AVI
Networks®

Avi Vantage 20.1.X Release Notes

Avi Technical Reference (v20.1)

Avi Vantage 20.1.X Release Notes

view online

Issues Resolved in 20.1.9

Release date: 04 May 2022
To refer to the upgrade checklist, click here.

- AV-98925: With Avi Vantage version 18.2.6 or higher, the RSA-PSS signature algorithms take precedence by default in the Avi SE and that may force compatibility issues with older SSL stacks that do not support these algorithms
- AV-132736: The SSL certificate?s private key is returned via GET API calls as part of the certificate content, when the certificate is uploaded incorrectly
- AV-136068: Service Engine might go down when the memory consumption goes high due to an error in the memory allocation sequence
- AV-139230: Connection closure time of a TCP session may increase when multiple DNS requests are pipelined by the client and the response is received from the pool member
- AV-140366: Mitigation for CVE-2022-0778
- AV-141739: Avi AWS cloud may modify the custom security group attached to the SEs instead of the Avi created custom security group
- AV-141840: If an application profile has a PKI profile selected and Add HTTP Request Headers enabled with the client certificate's NOT VALID AFTER option, then the SE might fail if the client does not send the certificate
- AV-142581: A warning message is displayed when searching for users via the UI in Administration > Accounts > Users

Key Change in 20.1.9

- If the client request contains X-forward-proto header, NSX Advanced Load Balancer will rewrite it. Only single `X-forward-proto` will be sent to the server.

Known Issue in 20.1.9

- AV-142713:

  Symptom: SE connection to Controller fails with the error `SSL: CERTIFICATE_VERIFY_FAILED` on Controller upgrade.

  Condition: The Controller has been upgraded, rolled back, and upgraded again, using the same set of NSX Advanced Load Balancer versions for the upgrades and if the:
  - Initial version was 18.2.5 or lower
  - Version to be upgraded to is 18.2.6 or higher

  Work Around: Before repeating the upgrade operation, check the following directories on all Controller nodes, and delete the following:
  - List of files:
    se.ova, se.qcow2, se.raw.gz, se_docker.tgz, se-disk1.vmdk, se.mf, se.ovf, se_nsxt.ovf', se_nsxt.mf, se_nsxt-disk1.vmdk, se_nsxt.ova from:

- List of Directories:
  /host/pkgs/ /vol/pkgs/

## Checklist for Upgrade to Avi Vantage Version 20.1.9 Refer to this section before initiating upgrade.

- Upgrading to Avi Vantage version 20.1.9 is supported from any of the following versions:
  - Avi Vantage version 17.2.x
  - 18.2.1 through 18.2.13
  - Avi Vantage version 20.1.x
    Note: Upgrade from versions higher than 18.2.13 to version 20.1.9 is not supported. For more information refer to:
    - Upgrade from Avi Vantage release 18.2.6 or higher
    - Upgrade from a version prior to Avi Vantage release 18.2.6

- Starting with Avi Vantage release 20.1.1 as per the HTTP/2 RFC, the cipher suites with TLS 1.2 listed here are not supported. Remove the ciphers before initiating upgrade to Avi Vantage version 20.1.1.

- Avi Vantage no longer supports VMware vCenter version 5.5. The End of General Support for vSphere 5.5 by VMware was on September 29th, 2018.
  Before upgrading to Avi Vantage version 20.1.8, it is recommended to upgrade to a current vCenter version. For more information, refer to the System Requirements article.

- An Avi Vantage deployment with FIPS mode enabled prior to 20.1.5, cannot be upgraded.

- Starting with Avi Vantage 20.1.5, the NSX-V Cloud Connector is not supported. The NSX-V cloud was deprecated in version 20.1.3, and is now unsupported. It is recommended to migrate to an NSX-T cloud connector, or switch to no-orchestrator mode with NSX-V.

- Starting with Avi Vantage version 20.1.1, the default disk size for new SEs is now 15 GB.
  For OpenStack deployments, ensure that the disk size for the requisite flavors is increased to a minimum of 15 GB

- Starting with Avi Vantage version 20.1.1, the Avi Controller and Service Engines use Python 3. Refer to the migration notes in the following sections:

  - For ControlScripts

  - For Python-based External Health Monitors

- Licensing Management of the Avi Service Engines has been updated. Refer to the Avi Vantage License Management article for more information.

- Avi Vantage now enforces system limits based on Controller cluster size. Refer to the System Limits article for more information.

- In case of Service Engine upgrade in a Nutanix Acropolis Hypervisor (AHV) environment, refer to the pre-upgrade changes.

- Starting with version 20.1, Avi Vantage has moved from Lua 5.1 to LuaJIT for compiling and running DataScripts. LuaJIT is relatively more restrictive with non-defined escape sequences. Using any escape sequence other than ones supported, (as defined in the Lua 5.1 Reference Manual) results in a compile error. Before upgrading to version 20.1 or higher, ensure the DataScripts do not use undefined escape sequences.
  If the DataScripts are not fixed before upgrade, the DataScripts using non-defined escape sequences, which worked earlier will now cause the virtual service to go down.

Issues Resolved in 20.1.8 Patch Releases

Issues Resolved in 20.1.8-3p1

- AV-140366: Mitigation for CVE-2022-0778.
- AV-136068: Service Engine failure due to a missing check in the memory allocation routine which gets triggered when Service Engine memory consumption goes high.
- AV-132736: Private-keys uploaded as part of Certificate are explicitly moved to avoid disclosure with any GET APIs.
- AV-98925: With the NSX Advanced Load Balancer version 18.2.6 or higher, RSA-PSS signature algorithms take precedence by default in the Avi SE and that may force compatibility issues with older SSL stacks that do not support these algorithms.

What's New in 20.1.8

Release date: 03 February 2022
To refer to the upgrade checklist, click here. ### Cloud Connector * AWS: Support for the region `ap-east-1`.

- LSC: Support for kernel version 3.10.0-1160.53.1.0.1.el7.x86_64 and 3.10.0-1160.45.1.el7.x86_64.

- NSX-T: Support for Active/Standby topology at AZ level.

Core LB Features

- L4 DataScript `avi.pool.get_server_info()` to return the server address and port for any request or response.

- L4 DataScript `avi.pool.get_server_ip()` to return the IP address of a request or response.

Security

- Mitigation for CVE-2021-44228.

WAF

- Support for XML exceptions.

Issues Resolved in 20.1.8

- AV-98655: TSO offload does not work if one of the member interfaces in inactive at the time of bond creation.

- AV-101483: GSLB configuration sync to other sites fail, if public IP is configured in the GSLB sites.

- AV-102522: When FIPS mode is enabled, the Service Engine may fail if HTTP Security Policy with per_ip + per_uri_path rate limiting rules are configured for a virtual service. Do not use HTTP Security Policy with per_ip + per_uri_path rate limiting rules in FIPS mode.

- AV-118269: Network resolution of GSLB site persistence pool fails when using per tenant VRF in vCenter, leading to VS placement failing if site persistence is enabled before the virtual service is placed on all requested number of SEs.

