere 6.0 Technical White Paper on Disaster Recovery (Server Virtualization*.

Other restrictions are as follows:

1. Only asynchronous DR is supported.

2. The tasks of the primary site are not backed up on the secondary site.

3. The ITA and HDC databases must be deployed together.

NOTE

UltraVR DR is not supported when the VRM (KVM) platform is used.

Application Scenario

Windows Virtual Desktop
●

5 NBI and DaaS

5.1 NBI

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

Northbound interfaces (NBIs) are provided for system and service management, allowing a third-party upper-layer management system to centrally manage and maintain the cloud platform FusionManager and desktop cloud service system FusionAccess.

Benefits

The NBIs enable the desktop cloud system to interwork with a third-party cloud management system.

5.1.1 System Management NBI

Version Requirements

The System Management NBI feature has been available since version 5.1.

Summary

The upper-layer management system interacts with the FusionAccess desktop system through the FusionManager system NBI to centrally manage and maintain the cloud platform and optimize the use of cloud platform resources.

Feature Description

Interface Security Hardening

The open application platform interface (API) feature supports HTTP and HTTPS. Users must enter the username and password for authentication to access the NBI. The password is encrypted using the RSA-2048 asymmetric encryption to ensure password transfer security. The open API supports login over the AD interface.

Obtaining O&M Management Data

Users can obtain the O&M management data of the FusionManager system through the open API, including real-time and historical alarm data and object-based real-time and historical monitoring data. This data helps users ascertain the system running status.

Obtaining Cloud Computing Resources

Through the open API, resource data of the FusionManager system can be obtained easily. The resources include cluster resources, server resources, VM resources, and switch resources.

Support for Maintenance Operations

Through the open API, maintenance operations can be performed on the FusionManager system. For example, start, shut down, restart, or migrate a VM, or power on, power off, or restart a server.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

5.1.2 Service Management NBI

Version Requirements

The Service Management NBI feature has been available since version 5.0.

Summary

FusionAccess provides an open NBI for provisioning virtual desktop services. The NBI enables users to rapidly provision services and to create, assign, start, restart, shut down, and unassign VMs.

Feature Description

The service provisioning NBI is provided in REST mode for customers to control service provisioning. Currently, the NBI provides resource management interfaces for the following functions:

- Fast service provisioning
- Creation of VMs
- VM attaching (common/linked clone)
- Adding or deleting users in the 1:N association mode
- Query of VM information, including information about a list of VMs or a single VM

- Operations on VMs, including starting, restarting, hibernating, waking up, shutting down, deleting, or unassigning VMs, and modifying VM specifications
- Computer group management
- Desktop group management
- Interfaces for special functions

The service provisioning NBI serves only one fixed customer. Multiple clients can be connected but the clients must belong to the same customer. The NBI does not support multiple tenants.

Application Scenario

Windows Virtual Desktop	Application Virtualization
5.1.3 ●	●

6 Compatibility and Huawei Ready

6.1 Compatibility with the Infrastructure Cloud Platform

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

The FusionAccess desktop cloud solution consists of the desktop access software FusionAccess, cloud platform software FusionSphere, and peripheral components.

Benefits

The virtualization platform software compatible with FusionAccess is specified.

6.1.1 FusionSphere

Version Requirements

The FusionSphere feature has been available since version 5.1.

The VRM + KVM platform is supported in version 6.2.

Summary

Huawei FusionAccess desktop cloud solution is compatible with the FusionSphere cloud platform.

Feature Description

Huawei FusionSphere offers an agile and efficient cloud operating system whose performance is tripled by distributed storage virtualization. Its virtualization performance was proved in the SPECvirt_sc2010 test to be industry-leading.

