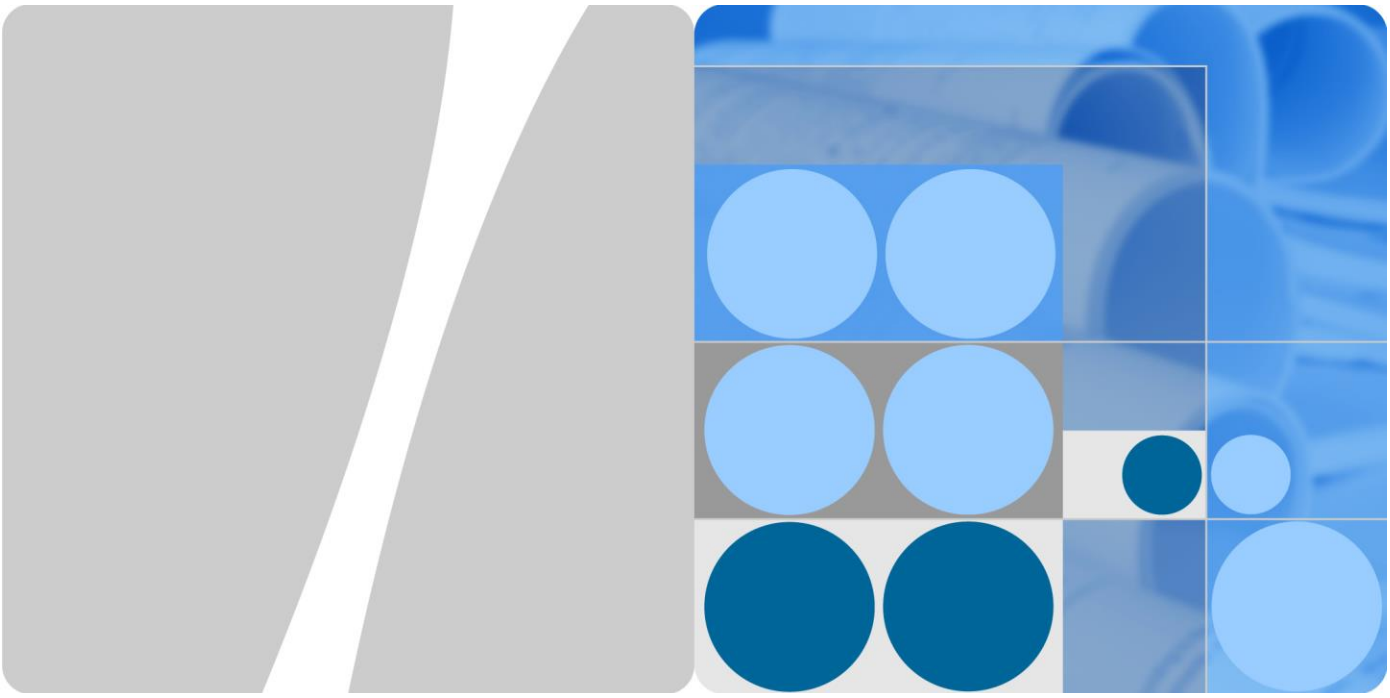


Agile Controller-Campus V100R002C10

High Reliability Technology White Paper

Issue	**01**
Date	**2016-04-15**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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 Overview

1.1 Product Overview

The Agile Campus-Controller is deployed on an enterprise campus network to provide policy control and collaborative security defense on the entire network. With a unified policy engine, the Agile Controller-Campus implements unified access control in an organization. It provides authentication and authorization for various terminals based on user information, terminal type, access time, access location, and access mode. In addition, the system provides guest management throughout the whole visiting process to allow guests to get network access anytime, anywhere. This helps improve work efficiency of guests, improve enterprise brand image, and reduce O&M workloads of the IT system.