- AV-118700: Service Engine can fail in some error conditions with the backend, when connection multiplexing is disabled.

- AV-118805: VMXNET3 interface receive stalls due to packet buffer depletion.

- AV-128228: `SE_SYN_TABLE_HIGH` alerts are seen for large number of embryonic connections without necessarily the underlying system under attack or memory stress.

- AV-128843: Application traffic in a GSLB environment can get disrupted in upgrade scenarios in the following conditions:
  - GSLB service is configured with NO DATAPATH health monitors and relies on Controller-status
  - GSLB federation is in maintenance mode
  - Site is upgraded to a newer version
- AV-121761: LSC: On hosts with large memory (>= 256 GB), when the Controller is also running on the same host, Service Engine may fail due to memory fragmentation.
- AV-121820: By default, faults are not available in the inventory APIs. A query parameter to include faults is introduced in the inventory APIs.
- AV-124588: HTTPS requests with chunked transfer encoding might timeout when DataScript or WAF is enabled on the virtual service.
- AV-124931: Auto-download of CRS fails when proxy is configured.
- AV-125094: Scanner Application Profile rate limiter with `report only` action does not get logged.
- AV-125377: External health monitor is unable to invoke ping since it requires raw socket access privileges.
- AV-125592: Controllers do not get license capacity when NSX serial keys are uploaded with zero quantity (unlimited licenses). Serial key is added with zero service cores.
- AV-125682: GCP cloud is failing to connect to the GCP API servers with `x509.CertificateInvalidError` when `crypto/tls/fipsonly` package is enabled.
- AV-125824: If a bond exists on the management interface NICs (>=10G), it can be broken while stopping / restarting / upgrading the Service Engines in LSC deployments.
- AV-125901: Avi GCP cloud does not allow updating project ID of SEs without deleting all the SEs.
- AV-126148: The Avi cloud connector fails to sync AWS Auto scaling groups if there are more than 200 servers in the cloud.
- AV-126153: When a patch is applied to the Controller or SE, file extraction can fail in some scenarios causing the patch operation to end prematurely.
- AV-126389: When RSS is enabled, packet buffers are not freed and eventually lead to connection failures due to a race condition during packet transmission on vNICs that have VLAN configured.
- AV-126508: BGP: Virtual service scale in can result in minor traffic disruption.
- AV-126754: Cluster VIP configuration fails in GCP cloud when the controllers have Public IP assigned to them.
- AV-127046: WAF tab in the UI is empty for some virtual services.
- AV-127244: Upgrade is successful even when the `max_active_versions` is greater than 2. This leads to an unsupported deployemnt where the NSX Advanced Load Balancer might be running with 3 different versions and can lead to SE sync issues.

- AV-127278: Existing static routes are overwritten due to pagination issues on the UI.
- AV-127481: Auto-deployment of CRS might fail.
- AV-127498: When the SE group is in a version lower than 20.1.5 and the Controller is in a version 20.1.5 or higher, the SE may fail if a pool has multiple resolve by DNS - based pool members and these pool members fail to resolve.
- AV-128044: When streaming request logs over Syslog format, VS-name is not included in streamed logs.
- AV-128063: Unable to mask query parameters in Application logs.
- AV-128707: The SE Agent process might leak an opened file descriptor and consume too much disk space.
- AV-128745: When a GSLB leader site is represented as FQDN instead IP address, the GSLB configuration replication from leader to follower site is not working.
- AV-128928: Server-initiated renegotiation was disabled in 20.1.5. This results in Server-initiated renegotiation failures for both Pools and HTTPS Health Monitor.
- AV-128998: If the leader site is running versions 20.1.1 until 20.1.5 and the follower is running versions > 20.1.5, Remote Site Watcher Sync can fail.
- AV-129150: NSX Advanced Load Balancer creates empty storage accounts on Azure cloud.
- AV-129171: With Linux Server Cloud and Avi or Infoblox IPAM configured in a scaled setup, the virtual service placement can get stuck due to unnecessary attached IP RPCs being issued and these RPCs timing out.
- AV-129587: After upgrade, some GSLB service members belonging to Avi sites can be marked *UP* even when member virtual services are down.
- AV-130174: For logs streaming in Syslog format, at times the Application profile UUID is included as App-name in header instead of the virtual service name.
- AV-130327: GSLB configuration sync fails when site is represented by Cluster-VIP/FQDN/public-network address translated IPs.
- AV-130959: Service Engine failure when a GET request with a body is sent to a virtual service with a HTTP/2 pool.
- AV-131131: SE memory is being computed as available memory as opposed to provisioned memory. SE VM with 2048 MB RAM allocated in vSphere, reported system memory inside the VM as 1987 MB leading to one `se_dp` instance being provisioned instead of two for bandwidth licensing.
- AV-131472: Auto-download of CRS via Pulse fails.
- AV-131180: Jumbo frame size is not supported for VMXNET3 interfaces.
- AV-131683: Virtual service VIP update fails when the subnet field is empty in a VIP of the virtual service.
- AV-131181: On receiving streamed logs, the reported timestamp in the log messages sometimes is displayed as PST time, if the Service Engine of the customers is configured to use PST as the system time zone.
- AV-131554: Service Engine failure occurs when a misconfigured SSL profile is attached to a pool.

- AV-132736: When a primary key is uploaded as part of a certificate body, after clicking the validate button, the primary key continues to be visible in the certificate section.
- AV-132924: GeoDb IP to country code mapping is mismatched.
- AV-133194: Openstack cleanup API fails to delete imported OpenStack tenants.
- AV-133360: The `Remote_site_watcher` process can get stuck if there is a GRPC connection failure during the resync process.
- AV-134202: Upgrade and Tiny portal service fail continuously after patch application fails.
- AV-134355: When a network's name is changed in the Controller, the name change does not reflect in the network runtime.
- AV-136284: The `show virtualservice authstats` command does not return an output even when an LDAP Auth Profile was attached to the virtual service.

Key Changes in 20.1.8

- Private keys uploaded as part of a certificate are explicitly removed to avoid disclosure with any GET APIs.
- Graceful disable of server is supported for an L7 virtual service with connection multiplexing disabled.
- When certificate sharing is enabled, the intermediate/CA certificate with the highest number of days for expiry in the current tenant is always selected. In the absence of an intermediate/CA in the current tenant, intermediate/CA is selected from the admin tenant, if any.
- The minimum value for X-Avi-Version that can be used when interacting with the Avi Controller is 18.2.6. It is recommended to update the automation assets, as required.

Known Issue in 20.1.8

- AV-142641: Macro API for virtual service deletion does not support API migration below X-Avi-Version 20.1.1.