Huawei FusionAccess desktop cloud solution is compatible with the FusionSphere cloud platform. The FusionSphere cloud platform provides virtual desktop systems with the secure and efficient virtualization platform and management functions.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

6.2 Desktop Cloud Compatibility

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

The Huawei FusionAccess Desktop Solution is an open system. Huawei works with desktop cloud vendors in the industry to complete the desktop cloud ecosystem through Huawei Ready certification.

Benefits

Software and hardware, peripherals, and terminals with which the Huawei FusionAccess Desktop Solution is compatible are determined, which enriches application scenarios and scopes of the Huawei FusionAccess Desktop Solution.

6.2.1 FusionAccess Huawei Ready

Version Requirements

The FusionAccess Huawei Ready feature has been available since version 5.1.

Summary

FusionAccess Huawei Ready is a product certification plan, which enables partners to verify that their products and solutions are compatible with Huawei cloud computing solutions.

Feature Description

FusionAccess Huawei Ready covers the system, hardware, software, peripherals, and terminals.

After certified by FusionAccess Huawei Ready, partners' products are compatible with Huawei cloud computing solutions so that partners' products can provide edges for the integrated solution.

Partners' products can be tested in a remote environment provided by the Huawei FusionAccess Desktop Solution or in a testing environment where the desktop cloud software trial edition has been installed.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

6.2.2 Peripheral Assistant

Version Requirements

The Peripheral Assistant has been available since version 5.3.

Summary

A peripheral troubleshooting tool is provided to locate faults when peripherals cannot work in desktop cloud scenarios.

Feature Description

The peripheral troubleshooting tool provides the following functions:

- Policy self-check: Automatically checks the peripheral policies of VMs and identifies typical device redirection modes.
- Configuration guidance: Displays the redirection mode of a peripheral device and provides illustrated configuration guidelines.
- Regular analysis: Automatically performs regular analysis or allows users to manually perform regular analysis for different redirection modes.
- In-depth analysis: Performs in-depth analysis on peripheral problems based on key log processes.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

7 System Deployment

7.1 Flexible Deployment Mode

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

Huawei FusionAccess Desktop Solution supports multiple desktop cloud software/hardware deployment modes: appliance, standard, heterogeneous, and GPU passthrough.

In the deployment mode where the FusionStorage is used to provide storage resource pools, features such as shutdown restoration, storage delay to zero, live and cold storage migration, and iCache are unavailable. An appropriate deployment mode should be selected depending on customer requirements.

Benefits

Different deployment modes are provided to support different application scenarios and deployment scales of desktop clouds.

7.1.1 FusionCube

Version Requirements

Version 6.0 integrates the **Desktop Cloud Blade Appliance** and **Desktop Cloud Rack Appliance**, and supports the FusionCube appliance platform, which is the latest ultra converged infrastructure.

Summary

FusionAccess software can be deployed on FusionCube appliance platform, and the desktop cloud appliance solution is provided.

Feature Description

FusionCube has three modes: FusionCube 2000, FusionCube 6000 and FusionCube 9000.

The FusionCube2000: It is based on the RH2288H server. Generally, the 3.5"SATA disk is used as the main storage and the SSD card is used as the cache, which is cost-effective. The GPU is also supported.

FusionCube 6000: It is based on X6800 server. A 4 U subrack supports a maximum of four computing and storage converged blades. It uses the cost-effective SATA+SSD solution and is suitable for medium- and small-sized scenarios. It does not support GPU.

FusionCube 9000: It is based on E9000 server. A 12 U subrack supports a maximum of eight computing and storage converged/GPU blades, or 16 computing blades. It supports the deployment of computing blades. Computing blades and storage blades can be deployed in the same subrack. Computing blades and GPU blades can share the storage resources of storage and converged blades. FusionCube 9000 can be applicable to the GPU HD graphics processing scenario. It supports M60/K1/K2/K2200/K4200 GPUs, adopts SAS+SSD solution, and is suitable for large- and medium-sized scenarios that require high performance.