The Agile Controller-Campus provides the following basic functions:

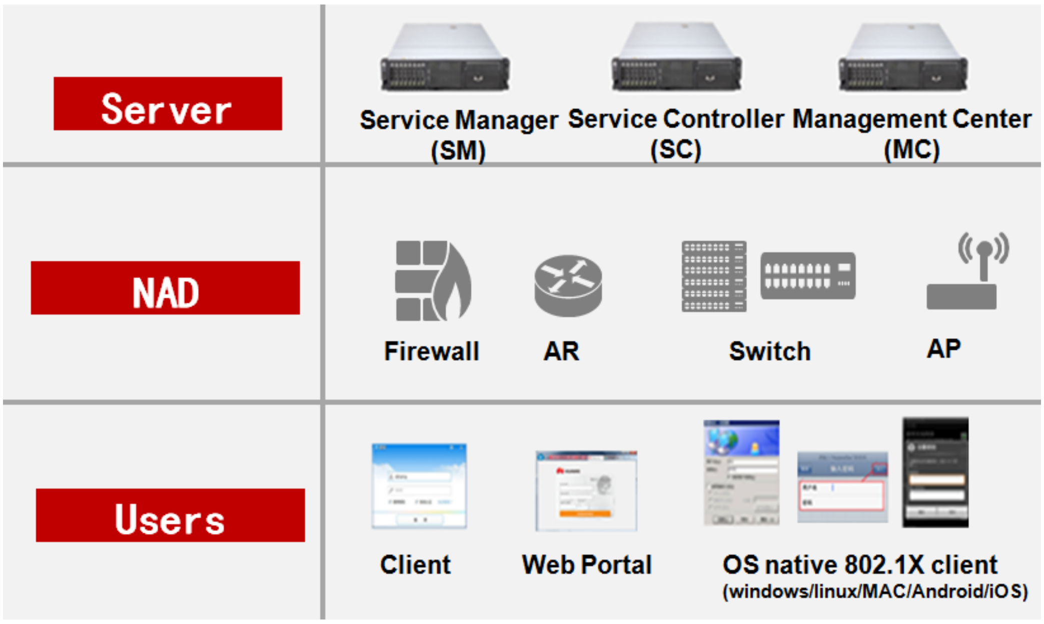
1. Network admission control: Provides multi-dimensional network access control function. It combines user identity, terminal type, access location, access time, and terminal compliance check result to form flexible network access authorization policies. Multiple network access control solutions are provided based on customers' network requirements. In a wired local area network (LAN), the 802.1X access control solution is provided. On a core network, the access control solution based on the Huawei security access control gateway (SACG) is provided. On a wireless network, the 802.1X access control solution based on 802.11i and guest access control solution based on Portal are provided. In a BYOD scenario, the Agile Controller-Campus flexibly manages authentication and authorization policies to support multi-dimensional access control, meeting service control requirements of different customers.
2. Free mobility: Provides a permission control model based on security groups. The administrator can divide access users and server resources into security groups and directly define user permissions to access resources based on security groups, ensuring experience of VIP users at the campus egress.
3. Guest management: Provides the guest management function to support full lifecycle guest management, implementing uniform management of guest application, approval, distribution, authentication, and deregistration.
4. Service chain: Defines service flows and service chain policies based on IP zones and security groups. Cooperated with Huawei agile switches, the Agile Controller-Campus

directs different network flows to different service devices for processing based on service needs.

5. Terminal security management: Provides terminal security policy management, including compliance check and security compliance monitoring.

1.2 Component Overview

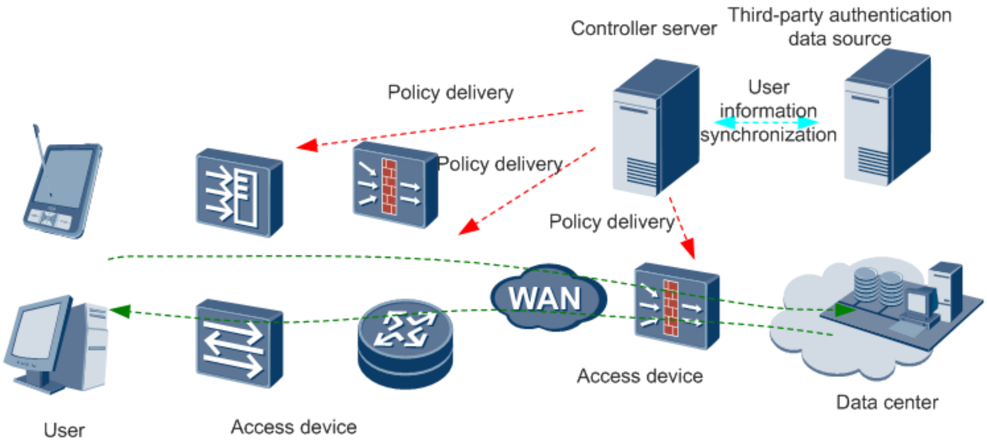
The Agile Controller-Campus is composed of the following components:



1. Service Manager (SM): The SM is responsible for service configuration and management such as user management, policy management, and log management of the Agile Controller-Campus. A single set of Agile Controller-Campus system has only one SM.
2. Management Center (MC): When the Agile Controller-Campus adopts the hierarchical deployment mode, an MC component must be deployed in the upper-level headquarters. The lower-level Agile Controller-Campus system registers to the upper-level MC. The MC can uniformly perform license management, terminal security policy template delivery, patch distribution policy template delivery, and software distribution tasks.
3. Service Controller (SC): The SC is responsible for interconnection with terminals or devices. A single set of Agile Controller-Campus system can have multiple SC components. The SC component can be installed on multiple servers to provide the following functions:
4. Authentication server: Manages terminal security and provides firewall-based access control service. A single set of Agile Controller-Campus system supports a maximum of 50 authentication servers.
5. Portal server: Uses the Portal protocol to provide the admission control service. A single set of Agile Controller-Campus system supports a maximum of 50 Portal servers.
6. RADIUS server: Uses the RADIUS protocol to provide the admission control service. A single set of Agile Controller-Campus system supports a maximum of 10 RADIUS servers.

7. Network server: Manages network devices and provides the free mobility and service chain functions. A single set of Agile Controller-Campus system supports at most two network servers, only one of which works properly.
8. Database: stores local account information and key service data of the Agile Controller-Campus. The current version uses Microsoft SQL Server database.
9. AnyOffice client: Is an authentication client and supports Windows XP and later operating systems. Users can use the AnyOffice client, standard 802.1X client, or mainstream browser for network access authentication.

To form a complete agile network solution or NAC solution, the Agile Controller-Campus needs to associate with network devices to support user-based access control and free mobility policies. In addition, the Agile Controller-Campus needs to associate with a third-party identity authentication source (such as the AD/LDAP/RSA SecureID server) in specific deployment scenarios. The following figure shows the association between the components.



2 Reliability Design

2.1 Reliability Solution Overview

On a network, the Agile Controller-Campus acts as the network admission authentication server and provides identity authentication, network admission control, and access rights control. Therefore, reliability of the Agile Controller-Campus is critical to the network. The Agile Controller-Campus provides component-level and solution-level reliability designs to ensure high reliability.

2.2 Component-level Reliability Solution

2.2.1 SC Reliability

The SC component of the Agile Controller-Campus includes authentication server, Portal server, RADIUS server, and network server, and the SC servers can be deployed in N+1 mode. After determining the number of SC servers based on the number of terminals, deploy an additional SC server as a backup. When either of the authentication server, Portal server, RADIUS server, and network server fails, the SC service can be switched to the backup SC server to ensure service continuity.

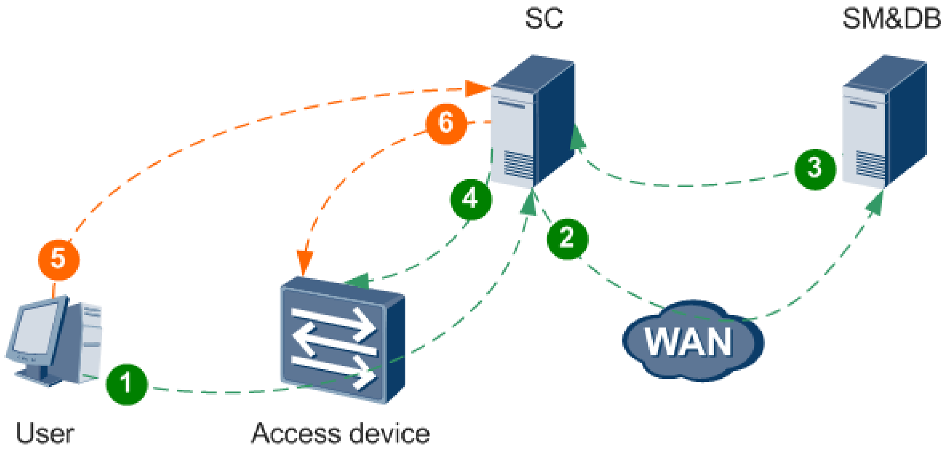
The backup implementation of SC servers is as follows:

- Authentication server: The authentication server provides the terminal security service and security access control gateway (SACG) service. If the authentication fails, users cannot be authenticated and cannot use intranet resources. You can specify the active and standby authentication servers on the SM. When the active authentication server fails to provide service, AnyOffice on a terminal can detect interruption of the heartbeat between the terminal and active authentication server. AnyOffice then switches to the standby authentication server for re-authentication, ensuring continuity of the terminal security service. You can specify the IP addresses of the active and standby authentication servers on an SACG firewall. When the firewall detects interruption of the heartbeat between itself and the active authentication server, the firewall connects to the standby authentication server to maintain continuity of the SACG service.

- Portal server: The Portal server provides Portal authentication. You can specify IP addresses of multiple Portal servers on a Portal gateway for Portal server backup. When the active Portal server fails or becomes unreachable due to a network failure, the Portal gateway connects to a standby Portal server. In addition, Huawei Portal gateways support the escape mechanism. After this function is enabled, a gateway can grant network access permission to users if the Portal server stops providing service. This mechanism prevents service interruption caused by a Portal server failure.
- RADIUS server: The RADIUS server provides RADIUS authentication. You can specify IP addresses of the active and standby RADIUS servers on a Huawei device. When the active RADIUS server fails, the device forwards authentication requests to the standby RADIUS server to ensure continuity of the RADIUS authentication service.
- Network server: The network server manages network devices and provides the free mobility and service chain functions. You can specify the active and standby network servers on the SM. The active network server provides service, whereas the standby network server does not. When the SM detects that the active network server has failed, the SM sets the standby network server to the active state.

2.2.2 Key Service Data Caching on the SC

The SC component (including the authentication server, Portal server, RADIUS server, and network server) of the Agile Controller-Campus can cache key service data, such as user accounts and configuration information. When the network connection between the SC and the database server is interrupted or the database fails, the SC obtains service data from the cache to ensure uninterrupted services.



The working process of the SC server cache mechanism is as follows:

1. During the first authentication, a user sends an authentication request to the local SC server.
2. The local SC server does not save any information about the user, so it forwards the authentication request to the Agile Controller-Campus server in the headquarters.
3. The Agile Controller-Campus server in the headquarters checks validity of the user. If the authentication succeeds, the Agile Controller-Campus server sends an authentication success message and policies for the user to the local SC server.
4. The local SC server requests the network access device to grant network access permission to the user, and saves the account and policy parameters of the users in the cache.

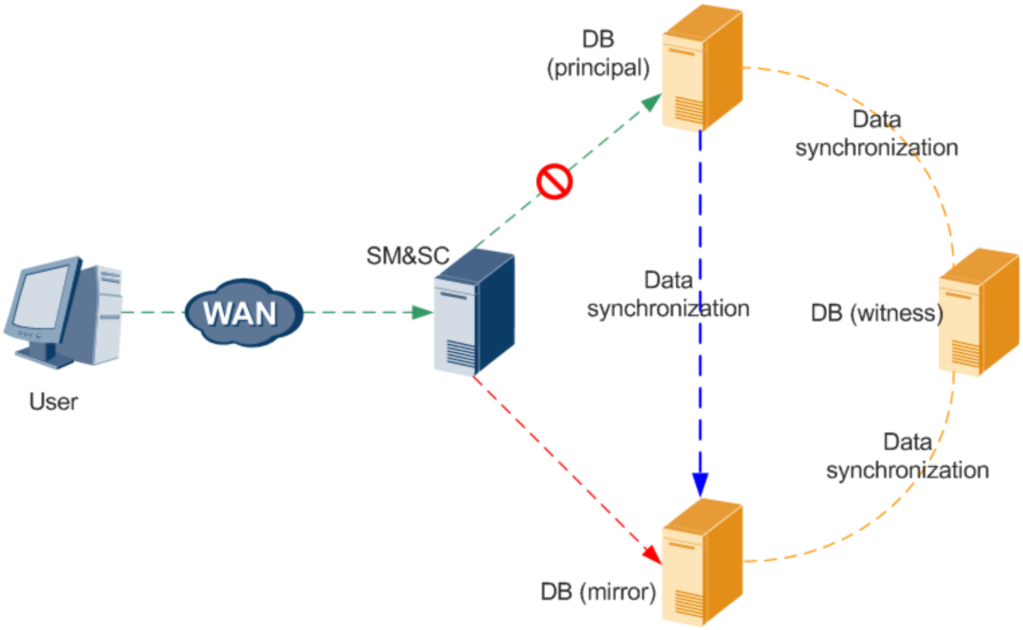
5. When the user connects to the network again, the user sends an authentication request to the local SC server.
6. The local SC server first searches the cache for the user information. After authenticating the user, the local SC server requests the network access device to grant network access permission to the user.

