SD-WAN Headend Design Guidelines

For supported software information, click here.

This article provides architectural and deployment guidelines for the Versa Networks headend components. The headend consists of a Versa Analytics cluster, a Versa Director, and a Versa Controller.

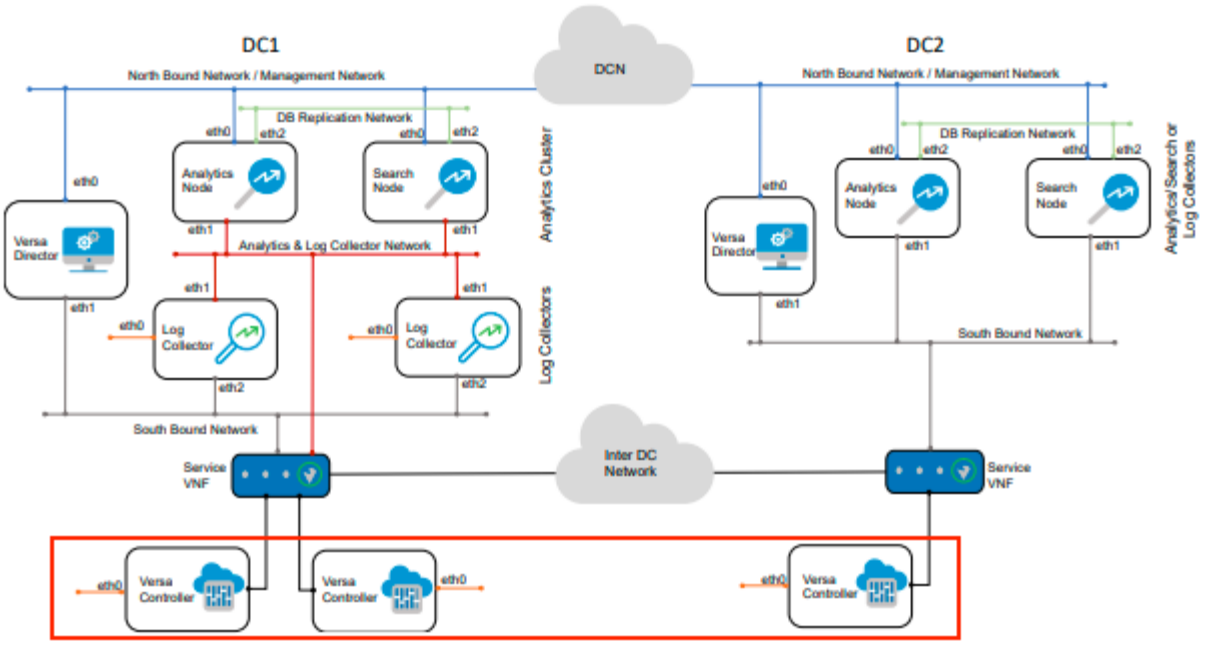
Design Considerations for Headend Architecture

A typical Versa SD-WAN headend architecture is fully resilient, providing geographical redundancy. When you deploy the headend in a public cloud, you deploy it in different availability zones. For these types deployments, the infrastructure must provide the capability for interconnectivity among the headend components.

The SD-WAN headend topology has the following components:

- Northbound segment, for management traffic
- Southbound segment, for control traffic
- Service VNF router to interconnect data centers

The following figure illustrates the headend components, which shows a topology that has headend components in two geographically separated data centers.



Administrators and other OSS systems use the northbound network to access the Versa Director, Analytics GUI, and REST APIs. The northbound network is also used to maintain synchronization between Versa Directors in a high availability cluster. Controller nodes require the northbound network to connect to Versa Director over the out-of-band (eth0) interface so that the Versa Director can provision the Controller nodes.