Specifications and constraints are as follows:

1. FusionCube 6000 supports GE and 10GE network modes, the GE network supports 3 subracks and 1000 users at most, and the 10GE network supports 24 subracks and 5000 users at most. FusionCube 9000 only supports the 10GE network with 8 subracks and 5000 users at most. FusionCube2000 supports GE and 10GE network modes. The GE network supports a maximum of 16 nodes, and the 10GE network supports a maximum of 264 RH2288H V3 servers in 22 cabinets.

2. FusionCube 6000 does not support GPUs. For scenarios that need GPUs, select FusionCube 9000 or FusionCube 2000. The supported GPUs include M60/K1/K2/K2200/K4200.

3. In appliance scenarios, if you want to enable the shutdown restoration function, FusionSphere 5.1U1 and later versions that match with FusionCube are required.

4. Appliance scenarios do not support **Secure Deletion** and cannot meet the requirements of projects that involve in **Secure Deletion** assessment for security industry. Therefore, the marketing is limited.

5. In an appliance scenario, cold data migration instead of hot migration is only supported between different FusionStorage storage pools.

6. FusionCube 9000 is transported without installing m60/K1/K2 GPUs, and the GPUs need to be installed onsite.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

7.1.2 FusionAccess Reference Architecture

Version Requirements

The FusionAccess Reference Architecture feature has been available since version 1.0.

Summary

The E9000 + IPSAN and RH2288H + IPSAN deployment modes support large-scale desktop deployment. A maximum of 20000 common virtual desktops are supported.

Dorado V3 all-flash storage is supported. For details about the desktop Dorado storage acceleration solution, see http://3ms.huawei.com/mm/docMaintain/mmMaintain.do?method=showMMDetail&f_id=STR170901380615505.

Feature Description

Standard VDI adopts the server + external storage mode. The following software is deployed in the standard VDI deployment mode: FusionCompute, FusionManager, and FusionAccess.

The E9000 + IPSAN and RH2288H + IPSAN deployment modes support large-scale desktop deployment. A maximum of 20000 common virtual desktops are supported.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

7.1.3 Software-Only Deployment Mode

Version Requirements

The Software-Only Deployment Mode feature has been available since version 1.0.

In version 6.0: ITA is deployed on the Linux operating system, and desktop management components are deployed on Linux.

Summary

FusionAccess is deployed on a third-party server, storage device, and switch.

Feature Description

The FusionAccess software is deployed on a third-party server, storage device, and switch. A maximum of 20,000 VMs can be deployed in heterogeneous deployment mode.

FusionAccess supports Huawei-developed servers including the RH2288H and E9000 to provide optimum performance. It also supports other heterogeneous servers. FusionCompute provides the heterogeneous capability.

Huawei-developed OceanStor S5500T, S2600T, S5800T, S6800T, and S5600 are supported in the IP SAN. The FusionAccess solution is compatible with the mainstreams third-party IP SAN storage devices available in the industry. FusionSphere provides the heterogeneous capability.

Desktop management components are deployed on Linux. The Linux ISO installation disk is provided, and components can be separately installed on Linux.

Interconnecting with Microsoft AD standard installation mode, ITA/WI/HDC/DB/License components can be installed on a single node (POC test scenario) and active-standby nodes by one-click (installAll).

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

7.1.4 CompactVDI

Version Requirements

The CompactVDI feature has been available since version 5.1.

Summary

CompactVDI adopts one to two RH2288H general servers as the basic hardware platform of the desktop cloud, and uses FusionSphere and FusionAccess to provide a simple task-based desktop solution for fewer than 100 users.

Feature Description

CompactVDI adopts one to two RH2288H general servers as the basic hardware platform of the desktop cloud, uses local server hard disks to provide storage capabilities, and uses FusionSphere virtual platform and FusionAccess software to provide virtual desktops for fewer than 100 users.

CompactVDI is suitable for medium- and small-sized scenarios that have simple service applications, require no personalized data and no high reliability.