2.2.3 Database Reliability

Local account data and service configuration data of the Agile Controller-Campus are all saved in the database. Therefore, the database must use a high reliability design to prevent service failures on the Agile Controller-Campus.

The Agile Controller-Campus supports Microsoft SQL Server and Oracle databases, which provide the database mirroring and Real Application Clusters (RAC) functions respectively to ensure database reliability.

SQL Server Database Reliability



Databases of the Agile Controller-Campus use the mirroring function of SQL Server to ensure high database reliability. When the principal database fails, the system automatically switches services to the mirror database.

Database mirroring maintains two copies of a database, which must reside on different server instances of SQL Server Database Engine. Generally, the server instances reside on computers at different locations. Starting database mirroring establishes a database mirroring session between the server instances.

One server instance acts as the principal server and serves the clients. The other server instance acts as a hot or warm standby server (mirror server) depending on the configuration and state of the database mirroring session. When the database mirroring session is synchronized, database mirroring provides a hot standby server that supports rapid failover without a loss of data from committed transactions. When the database mirroring session is not synchronized, the mirror server typically acts as a warm standby server (with possible data loss).

The principal and mirror servers communicate and cooperate as partners in a database mirroring session. The two partners perform complementary roles: principal and mirror. At any given time, one partner performs the principal role, and the other performs the mirror role. The partner that owns the principal role is known as the principal server, and its copy of the database is the current principal database. The partner that owns the mirror role is known as the mirror server, and its copy of the database is the current mirror database. When database mirroring is deployed in a production environment, the principal database is the production database.

Database mirroring needs to redo every insert, update, and delete operation that occurs on the principal database onto the mirror database quickly. Redoing is completed by sending a stream of active transaction log records to the mirror server, which applies log records to the mirror database in sequence, as quickly as possible. Unlike replication that works at the logical level, database mirroring works at the physical log record level. Since SQL Server 2008, the principal server compresses the stream of transaction log records before sending it to the mirror server. This log compression occurs in all mirroring sessions. Database mirroring enables automatic service failover to the mirror database upon a failure of the principal database.