The southbound network, or control segment, connects to the SD-WAN overlay through the Controller nodes. Because the Director and Analytics nodes are hosts and not routers, the topology requires an additional router to provide a redundant connection to both Controller nodes. A dynamic routing protocol (either OSPF or BGP) must be enabled on this router to provide accurate overlay IP prefix reachability status, and BFD must be enabled towards the service VNF device in the data center. This additional router can be an existing router in the data center network, or it can be a VOS edge device managed by Versa Director.

The solution assumes reachability between the data center networks over the Director northbound operations support system (OSS) network. If the control network service router experiences an outage, the Director node can be accessible using the northbound network, and and the administrator can gracefully fail over to the standby Director node.

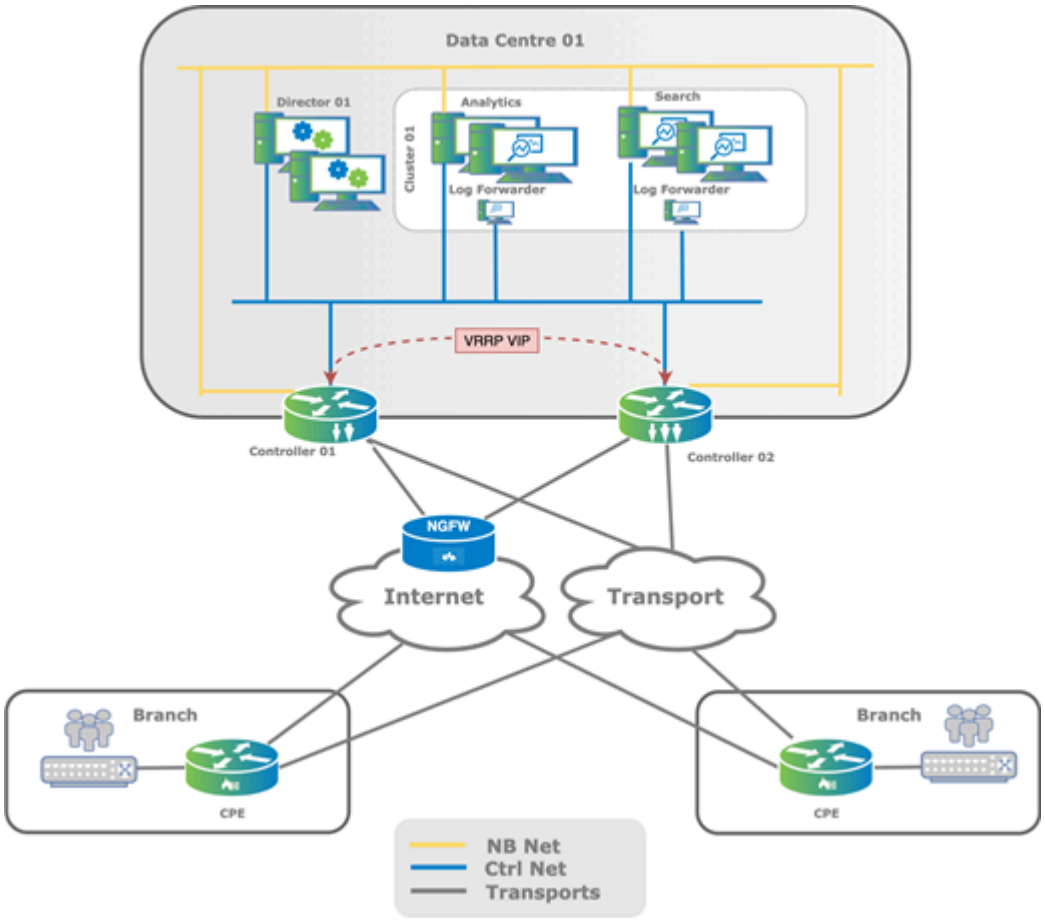
Note: It is not mandatory to always have the Controller nodes connect to all transport domains. Technically, the SD-WAN network can function if an SD-WAN branch device is connected to the Controller node over just one underlay. However, from a resiliency point of view, it is recommended that the Controller node connect directly to all the transport domains that you use.