Specifications and constraints on CompactVDI are as follows:

1. A maximum of two servers and 100 users are supported.

2. HA and storage redundancy is provided for management components. User VMs do not support hot migration and HA.

3. Capacity expansion is not supported.

4. The GPU feature is not supported.

Application Scenario

Windows Virtual Desktop	Application Virtualization
●	●

8 System Specifications

8.1 FusionAccess System Capacity Specifications

Availability

Standard Edition	SBC Standard Edition	Advanced Edition
●	●	●

Introduction

This section provides the system capacity specifications of Huawei FusionAccess desktop cloud solution.

Benefits

With knowledge of the system capacity specifications of Huawei FusionAccess, customers will select an appropriate deployment mode in a specific scenario.

8.1.1 System Capacity Specifications of Virtual Desktops

Version Requirements

The system capacity specifications of virtual desktops have been available since version 5.0.

Summary

This section provides the system capacity specifications of Huawei FusionAccess desktop cloud solution. The capacity specifications are helpful for desktop system design and deployment mode selection.

Feature Description

Huawei FusionAccess supports a maximum of 20,000 virtual desktops. The detailed specifications are as follows.

FusionAccess Management Capacity	Value (Reference Architecture)	Reference (Appliance)
Maximum number of users supported by a FusionAccess	20,000	5,000
Maximum number of HDCs supported by a FusionAccess	16	16
Maximum number of users supported by an HDC	5000	5000
Maximum number of concurrent login users supported by an HDC	10 users/second	10 users/second

Virtual Desktop Specifications	Value
Number of VCPUs per VM	1 to 64
Memory size per VM	1 GB to 4 GB (32-bit) 1 GB to 512 GB (64-bit)
Number of virtual interface cards (NICs) per each VM	1 to 12
Number of attached volumes per VM	1 to 11 (at least one system volume)
System disk capacity	5 GB to 2 TB
User disk capacity	1 GB to 2 TB
Desktop color depth	24-bit/32-bit
Maximum resolution	3840x2160

For Other specifications, see the *Huawei FusionAccess V100R006C10 System Specifications List*.

Application Scenario

Windows Virtual Desktop
●

9 Acronyms and Abbreviations

A	
AD	active directory
AG	access gateway
B	
BIOS	basic input/output system
C	
CA	certificate authority
CPU	central processing unit
D	
DHCP	Dynamic Host Configuration Protocol
DPM	dynamic power management
DVI-D	digital visual interface-digital
F	
FPS	frames per second
FQDN	full qualified domain name
FusionAccess	FusionAccess
FusionCompute	FusionCompute
FusionManager	FusionManager
FusionSphere	FusionSphere
H	
HA	high available
I	
IMGS	image server

IO	Input/output
IOPS	input/output operations per second
IP SAN	IP storage area networks
ISO	International Organization for Standardization
K	
KPI	key performance index
L	
LAN	local area network
LDAP	Lightweight Directory Access Protocol
LTE	Long Term Evolution
M	
MCNA	main compute node agent
N	
NAS	network attached storage
O	
OSS	operations support system
P	
PID	product ID
PV driver	paravirtualized driver
Q	
QoS	quality of service
R	
RAID	redundant array of independent disks
RDP	Remote Desktop Protocol
REL	Release
REST	Representational State Transfer
RPO	recovery point object
RTO	recovery time object
S	
SAN	storage area networks
SIM	subscriber identity module
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer

SSO	single sign-on
T	
TC	thin client
TSM	terminal security management
V	
vCPU	virtual central processing unit
VDA	virtual desktop agent
VDI	virtual desktop infrastructure
VGA	video graphic adapter
VID	vender ID
VLAN	virtual local area network
VNC	virtual network computing
VoIP	Voice over Internet Protocol
VPC	virtual private cloud
VPN	virtual private network
W	
WI	web interface
WIFI	wireless fidelity