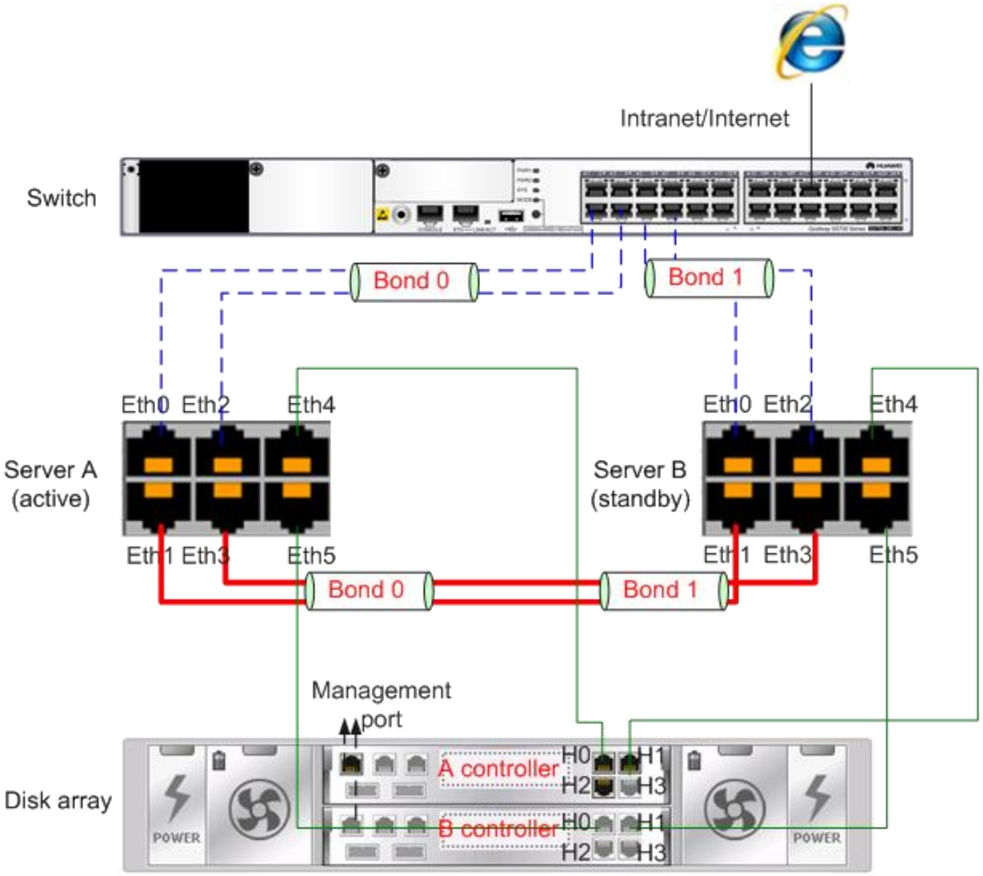
Oracle Database Reliability

Oracle database uses the RAC function to provide high reliability.

The RAC function requires at least two Oracle database servers and one disk array shared storage device for database load balancing. If one database server fails, the database service can seamlessly switch to the other database server.

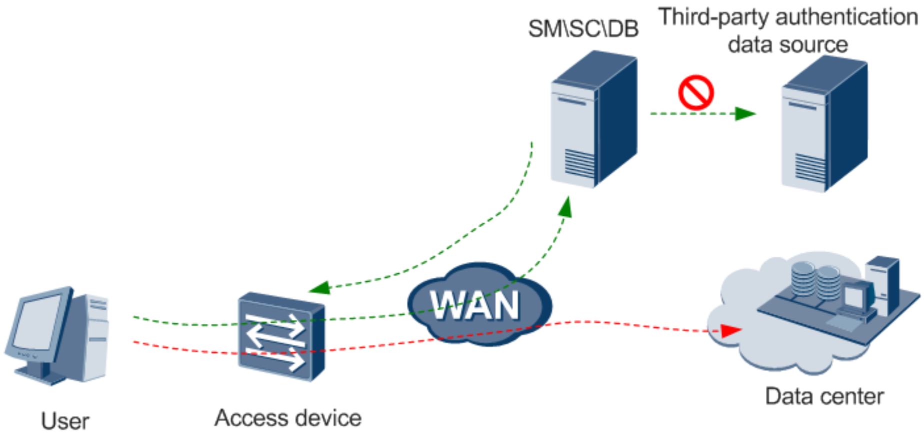
In the recommended RAC networking shown in xxx, two servers work in active/standby mode to improve reliability. Eth 0 and Eth 2 are bound into Bond 0, whereas Eth 1 and Eth 3 are bound into Bond 1. Bond 0 is connected to a switch, and Bond 1 is the heartbeat interface between the two servers. The switch is connected to an intranet or the Internet and provides users with access to the servers.

Eth 4 and Eth 5 are connected to service interfaces on two controllers on the disk array to enable servers to access data stored in the disk array.



2.2.4 External Data Source Reliability

The Agile Controller-Campus can synchronize LDAP account information from an external data source server for local authentication. Because the Agile Controller-Campus only synchronizes account names without passwords, the accounts still need to be authenticated by the LDAP server. The Agile Controller-Campus can also use the LDAP protocol to send account information to the LDAP server for identity authentication. If the LDAP server fails or becomes unreachable due to a network failure, the authentication and admission control services on the Agile Controller-Campus are interrupted.