Note: The Director northbound OSS network must be separate from the control network to avoid the possibility that a split-brain state arises between the Director nodes. In a split-brain scenario, both Director nodes are up but network reachability between them is lost. The results is that both Director nodes assume that they are the active nodes.

If internet access is enabled to the Versa Director then you must secure the northbound traffic with appropriate security.

Where users are able to access Versa Director directly from the internet such as the cloud-hosted Versa Directors, you must use a third dedicated interface into a DMZ. This allows separation between the link used for Director Sync and the user internet access to the Director.

The following figure shows a simple single data center deployment that is not geographically dispersed and in which service VNF routers are not required. This topology uses flat Layer 2 LANs for both the northbound and control networks, and it uses VRRP in the control LAN for gateway redundancy. However, this design is not suitable for creating Layer 3 security zones at the headend. If security is required, you must configure firewalls in bridge mode.



Headend Deployment Options

You can deploy the typical headend architectures shown above as host OSs on physical hardware, which is called a bare-metal deployment. You can also deploy these headend architectures in a virtualized architecture, for which Versa Networks supports ESXi and KVM, and the AWS, Azure, and Google Cloud Platform public clouds.

Deploying the headend on bare-metal hardware provides better performance and scalability, typically, 20 to 30 percent over a virtualized architecture. However, deploying on physical hardware has hardware dependencies. For example, not all server hardware, such as special RAID controllers, is supported.

For both bare-metal and virtualized deployments, it is important to follow the hardware requirements described in Hardware and Software Requirements for Headend.

Firewall Dependencies for Headend Deployment in a Data Center

When you implement the headend in an existing data center, several protocols and functions are required to connect to the data center. You must follow the requirements for connectivity, reachability, and security. For more information on firewall requirements, see Firewall Requirements.

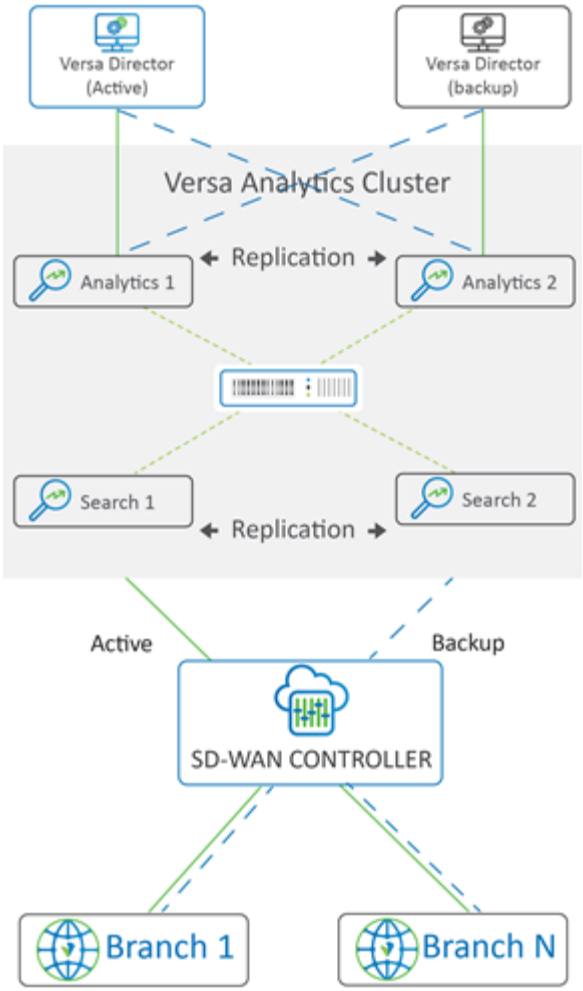
Best Practices for Hardening the Headend

If you deploy Versa Directors that are exposed to the internet so that external users can access them, you must apply additional by using common IT hardening practices. This includes installing Ubuntu OS patches, installing official certificates (Versa Networks software ships with self-signed certificates), and changing the default passwords. Note that you must use the OS patches provided by Versa and not install OS patches directly from Ubuntu.