## Checklist for Upgrade to Avi Vantage Version 20.1.8 Refer to this section before initiating upgrade.

- Upgrading to Avi Vantage version 20.1.8 is supported from any of the following versions:
    - Avi Vantage version 17.2.x
    - 18.2.1 through 18.2.13
    - Avi Vantage version 20.1.x
      Note: Upgrade from versions higher than 18.2.13 to version 20.1.8 is not supported. For more information refer to:
        - Upgrade from Avi Vantage release 18.2.6 or higher
        - Upgrade from a version prior to Avi Vantage release 18.2.6
- Starting with Avi Vantage release 20.1.1 as per the HTTP/2 RFC, the cipher suites with TLS 1.2 listed here are not supported. Remove the ciphers before initiating upgrade to Avi Vantage version 20.1.1.

- Avi Vantage no longer supports VMware vCenter version 5.5. The End of General Support for vSphere 5.5 by VMware was on September 29th, 2018.
  Before upgrading to Avi Vantage version 20.1.8, it is recommended to upgrade to a current vCenter version. For more information, refer to the System Requirements article.

- An Avi Vantage deployment with FIPS mode enabled prior to 20.1.5, cannot be upgraded.
- Starting with Avi Vantage 20.1.5, the NSX-V Cloud Connector is not supported. The NSX-V cloud was deprecated in version 20.1.3, and is now unsupported. It is recommended to migrate to an NSX-T cloud connector, or switch to no-orchestrator mode with NSX-V.
- Starting with Avi Vantage version 20.1.1, the default disk size for new SEs is now 15 GB.
  For OpenStack deployments, ensure that the disk size for the requisite flavors is increased to a minimum of 15 GB
- Starting with Avi Vantage version 20.1.1, the Avi Controller and Service Engines use Python 3. Refer to the migration notes in the following sections:
  - For ControlScripts
  - For Python-based External Health Monitors
- Licensing Management of the Avi Service Engines has been updated. Refer to the Avi Vantage License Management article for more information.
- Avi Vantage now enforces system limits based on Controller cluster size. Refer to the System Limits article for more information.
- In case of Service Engine upgrade in a Nutanix Acropolis Hypervisor (AHV) environment, refer to the pre-upgrade changes.
- Starting with version 20.1, Avi Vantage has moved from Lua 5.1 to LuaJIT for compiling and running DataScripts. LuaJIT is relatively more restrictive with non-defined escape sequences. Using any escape sequence other than ones supported, (as defined in the Lua 5.1 Reference Manual) results in a compile error. Before upgrading to version 20.1 or higher, ensure the DataScripts do not use undefined escape sequences.
  If the DataScripts are not fixed before upgrade, the DataScripts using non-defined escape sequences, which worked earlier will now cause the virtual service to go down.

Issues Resolved in 20.1.7 Patch Releases

Issues Resolved in 20.1.7-2p16

- AV-142491: Enabling the `deactivate_vm_discovery` flag in a vCenter cloud causes `vi-mgr` to fail
- AV-115797: `SE_DOWN` event is not displayed under Operations > Events . All Events and user login events are not displayed in the Config Audit Trail.

Issue Resolved in 20.1.7-2p15

- AV-140199: In case of `syslog_over_TLS` and `TCP_over_TLS` modes, when external log server is restarted, log streaming stops working.

Issues Resolved in 20.1.7-2p14

- AV-142624: Events and logs are timing out and new events/logs are not visible on the UI/API. When the log manager indexes a file, if the file is corrupted or not able to read the log from the file, the indexer is stuck in loops.
- AV-142581: A warning message is displayed when searching for users via the UI in Administration > Accounts > Users
- AV-141739: Avi AWS cloud may modify the custom security group attached to the SEs instead of the Avi-created custom security groups
- AV-140529: If there are subnets having duplicate names, Avi's AWS cloud may pick up incorrect subnet for the SE

Issues Resolved in 20.1.7-2p13

- AV-139230: Connection closure time of a TCP session may increase when multiple DNS requests are pipelined by the client and the response is received from the pool member.
- AV-138352: Multiple updates to enhanced virtual service parent could result in failure when traffic is sent to its child virtual service.

Issues Resolved in 20.1.7-2p12

- AV-140366: Mitigation for CVE-2022-0778.
- AV-139248: In vCenter cloud, sometimes, the Controller adds two vNICs on the SE in the same network and VRF.
- AV-138278: Under SE group configuration, changes made in Data Store Scope in Service Engine Virtual Machine does not persist after clicking Save, specifically when the Shared is selected at first and then changed to Any or Local.
- AV-138269: After a SE group with a set of asymmetrically placed shared VIP virtual services (with some placed on only one SE) is upgraded, shared VIP virtual service placement for this set will not work properly.
- AV-135843: After applying the Controller patch, the indexer service fails.
- AV-133360: Remote_site_watcher process can get stuck if there is a GRPC connection failure during resync process.

Issues Resolved in 20.1.7-2p11

- AV-138439: SE failure due to flow table entry leak with the delayed flow table entry delete feature in a stressed up system.
- AV-135843: After applying the Controller patch, the indexer service fails.
- AV-131444: Support for searching Avi objects using markers.
- AV-128145: The DNS Virtual Service dropdown is empty in the GSLB site configuration screen.

Issues Resolved in 20.1.7-2p10

- AV-136284: The `show virtualservice` authstats did not return any output even when an LDAP Auth Profile was attached to the virtual service.
- AV-136068: ServiceEngine failed due to insufficient memory.
- AV-133194: The`Openstack-cleanup` API fails to delete imported OpenStack tenants.
- AV-118700: Service Engine can fail in some error conditions with the backend, when connection multiplexing is disabled.

Issues Resolved in 20.1.7-2p9

- AV-131472: Auto-download of CRS via Pulse fails.
- AV-128707: The SE Agent process might leak an opened file descriptor and consume too much disk space.

Issues Resolved in 20.1.7-2p8

- AV-132924: GeoDb IP to country code mapping is mismatched.
- AV-131180: Jumbo frame size is not supported for VMXNET3 interfaces.

Issues Resolved in 20.1.7-2p7

- AV-132431: Mitigation for CVE-2021-44228.
- AV-131181: On receiving streamed logs, the reported timestamp in the log messages sometimes is displayed as PST time, if the Service Engine of the customers is configured to use PST as the system time zone.
- AV-128943: OpenStack: Support for Keystone v2.0
- AV-128928: Server-initiated renegotiation was disabled in 20.1.5. This results in Server-initiated renegotiation failures for both Pools and HTTPS Health Monitor.
- AV-127498: When the SE group is in a version lower than 20.1.5 and the Controller is in a version 20.1.5 or higher, the SE may fail if a pool has multiple resolve by DNS - based pool members and these pool members fail to resolve.
- AV-127046: WAF tab in the UI is empty for some virtual services.
- AV-126506: Support for getting pool IP and port through DataScript in response event.

Issue Resolved in 20.1.7-2p6

- AV-118805: VMXNET3 interface receive stalls due to packet buffer depletion.

Issues Resolved in 20.1.7-2p5

- AV-127278: Existing static routes are overwritten due to pagination issues on the UI.
- AV-128044: When streaming request logs over Syslog format, VS-name is not included in streamed logs.
- AV-128063: Unable to mask query parameters in Application logs.