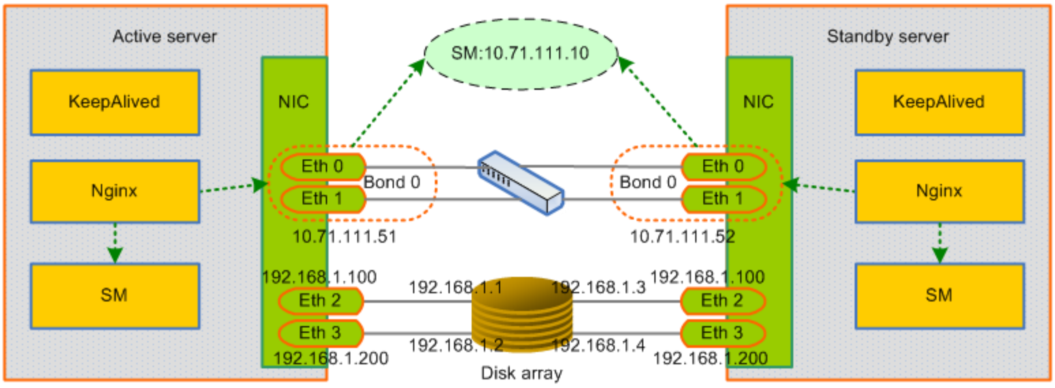
To enhance reliability of the authentication and admission control services, the Agile Controller-Campus supports backup of external data source servers. When the Agile

Controller-Campus detects a failure of the active LDAP server, it switches the authentication service to the standby LDAP server.

2.2.5 SM/MC Reliability

The SM/MC servers running the Linux but not Windows operating system support high availability design.

SM/MC reliability is ensured by the active/standby networking, and Keepalived cluster software is used to implement switchover between active/standby SM/MC servers. Keepalived performs health check for applications, sets and monitors bound network adapters, and provides a virtual IP address to external users. When Keepalived detects application down on the active server, Keepalived re-elects a new active server and directs requests to the virtual IP address to the new active server. The IP address configured on the SM (subordinate node of the MC) and SC (subordinate node of the SM) must be the virtual IP address provided by Keepalived.



- During the SM/MC installation, the database system provided by the customer must be specified for the database connection.
- Two servers are deployed in active/standby mode and connected to the same shared disk array. The SM is installed on both servers.
- Bonding technology is used to bind two network adapters.
- The shared disk array uses two network adapters and ensures network reliability through the multipathing software.
- Keepalived technology is used to provide a virtual IP address to external users.
- Ngnix technology is used to implement load balancing between servers.
- Rsync technology is used to synchronize files between the SM and SC.
- The SM/MC uses the shared disk array for file sharing. The file paths on the active/standby SM/MC servers must be the same.
- The customer can use network attached storage (NAS) to substitute the shared disk array.

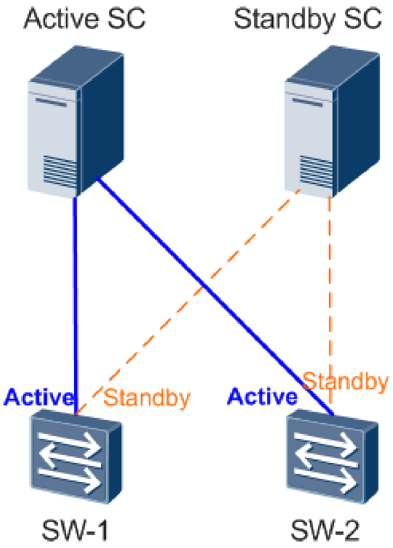
2.3 Solution-Level Reliability Solution

Different solution-level reliability solutions are provided for association between the Agile Controller-Campus servers and network devices.

