H3C SeerEngine-WAN Controller

Release Date: July, 2020

New H3C Technologies Co., Limited
Product overview

Wide area networks (WANs) have long served the sole purpose of connecting geographically dispersed locations. Independent of application systems, traditional WANs are primarily managed from the perspective of network nodes instead of applications.

As cloud computing grows rapidly and gains large-scale deployments, enterprises are increasingly moving their on-premises IT systems to the cloud. Wherever the applications are located, users want to have the same experience. Traditional WAN architectures can hardly address these challenges because of their complexity, rigidity, and lack of programmability. To align with the business growth in this cloud computing era, enterprises must transform their WAN architectures.

H3C Application-Driven WAN (AD-WAN) is an open, programmable, and scalable architecture. Using innovative H3C SeerNetwork Architecture (SNA) designed for digital networks, AD-WAN enables not only network wide unified network management, control, and analytics, but also provides a user-oriented, unified portal for end-to-end orchestration and unified service orchestration across networks.

As the core component for control and analytics, SeerEngine-SDWAN manages zero-touch deployment and onboarding of devices, automated service deployment, and traffic engineering policy deployment.

Features and benefits

ZTP

SeerEngine-SDWAN provides multiple zero touch provisioning (ZTP) capabilities. ZTP allows network devices to come online and obtain configurations automatically. This reduces the deployment cost and risks of misoperations. AD-WAN supports ZTP via USB or URL.

- **ZTP via USB**

  The network administrator imports information about devices to deploy, such as device names and serial numbers, to the SeerEngine-SDWAN controller, writes configuration files to USB drives, and transports the USB drives and devices to branches.

  The onsite installer inserts the USB drives into the devices and powers on the devices. After loading information required for registration, such as WAN connectivity and controller information (for example, controller address and password), the
devices attempt to register on the controller.

- **ZTP via URL**

  The network administrator imports information about branch sites and devices into the SeerEngine-SDWAN controller. The onsite installer obtains the ZTP URL from the network administrator through an email. Opening this URL redirects the devices to the SeerEngine-SDWAN controller to automatically obtain WAN interface, network access, and VPN settings, and information about the controller. Then, the devices try to register on the controller, and the controller deploys underlay network settings to the devices automatically after successful registration.

**Automated service deployment**

H3C SeerEngine-SDWAN supports automated deployment of VPN, LAN, and QoS services across the entire network, and provides the following features:

- Defining applications based on the IP 5-tuple, DSCP, VPN information, and application-layer packet characteristics.
- Defining policies based on route selection, bandwidth, and service quality requirements (delay, jitter, and packet loss rate) and the time range.
- One-key deployment of configurations from SeerEngine-SDWAN.

**VPN service deployment**

After a device comes online through ZTP, the SeerEngine-SDWAN controller deploys IPsec tunnel settings automatically, depending on whether the WAN interface of the device has an Internet link present. It can also deploy VXLAN tunnels over physical networks using different WAN links and provide undifferentiated scheduling services.

At the LAN side, VPNs are deployed to isolate services of users.

**LAN service deployment**

The SeerEngine-SDWAN controller supports automated deployment of a complete set of Layer 3 gateway configurations to LAN access networks based on user-defined LAN service settings and network planning without manual intervention. If a Layer 3 gateway already exists in a branch, you only need to deploy IP addresses for the LAN interfaces on the branch devices from the controller.

**LAN Network Creation**
- Network segment allocation
- VLAN assigned

**LAN Business Management**
- Automatically deploy DHCP
- Each service can be bound to different VLAN

**LAN Side Routing**
- Automatically deploy IGP routing
QoS service deployment

SeerEngine-SDWAN supports application group-based bandwidth limit. The bandwidth limit settings are issued to LAN interfaces of the network devices.

- If the bandwidth leased from the service provider is smaller than the interface bandwidth, you can configure bandwidth limit for WAN interfaces on the device management page to prevent the excessive traffic from being dropped at the service provider side.
- If multiple applications are running on the network and congestion occurs, you can apply a bandwidth guarantee policy on the application policy page to ensure that high-priority applications can obtain guaranteed bandwidth and low latency.
- You can dynamically adjust the bandwidth limit settings according to the actual network conditions to guarantee enough bandwidth for high-priority services on the network.

Intelligent and flexible traffic engineering

SeerEngine-SDWAN supports multiple types of link selection policies for traffic engineering.
● **Link based**—Selects a link based on the bandwidth usage and link priority defined by link color. When the bandwidth usage on a link exceeds the threshold, the device automatically switches the traffic to another qualified link based on the TE policy issued by the controller.

● **Quality based**—Selects a link based on the latency, packet loss rate, and jitter of the links. When the link latency exceeds the threshold, the device automatically switches the traffic to another qualified link based on the TE policy issued by the controller.

● **Time range based**—Selects a link based on time ranges. This type of link selection allows for periodic traffic engineering so that high-priority applications can always obtain high reliability in specific time ranges.

● **Combination of multiple policies**—Defines a set of policies for a service. For example, for real-time services such as video conference, you can configure a comprehensive policy based on latency, packet loss rate, bandwidth usages, etc., to guarantee ultimate user experience.

**Network visibility**

SeerEngine-SDWAN uses network information collection and data drilldown technologies to provide global and multi-dimensional visibility to facilitate O&M, including the following:

● **Application traffic visibility**—Provides users with real-time information about services, including bandwidth information, traffic information, and health status.

**Global resource monitoring**

Network topology management provides the network topology from different perspectives.

- **Converged topology**—Displays the topology of all network devices managed by the SeerEngine-SDWAN controller.
Dashboard—Displays the state and physical location information for network devices on a map.

Value-added service

SeerEngine-SDWAN supports WAN optimization technologies Web caching and WAAS.

- **Web caching**—Implemented by storing reusable HTTP and HTTPS responses and documents such as apk and doc files in the cache to make subsequent requests faster.
- **WAAS**—Allows you to define actions to perform on applications to improve the performance of applications on a WAN.
High availability

- Dual gateways in a site
  You add devices to a site and add interfaces of the devices to a LAN service network for service deployment. If you enable VRRP, the system can provide gateway high availability. If the LAN interface working mode is set to bridge, you can select the access or trunk link type.

- 2+1 light disaster recovery
  You deploy a controller cluster for 2+1 disaster recovery. When the controller cluster splits and only one controller member is left active, the controller member will enter emergency mode in five minutes. In emergency mode, you can log in to the controller to view services but cannot create, edit, or delete services. When only one controller member is active, you can use the standby member to replace any failed member to rebuild the cluster with the active controller.

Running environment

<table>
<thead>
<tr>
<th>CPU</th>
<th>Memory</th>
<th>Disk</th>
<th>NIC</th>
</tr>
</thead>
</table>
| x86-64 (Intel64/AMD64), 2 4-core, 2.6GHz processor or higher | 64GB or higher | RAID controller: 1GB cache, with data protection upon power failures. Use either of the following hard drive specifications:  
  - 1TB (or higher) SAS SSD or NVMe SSD.  
  - 2 × 1TB (or higher) 7.2K RPM SATA/SAS drives, with RAID1, RAID5, or RAID10 configured. The capacity of the RAID array must be not less than 1 TB. | 2 × 1Gbps or higher NICs that support Linux NIC bonding in mode 2 or mode 4. |
# Ordering Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>H3C SeerEngine WAN Software Additional 1 Server Node License</td>
<td>Required.</td>
</tr>
<tr>
<td>H3C SeerEngine WAN Software Additional 1 Branch Access NE License</td>
<td>Optional.</td>
</tr>
</tbody>
</table>