Issues Resolved in 20.1.7-2p4

- AV-125824: If a bond exists on the management interface NICs (>=10G), it can be broken while stopping / restarting / upgrading the Service Engines in LSC deployments.
- AV-121820: By default, faults are not available in the inventory APIs. A query parameter to include faults is introduced in the inventory APIs.

Issues Resolved in 20.1.7-2p3

- AV-126389: When RSS is enabled, packet buffers are not freed and eventually lead to connection failures due to a race condition during packet transmission on vNICs that have VLAN configured
- AV-126153: When a patch is applied to the Controller or SE, file extraction can fail in some scenarios causing the patch operation to end prematurely.
- AV-125901: Avi GCP cloud does not allow updating project ID of SEs without deleting all the SEs.
- AV-125682: GCP cloud is failing to connect to the GCP API servers with `x509.CertificateInvalidError` when `crypto/tls/fipsonly` package is enabled.
- AV-125592: Controllers do not get license capacity when NSX serial keys are uploaded with zero quantity (unlimited licenses). Serial key is added with zero service cores.
- AV-125377: External health monitor is unable to invoke ping since it requires raw socket access privileges.

Key Changes in 20.1.7-2p3

- AV-116516: Graceful disable of server is supported for an L7 virtual service with connection multiplexing disabled.

Issues Resolved in 20.1.7-2p2

- AV-124931: Auto-download of CRS fails when proxy is configured
- AV-121761: LSC: On hosts with large memory (>= 256 GB), when the Controller is also running on the same host, Service Engine may fail due to memory fragmentation.

Issue Resolved in 20.1.7-2p1

- AV-124588: HTTPS requests with chunked transfer encoding might timeout when DataScript or WAF is enabled on the virtual service.

What?s New in 20.1.7

Release date: 17 September 2021
To refer to the upgrade checklist, click here.

Cloud Connector

- GCP: Support to specify service account for newly created SEs
- GCP: Support for configurable cloud virtual service /32 static default route priority
- LSC: Support for base kernel versions 3.10.0-1160.36.2.el7 and 3.10.0-1160.25.1

Core LB Features

- Support to disable primary pool when it is down using the field `deactivate primary pool on down`

Issues Resolved in 20.1.7

- AV-87320: In a Terraform plan with nested blocks, the Avi Terraform provider sets default values for the optional fields which were not defined in the plan
- AV-113654: In the Avi UI, after adding a new GSLB site when the Save and Set DNS Virtual Services button was clicked, the HTTP error, 403: GSLB Operations are NOT Permitted is displayed
- AV-116411: Service Engine fails when a HTTP/1.0 request is sent without a host header to a virtual service with a pool with both HTTP/2 and SSL enabled
- AV-115671: In an OpenStack cloud, the Controller may initiate multiple Add VNIC operations on the SE for the same network and VRF before the vNIC IP limit is reached, causing potential traffic issues
- AV-115729: Fixed cleanup of DHCP client on Avi interfaces upon SE shutdown
- AV-116043: Cluster based events are not generated when the Controller cluster leader is restarted
- AV-116206: dhclient anomaly in SE deployments in LSC deployments
- AV-116243: The Avi Controller on AWS C2S environment fails to create new SEs
- AV-116398: AWS: Removing the application domain name from a shared virtual service results in the deletion of a random entry from the list
- AV-116440: Reindexing a HTTP policy via the UI using Virtual Service >Policies>HTTP Requests>Move To does not work
- AV-116620: In an OpenStack cloud, the Service Engine Group page is inaccessible via the UI
- AV-116738: Due to miscalculation on Docker?s memory usage, the memory balancer does not get triggered causing cluster leader failover

- AV-116791: For OpenStack clouds using BGP, configuring a BGP peer network displays the error Network object not found
- AV-116974: SE may fail due to invalid memory access in local port processing
- AV-116327: High disk usage on the Controller leader node due to excess files in /var/lib/avi/systeminfo
- AV-117141: PKI profile does not support API versioning
- AV-117414: An L4 object?s name exceeding 128 characters may lead to SE failure
- AV-117715: In an L4-SSL virtual service, disabling a server while it?s handing the traffic results in SE failure
- AV-117720: App Cookie persistence fails when used in combination with the avi.http.remove_header (?Set-Cookie?) and avi.http.add_header (?Set-Cookie?) DataScript APIs, if the app cookie persistence and DataScript are on the same virtual service
- AV-117865: SE fail-over time is higher (more than three minutes) in AWS
- AV-117960: The Avi Controller upgrade with AWS cloud can fail if the cloud is in failed state
- AV-117967: Static route is prioritised over connected route which can lead to incorrect routing of packets in write access environments
- AV-118062: GCP DPDK RSS configured environments with scaled-out virtual services may present intermittent front-end connection resets
- AV-118134: When a virtual service is configured with use_vip_as_snat or effectively using VIP IP as SNAT, consecutive migrations to the same SE may render the virtual service with that VIP inoperative
- AV-118242: The character ?;? is not allowed as a URL query parameter delimiter.
- AV-118264: SE fails if the NAT policy is configured with source/destination port match and when a routable ICMP packet to external world lands on the SE
- AV-118277: High disk usage on SE because of IP reputation files consuming space
- AV-118468: A DNS virtual service created with System-UDP-Fast-Path (not recommended) can lead to flow table entry (subsequently memory) build-up upon reflection attack
- AV-118500: Self-signed certificates and certificate signing requests generated on the Controller are created correctly when using HSM
- AV-118700: Service Engine can fail in some error conditions with the backend, when connection multiplexing is disabled
- AV-118802: System generates duplicate diffs for federated objects which can potentially lead to streaming of incorrect config objects to follower sites in a GSLB federation
- AV-119910: The Controller service `vcenter_mgr` may fail when the SE is deleted
- AV-119914: System generates duplicate diffs for federated objects which can potentially lead to streaming of incorrect config objects to follower sites in a GSLB federation

- AV-119921: In a persistence profile, the `ip_mask` behaves as an inverse CIDR mask and distributes the clients across servers instead of ensuring the clients in the same subnet are connected to the same servers

- AV-119491: When using auto allocation with cloud native IPAM in AWS cloud, a virtual service VIP update which removes the existing VIP level `subnet_uuid` and `ipam_network_subnet level network_uuid` and `subnet_uuid` fields while keeping the same ipam_network_subnet subnet CIDR results in the VIP getting a new IP but the new IP is not attached in the cloud

- AV-119449: Log manager runs into bad states if the log files get deleted when trying to get the file stats

- AV-119952: Fetching GSLB status is leading to high CPU usage of DBcache, which may affect the inventory processing time

- AV-119971: When Ignore request body parsing errors due to partial scanning is enabled in a WAF Profile and Enable Request Body Buffering is also enabled in the Application profile, the parsing errors are not ignored in WAF and the request is denied.