For more information, see the system hardening articles.

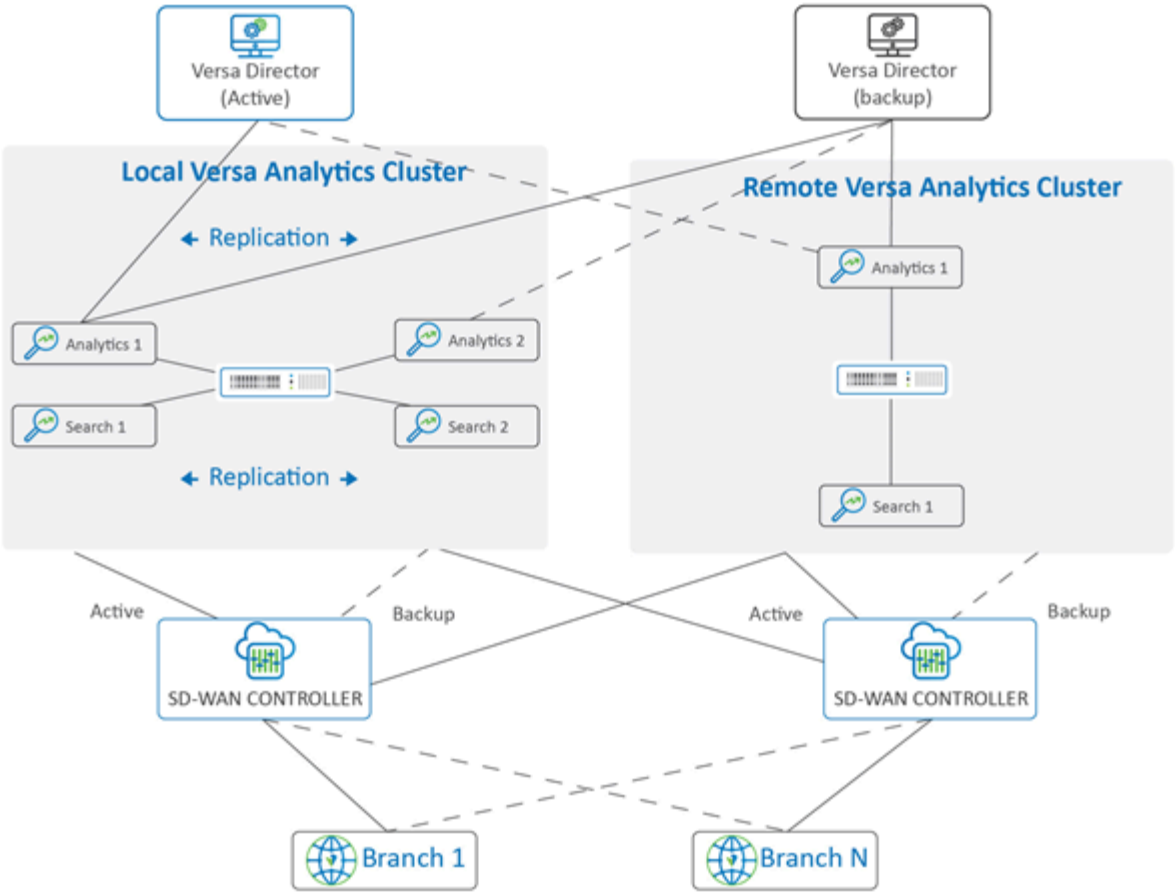
Versa Analytics Deployment Options

The minimum recommended Versa Analytics deployment for full redundancy requires a cluster of four Analytics nodes, as illustrated in the figure below. This design provides active-active high availability (HA), with two nodes having the Search personality and two nodes having the Analytics personality. Redundancy is achieved by replicating the data between one or more nodes of the cluster. Because there is a large amount of data movement between the nodes of the cluster, the network latency must be low for the best storage and query performance. Therefore, it is recommended that you allocate the nodes of the same cluster in the same data center, or at least within the same availability zone. Note that synchronization of the Cassandra database requires less than 10 milliseconds of latency between the nodes in the same cluster.