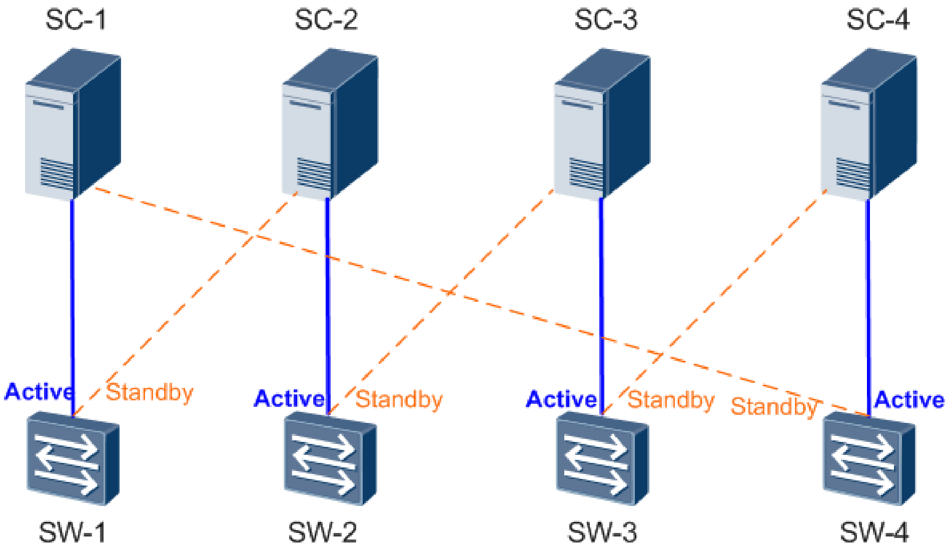
2.3.1 N+1 Server Backup Solution

When the Agile Controller-Campus works with network devices like switches and WLAN devices, it provides RADIUS and Portal server capabilities. Switches and WLAN devices support 1+1 backup of RADIUS/Portal servers, so the Agile Controller-Campus server can be deployed in 1+1 or N+1 mode to enhance reliability.

1. In small- and medium-scale scenarios, the 1+1 deployment is recommended for the Agile Controller-Campus servers. The active SC server is specified as the active RADIUS/Portal server for all the switches and WLAN devices, and the standby SC server is specified as the standby RADIUS/Portal server. If the active SC server fails or becomes unreachable due to a network failure, the switches and WLAN devices switch to the standby SC server. Users who have been authenticated before the switchover are not affected and still online after the switchover. Subsequent users are authenticated by the new active SC server.



2. In large-scale scenarios, the N+1 deployment is recommended for the Agile Controller-Campus servers due to limitation of server performance. Specify different active and standby RADIUS/Portal servers for switches and WLAN devices based on the number of users connected to the devices and locations of the devices. When any SC server fails or becomes unreachable due to a network failure, the associated switches and WLAN devices can switch to another SC server to prevent interruption of the authentication service.



2.3.2 Escape Mechanisms

If both the active and standby SC servers fail or become unreachable because of network failures, switches and WLAN devices can use escape mechanisms to ensure service availability.

1. Critical VLAN solution: In 802.1X authentication, if the Agile Controller-Campus server breaks down or the network becomes unreachable, users cannot normally access network resources, affecting services. Critical VLAN can be configured on 802.1X switches to solve this problem.

   After 802.1X authentication is enabled on a switch, the switch sets up a heartbeat connection with the RADIUS server. If the heartbeat connection is broken, the switch adds user access interfaces to the critical VLAN. Users can then use network resources in the critical VLAN without authentication.

2. Authentication event solution: You can run the **authentication event authen-server-down user-group** *xxx* command on a switch to configure it to add terminals to a specified user group after detecting a RADIUS server Down event. The Agile Controller-Campus then assigns temporary network access rights to the user group.

3. Portal escape solution: When a switch or WLAN device works with the Agile Controller-Campus as a Portal gateway, you can enable Portal probe and escape on the Portal gateway. When the connection to the Portal server or the Portal server itself fails, users under the Portal gateway can still connect to the network and have certain network access rights. In addition, the Portal gateway generates logs and traps for the network failure or Portal server failure. Besides, the user information synchronization mechanism ensures that user information on the Portal server is the same as that on the gateway, preventing re-authentication.

NOTE

For details on the dependency of the models and versions of switches and WLAN devices for the reliability solutions, see the *Specification List*.