- AV-120361: Connection to pool server is not using the updated key/certificate in the `SSLKeyAndCertificate` object assigned to the pool.

- AV-120542: Virtual Service traffic capture with GRO or TSO enabled system might lead to SE failure

- AV-121618: OpenStack: On configuring a flavor in the SE group to have the same set of resources as the other flavors in the OpenStack cloud, the wrong flavor will be used when creating the SEs

- AV-121268: Inconsistent Network Interface MAC address/BDF to interface name mapping on Avi SE on CSP causes SE startup to fail or results in post-upgrade failure

- AV-122772: When auto gateway is enabled, TCP Mss can be NULL for IPv6 connections.

- AV-122836: When GSLB leader site is represented with cluster VIP, configuration replication between sites is not working.

Key Changes in 20.1.7

- The life span of persistence entries is increased to 86400

- Prior to NSX Advanced Load Balancer version 20.1.7, it was not possible to configure a service match criterion for policies under a child virtual service due to the lack of existing services object to be verified against. Starting with NSX Advanced Load Balancer 20.1.7, in SNI virtual hosting and Enhanced Virtual Hosting, for policies under a child virtual service, the service match criterion is matched against its parent virtual service.

- By default faults are not available in the inventory APIs. A query parameter to include faults is introduced in the inventory APIs.

- The minimum value for X-Avi-Version that can be used when interacting with the Avi Controller is 18.2.6. It is recommended to update the automation assets, as required.

Known Issue in 20.1.7

- AV-127481: Auto-deployment of CRS might fail.
  Workaround: Manually download the CRS and upload it to the system.

- AV-142641: Macro API for virtual service deletion does not support API migration below X-Avi-Version 20.1.1.

## Checklist for Upgrade to Avi Vantage Version 20.1.7 Refer to this section before initiating upgrade.

- Upgrading to Avi Vantage version 20.1.7 is supported from any of the following versions:
  - Avi Vantage version 17.2.x
  - 18.2.1 through 18.2.13
  - Avi Vantage version 20.1.x

  Note: Upgrade from versions higher than 18.2.13 to version 20.1.7 is not supported.
  For more information refer to:
  - Upgrade from Avi Vantage release 18.2.6 or higher
  - Upgrade from a version prior to Avi Vantage release 18.2.6

- Starting with Avi Vantage release 20.1.1 as per the HTTP/2 RFC, the cipher suites with TLS 1.2 listed here are not supported. Remove the ciphers before initiating upgrade to Avi Vantage version 20.1.1.

- Avi Vantage no longer supports VMware vCenter version 5.5. The End of General Support for vSphere 5.5 by VMware was on September 29th, 2018.
  Before upgrading to Avi Vantage version 20.1.7, it is recommended to upgrade to a current vCenter version. For more information, refer to the System Requirements article.

- An Avi Vantage deployment with FIPS mode enabled prior to 20.1.5, cannot be upgraded.

- Starting with Avi Vantage 20.1.5, the NSX-V Cloud Connector is not supported. The NSX-V cloud was deprecated in version 20.1.3, and is now unsupported. It is recommended to migrate to an NSX-T cloud connector, or switch to no-orchestrator mode with NSX-V.

- Starting with Avi Vantage version 20.1.1, the default disk size for new SEs is now 15 GB.
  For OpenStack deployments, ensure that the disk size for the requisite flavors is increased to a minimum of 15 GB

- Starting with Avi Vantage version 20.1.1, the Avi Controller and Service Engines use Python 3. Refer to the migration notes in the following sections:

  - For ControlScripts

  - For Python-based External Health Monitors

- Licensing Management of the Avi Service Engines has been updated. Refer to the Avi Vantage License Management article for more information.

- Avi Vantage now enforces system limits based on Controller cluster size. Refer to the System Limits article for more information.

- In case of Service Engine upgrade in a Nutanix Acropolis Hypervisor (AHV) environment, refer to the pre-upgrade changes.

- Starting with version 20.1, Avi Vantage has moved from Lua 5.1 to LuaJIT for compiling and running DataScripts. LuaJIT is relatively more restrictive with non-defined escape sequences. Using any escape sequence other than ones supported, (as defined in the Lua 5.1 Reference Manual) results in a compile error. Before upgrading to version 20.1 or higher, ensure the DataScripts do not use undefined escape sequences.
  If the DataScripts are not fixed before upgrade, the DataScripts using non-defined escape sequences, which worked earlier will now cause the virtual service to go down.

Issues Resolved in 20.1.6 Patch Releases

Issue Resolved in 20.1.6-2p20

- AV-140529: If there are multiple subnets having duplicate names, NSX Advanced Load Balancer's AWS cloud may pick up the incorrect subnet for the SE

Issue Resolved in 20.1.6-2p18

- AV-141095: Request timeout on a virtual service when the DatpaScript line `avi.http.response(200)` is called in the response event.

Issues Resolved in 20.1.6-2p17

- AV-141095: Request timeout on a virtual service when the DataScript line avi.http.response(200) is called in the Response Event.
- AV-138792: Service Engine might crash with the combination of Error page configuration on failed requests and Clients sending pipelined HTTP posts on the same front end TCP connection.
- AV-129536: vCenter cloud may go down with vcenter 7.0 and above

Issues Resolved in 20.1.6-2p16

- AV-135843: After applying the Controller patch, the indexer service fails.
- AV-130327: GSLB configuration sync fails when site is represented by Cluster-VIP/FQDN/public-Natted IPs.

Issues Resolved in 20.1.6-2p15

- AV-136539: Spinning SEs from the Azure Market place does not work. Azure Marketplace invalidated all the existing Avi Controller and SE Plans(SKUs).
- AV-136068: Service Engine failure due to insufficient memory.
- AV-133382: When certificate sharing is enabled, the intermediate/CA certificate with the highest number of days for expiry in the current tenant is always selected. In the absence of an intermediate/CA in the current tenant, intermediate/CA is selected from the admin tenant, if any.

Issue Resolved in 20.1.6-2p14

- AV-132736: When a primary key is uploaded as part of a certificate body, then after clicking the validate button, the primary key continues to be visible in the certificate section.

Issues Resolved in 20.1.6-2p13

- AV-131472: Auto-download of CRS via Pulse fails.
- AV-133360: The `Remote_site_watcher` process can get stuck if there is a GRPC connection failure during the resync process.
- AV-134202: Upgrade and Tiny portal service fail continuously after patch application fails.

Issue Resolved in 20.1.6-2p12

- AV-131683: VSVIP update fails when the subnet field is empty in a VIP of the concerned VSVIP

Issues Resolved in 20.1.6-2p11

- AV-132431: Mitigation for CVE-2021-44228.

- AV-131131: SE memory is being computed as available memory as opposed to provisioned memory. SE VM with 2048 MB RAM allocated in vSphere, reported system memory inside the VM as 1987 MB leading to one `se_dp` instance being provisioned instead of two for bandwidth licensing.
- AV-127046: WAF tab in the UI is empty for some virtual services.