Recommended Production Analytics Deployment

To provide geographical resilience and also to provide disaster recovery, you can add a second Versa Analytics cluster, as illustrated in the following figure below. The second cluster can have either the same number of nodes as the main cluster or a different number of analytics and search nodes. For disaster recovery, you typically use a smaller Analytics cluster that is activated only if the primary site fails. Note that when you use clusters of different sizes, it is important to check that that the smaller cluster can accommodate the number of LEF connections from the branches.



It is recommended that your topology have a backup Analytics cluster for disaster recovery. If the active Analytics cluster goes down, the backup continues to process the logs and statistics. When the active cluster becomes available again, the logs and statistics from the back can then be synchronized to the active cluster.

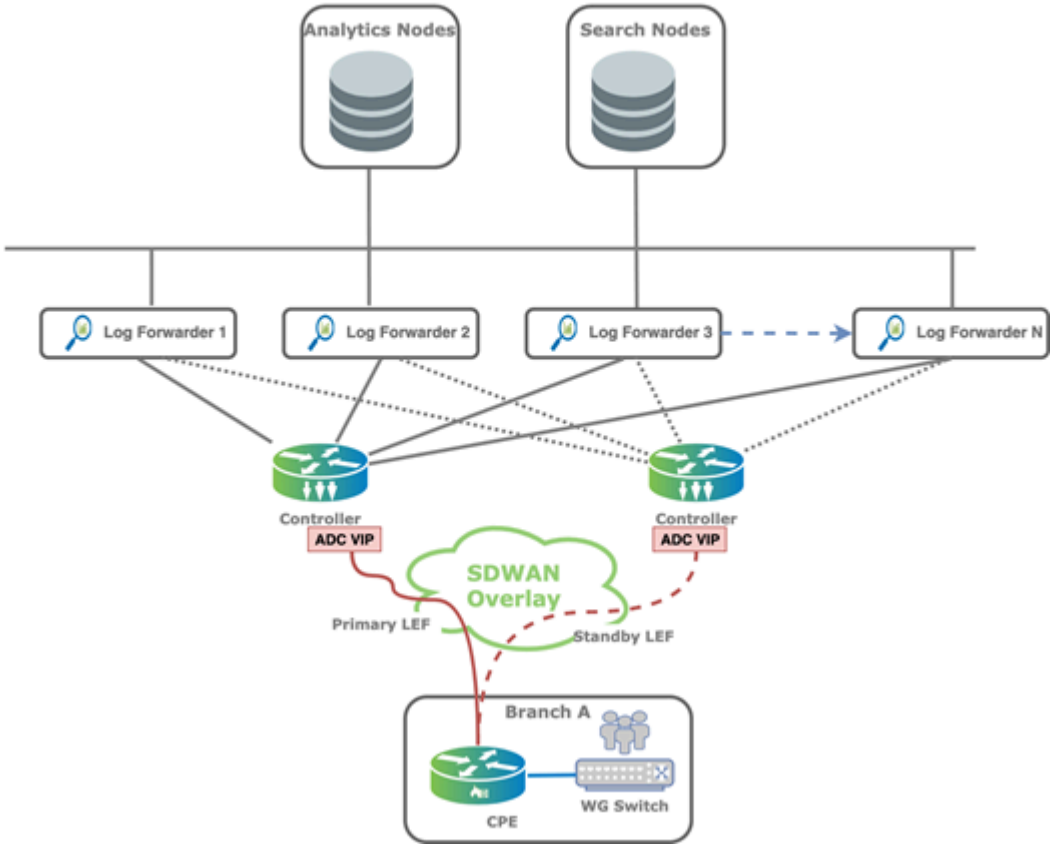
If the topology has multiple Analytics clusters, database replication happens automatically only within the same cluster.