What's New in 20.1.6-2p10

- AV-131180: Jumbo frame support for VMXNET3 interfaces.

Issue Resolved in 20.1.6-2p10

- AV-127498: When the SE group is in a version lower than 20.1.5 and the Controller is in a version 20.1.5 or higher, the SE may fail if a pool has multiple resolve by DNS - based pool members and these pool members fail to resolve.

Issue Resolved in 20.1.6-2p9

- AV-129587: After upgrade, some GSLB service members belonging to Avi sites can be marked *UP* even when member virtual services are down.

Issues Resolved in 20.1.6-2p8

- AV-128928: Server-initiated renegotiation was disabled in 20.1.5. This results in Server-initiated renegotiation failures for both Pools and HTTPS Health Monitor.
- AV-128843: Application traffic in a GSLB environment can get disrupted in upgrade scenarios in the following conditions:
  - GSLB service is configured with NO DATAPATH health monitors and relies on Controller-status.
  - GSLB federation is in maintenance mode
  - Site is upgraded to a newer version
- AV-127046: WAF tab in the UI is empty for some virtual services
- AV-118700: Service Engine can fail in some error conditions with the backend, when connection multiplexing is disabled.

Issues Resolved in 20.1.6-2p7

- AV-120361: Connection to pool server is not using the updated key/certificate in the SSLKeyAndCertificate object assigned to the pool.
- AV-122836: When GSLB leader site is represented with cluster VIP, configuration replication between sites is not working.
- AV-122772: When auto gateway is enabled, TCP Mss can be NULL for IPv6 connections.
- AV-123515: Support to use NSX-DC SP {Base, Advanced, Professional, Enterprise+} serial keys.
- AV-124931: Auto-download of CRS fails when proxy is configured.
- AV-125377: External health monitor is unable to invoke ping since it requires raw socket access privileges.
- AV-125824: If a bond exists on the management interface NICs (>=10G), it can be broken while stopping / restarting / upgrading the Service Engines in LSC deployments
- AV-126389: When RSS is enabled, packet buffers are not freed and eventually lead to connection failures due to a race condition during packet transmission on vNICs that have VLAN configured

Issue Resolved in 20.1.6-2p6

- AV-124588: HTTPS requests with chunked transfer encoding might timeout when DataScript or WAF is enabled on the virtual service.

Issues Resolved in 20.1.6-2p5

- AV-122365: AKO-created VIPs on AWS cloud may go down, if new FQDNs are added or removed from the Kubernetes Cluster ingresses
- AV-120361: Connection to pool server is not using the updated key/certificate in the SSLKeyAndCertificate object assigned to the pool

Issue Resolved in 20.1.6-2p4

- AV-121268: Inconsistent Network Interface MAC address/BDF to interface name mapping on Avi SE on CSP causes SE startup to fail or results in post-upgrade failure

Issues Resolved in 20.1.6-2p3

- AV-120542: Symptoms: Virtual Service traffic capture with GRO or TSO enabled system might lead to SE failure.
- AV-118802: System generates duplicate diffs for federated objects which can potentially lead to streaming of incorrect config objects to follower sites in a GSLB federation.
- AV-119449: Log manager runs into bad states if the log files get deleted when trying to get the file stats
- AV-118895: The life span of persistence entries is increased to 86400
- AV-117967: Static route is prioritised over connected route which can lead to incorrect routing of packets in write access environments

Issues Resolved in 20.1.6-2p2

- AV-117865: SE fail-over time SE is higher (more than three minutes) in AWS
- AV-116243: The Avi Controller on AWS C2S environment fails to create new SEs

Issues Resolved in 20.1.6-2p1

- AV-115729: Fixed cleanup of DHCP client on Avi interfaces upon SE shutdown
- AV-116043: Cluster events were not getting generated when the leadership changed in the cluster.
- AV-116206: dhclient anomaly in SE deployments in LSC deployments.
- AV-116327: The files in /var/lib/avi/systeminfo/ consume over 100 GB disk space.
- AV-117141: Configuring the PKI Profile object fails, when using Avi Vantage version 20.1.3 as x-avi-version, if the field Labels is a part of the configuration because the field Labels is deprecated and is no longer valid.
- AV-117414: Symptoms: If the L4 objects' name exceeded more than 128 bytes, it may cause the SE to fail.
- AV-117960: The Avi Controller upgrade with AWS cloud can fail if the cloud is in failed state.
- AV-118134: When a virtual service is configured with `use_vip_as_snat` or effectively using VIP IP as SNAT, consecutive migrations to the same SE may render the virtual service with that VIP inoperative.
- AV-118264: ICMP NAT may lead to SE failure with L4 NAT policy.
- AV-118468: A DNS VS created with System-UDP-Fast-Path (not recommended) can lead to flow table entry (subsequently memory) build-up upon reflection attack.
- AV-118786: License keys can be re-used on the same Controller causing unwanted increase on service core slots.

What's New in 20.1.6

Release date: 17 June 2021
To refer to the upgrade checklist, click here.

Automation

- Support for HashiCorp Network Infrastructure Automation (NIA)

- Avi Terraform Provider published to Terraform registry
- Avi Ansible Collection (Beta)

Load Balancing

- IPAM/ DNS: Infoblox: In an existing virtual service, the Allocation IP Type for an auto-allocated IP address can now be modified.
- Support to load balance Active FTP traffic for Active/Standby HA mode.

Networking

- BGP: Local AS Override for an iBGP Profile in VRF

Public/ Private Clouds

- AWS Auto scaling: Support for user-defined delay parameter before removing auto scaling group servers which have been marked down.
- NSX-T VLAN logical segment support for data network
- OpenStack: Open Virtual Network (OVN) support
- GCP: Shared VPC Multi-NIC support

Security

- Support for multiple authentication profiles for the Controller
- API/CLI support for triggering the renewal of SSL Certificates

WAF

- Simplified WAF policy when configuring via CLI/ API: CRS rules and application signature rules are derived from the `wafcrs` and `wafapplicationsignatureprovider` objects respectively to avoid redundancy.
- Consolidation for Learnt Data: Support for evaluating the URIs and consolidating the common section of the URI to reduce the programmed PSM location number.

Issues Resolved in 20.1.6

- AV-93678: SE failure may occur when FIX library with incorrect tag is present in the Tag group.
- AV-100542: NSX-T: When an interface is assigned static IP, the interface configuration may sometimes result in virtual service fault.
- AV-105267: CRL refresh can increase memory allocations into `SE_MTYPE_OPENSSL_CONN_128` instead of `SE_MTYPE_OPENSSL` due to an issue with memory accounting into incorrect type resulting in connection memory usage instead of configuration memory.
- AV-108871: Virtual service traffic may get affected on missing datapath rules due to race condition in an SE deployed in non-DPDK environments.
- AV-109476: Increased memory consumption on Controller after running show tech support.

- AV-110784: VMware vCenter Cloud: Avi cloud configuration stuck at *vCenter resyncing in progress* after datastore changes on vCenter.
- AV-111289: When a WAF policy is modified in UI automation or exported and then modified in the UI by adding new tags, and then imported again, the error Cannot change immutable field: tags is displayed.
- AV-111297: PUT/PATCH requests on `snmptrapprofile` fail with the error, String field community cannot contain special characters.
- AV-111556: Oracle Cloud: Service Engine failure due to port conflict on port 9003 with Oracle agent running in the Service Engine host virtual machine.
- AV-111655: In the Essentials License tier, creating and editing SSL certificates via the UI is not allowed
- AV-111683: Controller operations such as local configuration backup, scheduler events may fail when remote authentication via TACACS is enabled and the option Allow Local User Login is disabled.
- AV-111811: Using the @ipMatch operator in WAF rules may display the error message, Error in IpMatch operator if multiple IP addresses with different prefix length are used in this operator.
- AV-111857: L3 Scaled out VS during flow migration scenarios might cause the SE to fail.
- AV-111864: The number of virtual services per SE is limited to 1000, even for a use case where there are a few parents and hundreds of child virtual services
- AV-111906: When migrating to Avi Vantage version 20.1.3 or higher might fail if the `wafpolicypsmgroup` object contains a location that does not have any rules configured.
- AV-111940: When tunnel mode is enabled, receiving a packet when the virtual service is down, might cause SE failure.
- AV-112114: BGP multi-hop peering does not work with default routes.
- AV-112003: NSX-T: VLAN Management: SE fails to connect to the Controller in static IP mode if not L2 adjacent
- AV-112139: In the FIPS mode, SSH rekeying is not enforced to be triggered every one hour.
- AV-112191: Both response signing and assertion signing are required from the IDP side for successful SAML authentication after 20.1.1 Controller version.
- AV-112223: Cloud configuration specific to NSX-T gets reset to null when the NSX-T manager credentials are modified in the Cloud UI.
- AV-112246: AWS: The cloud image status is not updated to *Failed* on deletion of versioning-enabled S3 buckets.
- AV-112248: SE.pkg is not signed with the correct Secure Channel Certificate when upgraded from a version less than 18.2.6 (V1 to V2 upgrade)
- AV-112284: GSLB: When configuring a global service from the followers, the user credentials get printed along with the site information
- AV-120446: In Avi version 20.1.5, the SE has gemengine-1.3 that is not working for RSA ciphers when HSM is running in FIPS mode.
- AV-122365: AKO-created VIPs on AWS cloud may go down, if new FQDNs are added or removed from the Kubernetes Cluster ingresses

- AV-112512: In an Avi Controller version 20.1.3 through 20.1.5, the analytics profile may have incorrect values for fields like `disable_se_analytics`, `disable_ondemand_metrics` and `disable_vs_analytics` if the profile is created using APIs / SDKs and Avi API Version is less than 20.1.3.
- AV-112856: The Controller allows saving virtual service VIP FQDNs without a valid hostname.
- AV-113238: When configuring custom IP in the `IPReputationDB`, rules using is_good, reputation_type = avi.utils.get_ip_reputation(ip_addr) for types *CLOUD*, `TOR`, `MOBILE` may not work correctly.
- AV-113341: Objects are not filtered according to RBAC markers when queried with the UUID in the URL.
- AV-113532: Unable to load logs and events because the log indexer fails due to segment fault consistently when initializing.
- AV-113786: Azure: Service Engine may be falsely marked due to missing responses to Azure health check.
- AV-113939: The Service Engine fails when an HTTP/2 POST request is sent to a virtual service and all servers in the pool are down.
- AV-114228: Unable to load vCenter datastore in SE Group NSX-T cloud.
- AV-114203: Intensive WAF logging phase rules that operate on large amounts of data or use many macro expansions (for example, CRS 980100 and 980110), high Service Engine latency, or operating on large response bodies in WAF context can result in missing WAF logs.
- AV-114408: Service engine can fail during low memory conditions when the option `detect_ntlm_app` is enabled.
- AV-114426: Adding a policy match rule for cache-control or Pragma header might result in a Service Engine failure.
- AV-114653: Service engine fails when attempting to reuse a connection to the LDAP server that has already been closed.
- AV-115301: RBAC: Users with limited permissions (via markers/ labels) are sometimes unable to access objects.

Key Changes in 20.1.6

- Avi Vantage no longer supports VMware vCenter version 5.5. VMware completed End of General Support for vSphere 5.5 on September 29th, 2018.
  Before upgrading to Avi Vantage version 20.1.6, it is recommended to upgrade to a current vCenter version. For more information, refer to the System Requirements article.
- The virtual machine hardware version for the Avi Controller and the Avi Service Engines has been updated from version 10 to version 11. On upgrade, existing Controllers and Service Engines will continue on version 10. New Service Engines created after upgrade to 20.1.6 will use version 11.
- The Controller OVA image is now a signed image. This ensures that any attempts to tamper with the OVA file result in an exception when deploying the OVA.
- The Avi Controller OVA supports additional OVF properties. The following properties have been added to facilitate automated deployment of the Avi Controller by the NSX Manager in a future release:
  - NSX-T Node ID
  - NSX-T IP Address
  - Authentication token of NSX-T

  - NSX-T thumbprint
  - Hostname of Avi Controller

These fields should be left blank in case of a direct deployment of the Avi Controller.

- WAF Policy:
  - The fields `crs_groups` and `application_signature.rules` are deprecated.
  - In the CLI/ API, to override attributes of the CRS or application rules, use the new `crs_groups_overrides` and `application_signature.rule_overrides` instead.
- The minimum value for X-Avi-Version that can be used when interacting with the Avi Controller is 18.2.6. It is recommended to update the automation assets, as required.

Known Issues in 20.1.6

- AV-115513: LSC:
  - Upgrade/patch may not work if the Controller is running as a container on a host running RHEL 8.x, Ubuntu 18.04 or Ubuntu 20.04.
  - Podman version higher than 1.6.4 is not supported.
- AV-142641: Macro API for virtual service deletion does not support API migration below X-Avi-Version 20.1.1.

## Checklist for Upgrade to Avi Vantage Version 20.1.6 Refer to this section before initiating upgrade.

- Upgrading to Avi Vantage version 20.1.6 is supported from any of the following versions:
  - Avi Vantage version 17.2.x
  - 18.2.1 through 18.2.12
  - Avi Vantage version 20.1.x

  Note: Upgrade from version 18.2.13 and higher to version 20.1.6 is not supported.
  For more information refer to:
  - Upgrade from Avi Vantage release 18.2.6 or higher
  - Upgrade from a version prior to Avi Vantage release 18.2.6

- Starting with Avi Vantage release 20.1.1 as per the HTTP/2 RFC, the cipher suites with TLS 1.2 listed here are not supported. Remove the ciphers before initiating upgrade to Avi Vantage version 20.1.1.