Role of the Log Forwarder

The Versa Operating System™ (VOS™) edge devices generate logs destined for the Analytics database. These logs are carried in an IPFIX template and are delivered to the log forwarder. The log forwarder removes the IPFIX template overhead and stores the logs in clear text on log collector disk. The Analytics database servers can then access the logs from the log forwarder. Optionally, logs can be forwarded in syslog format to third-party log forwarders.

The log forwarder function is part of the Versa Analytics node. It can run on the Versa Analytics node itself or as a standalone log forwarder, where a separate VM or server is dedicated to this role. For larger deployments, especially for deployments with 1000 or more branches, it is recommended that you separate the log forwarder function, because it

provides better scalability for the Analytics platform. When the log forwarder runs on a separate device, you typically deploy it south of the Analytics or Search nodes, as shown in the following figure.



Best Practices for Versa Analytics Sizing

The scaling of a Versa Analytics cluster is driven by the logging configuration for the individual features enabled on VOS edge devices. Most features include an optional logging configuration to log events related to a specific rule or profile. The number of features for which you enable logging and the volume of logs that each feature generates has a direct impact on the sizing and scalability of the Versa Analytics cluster.

Versa Analytics has two distinct database personalities, Analytics node and Search node. The Analytics node delivers the data for most of the dashboards shown in the Analytics GUI. These data are aggregated data, and the data aggregation is enabled by default. Therefore, the dashboards are populated without configuration on the VOS edge devices. Analytics node scaling is determined by granularity of the reported data, which is usually set between 5 and 15 minutes. The topology also affects the scaling of the Dashboard feature. A full-mesh topology with multiple underlays generates more SLA logging messages compared to a hub-spoke topology with a single underlay. This is because SLA monitoring between branches in the underlay contributes significantly to the log volume as it reports SLA measurements to the Analytics node.

The primary tasks of the Search node are to store logging and event data, and to drive the log sections and log tables on the Dashboard. These functions are heavily utilized, because every event in the network triggers a log entry on the Search node. In a minimal default configuration, the only information that is logged to the search nodes are the alarm logs. The sizing of the search node depends on the following:

- Number of features enabled with logging
- Logging data volume and log rate
- Retention period of logged data
- Packet capture—You should enable packet capture and traffic monitoring only for traffic related to specific troubleshooting. Packet captures are not stored in the database, but rather as stored as PCAP files. If these files are not processed correctly, they can quickly fill up the disk space.

Feature such as firewall logging and traffic monitor logging (Netflow) have a significant impact on the overall scaling of the Analytics cluster. Therefore, it is recommended that you avoid creating wildcard logging rules. In response to an increases analytics load, you can scale both the Analytics and Search nodes horizontally. Versa Networks has a calculator tool that can help you size an Analytics cluster based on the information described in the next section.

Best Practices for Headend Design

A stable and fault-tolerant solution requires proper design of the headend. A proper design factors in the expected utilization in order to dimension the compute resources so that they can be horizontally scaled out when required. The headend design must be well thought out high availability design, to ensure that there is no single point of failures. Finally, the headend must be secured and hardened to avoid possible security vulnerabilities.

It is recommended that you consider the following when deploying a Versa Networks headend:

- Ensure that you configure DNS on the Director and Analytics nodes. DNS is used for operations such as downloading security packs (SPacks) an, on Analytics devices, for reverse lookup.
- Ensure that you configure NTP and synchronize it across all nodes in the SD-WAN network. It is recommended that you configure all nodes to be in the same time zone, to make log correlation between various components practical.
- Perform platform hardening procedures such as signed SSL certificates, password hardening, and SSL banners for CLI access.
- Ensure that you have installed the latest OS security pack (OS SPack) on all components and that you have installed the latest SPack on the Director node
- Ensure that the appropriate ports on any intermediate firewalls are open.

For more information, see the hardening articles.

For assistance with the design and validation of the headend before you move it into production, contact Versa Networks Professional Services.

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

Firewall Requirements
Hardware and Software Requirements for Headend
Scalability and Performance