- Avi Vantage no longer supports VMware vCenter version 5.5. The End of General Support for vSphere 5.5 by VMware was on September 29th, 2018.
  Before upgrading to Avi Vantage version 20.1.6, it is recommended to upgrade to a current vCenter version. For more information, refer to the System Requirements article.

- An Avi Vantage deployment with FIPS mode enabled prior to 20.1.5, cannot be upgraded.

- Starting with Avi Vantage 20.1.5, the NSX-V Cloud Connector is not supported. The NSX-V cloud was deprecated in version 20.1.3, and is now unsupported. It is recommended to migrate to an NSX-T cloud connector, or switch to no-orchestrator mode with NSX-V.

- Starting with Avi Vantage version 20.1.1, the default disk size for new SEs is now 15 GB.
  For OpenStack deployments, ensure that the disk size for the requisite flavors is increased to a minimum of 15 GB

- Starting with Avi Vantage version 20.1.1, the Avi Controller and Service Engines use Python 3. Refer to the migration notes in the following sections:

  - For ControlScripts

    - For Python-based External Health Monitors

- Licensing Management of the Avi Service Engines has been updated. Refer to the Avi Vantage License Management article for more information.
- Avi Vantage now enforces system limits based on Controller cluster size. Refer to the System Limits article for more information.
- In case of Service Engine upgrade in a Nutanix Acropolis Hypervisor (AHV) environment, refer to the pre-upgrade changes.
- Starting with version 20.1, Avi Vantage has moved from Lua 5.1 to LuaJIT for compiling and running DataScripts. LuaJIT is relatively more restrictive with non-defined escape sequences. Using any escape sequence other than ones supported, (as defined in the Lua 5.1 Reference Manual) results in a compile error. Before upgrading to version 20.1 or higher, ensure the DataScripts do not use undefined escape sequences.
  If the DataScripts are not fixed before upgrade, the DataScripts using non-defined escape sequences, which worked earlier will now cause the virtual service to go down.

Issues Resolved in 20.1.5 Patch Releases

Issues Resolved in 20.1.5-2p12

- AV-129536: vCenter cloud may go down with vcenter 7.0 and above.
- AV-135843: After applying the Controller patch, the indexer service fails.
- AV-140366: Mitigation for CVE-2022-0778.
- AV-141095: Request timeout on a virtual service when the DataScript line `avi.http.response(200)` is called in the Response Event.
- AV-142624: Events and logs are timing out and new events/logs are not visible on the UI/API. When the log manager indexes a file, if the file is corrupted or not able to read the log from the file, the indexer is stuck in loops.
- AV-144621: vCenter cloud discovery might fail with inventory state VCENTER_INVENTORY_RETRIEVING_DC in vCenter cloud version 7.0 and higher.
- AV-132431: Mitigation for CVE-2021-44228.

Issues Resolved in 20.1.5-2p11

- AV-138792: Service Engine might crash with the combination of Error page configuration on failed requests and Clients sending pipelined HTTP posts on the same front end TCP connection.
- AV-136068: Service Engine failure due to insufficient memory.
- AV-135843: After applying the Controller patch, the indexer service fails.
- AV-134355: When a network's name is changed in the Controller, the name change does not reflect in the corresponding `NetworkRuntime` object.
- AV-133360: Remote_site_watcher process can get stuck if there is a GRPC connection failure during resync process.
- AV-131472: Auto-download of CRS via Pulse fails
- AV-122836: When GSLB leader site is represented with cluster-VIP, configuration replication between sites is not working.
- AV-115393: The vCenter cloud may go down during the inventory processing of Distributed Virtual Port Group / VM / Hosts.

Issues Resolved in 20.1.5-2p10

- AV-128998: The Remote Site Watcher Sync fails if Leader is of version 20.1.1 or above until 20.1.5 and Follower is of version 20.1.5 or above. This is because of uncommon federated objects list. To avoid this scenario, the objects to be synced are considered to be only the common objects between the leader and follower.

- AV-125824: If a bond exists on the management interface NICs (>=10G), it can be broken while stopping / restarting / upgrading the Service Engines in LSC deployments
- AV-98655: TSO offload does not work if one of the member interfaces in inactive at the time of bond creation.

Issues Resolved in 20.1.5-2p9

- AV-126389: When RSS is enabled, packet buffers are not freed and eventually lead to connection failures due to a race condition during packet transmission on vNICs that have VLAN configured
- AV-125377: External health monitor is unable to invoke ping since it requires raw socket access privileges.

Issues Resolved in 20.1.5-2p8

- AV-124931: Auto download of CRS fails when proxy is configured.
- AV-120446: In Avi version 20.1.5, the SE has gemengine-1.3 that is not working for RSA ciphers when HSM is running in FIPS mode.

Issues Resolved in 20.1.5-2p7

- AV-119952: Fetching GSLB status is leading to high CPU usage of DBcache, which maybe effecting the inventory processing times.

Key Changes in 20.1.5-2p7

- AV-120066: By default faults are not available in the inventory APIs. A query parameter to include faults is introduced in the inventory APIs.

Issue Resolved in 20.1.5-2p6

- AV-118277: High disk usage on Service Engine because of IP reputation files consuming space

Issues Resolved in 20.1.5-2p5

- AV-118500: Self-signed certificates and certificate signing requests generated on the Controller are created correctly when using HSM.
- AV-117720: App Cookie persistence fails when used in combination with the avi.http.remove_header ("Set-Cookie") and avi.http.add_header ("Set-Cookie") DataScript APIs, if the app cookie persistence and DataScript are on the same virtual service.
- AV-117388: Cluster-based alerts are not generated for cluster fail over events.
- AV-116620: In an OpenStack cloud, the Service Engine Group page is inaccessible via the UI.
- AV-116440: Moving a rule in HTTP policy under Virtual Service >Policies>HTTP Requests>Move To does not work.
- AV-116157: Traffic logs are not displayed in the Avi UI. On the Controller, no matching log files are synced from the SE. Delayed response to log queries due to timeout on the Controller.

Issues Resolved in 20.1.5-2p4

- AV-115671: In an OpenStack cloud, the Controller can initiate multiple addition of vNIC operations on the SE for the same network and VRF before the vNIC IP limit is reached, causing potential traffic issues.
- AV-115729: The SE is not connected to the Controller after the se_dp process is stopped.
- AV-115732: `se_dp` and `se_ns_helper` failure seen after SE reboot.
- AV-116043: Cluster events were not getting generated when the leadership changed in the cluster.
- AV-116148: The status of a successful application signature sync is displayed as Failed in the UI.
- AV-116206: dhclient anomaly in SE deployments in LSC deployments.
- AV-116327: The System info folder (/var/lib/avi/systeminfo/) becomes larger in size and occupies large disk space.

- AV-116411: Service Engine fails when a HTTP/1.0 request is sent without a Host header to a virtual service with a pool with both HTTP/2 and SSL enabled.
- AV-116418: Service Engine fails when running the DataScript with the function call avi.http.get_host_tokens ("MODIFIED") over HTTP/1.0 traffic that does not have the Host headers.
- AV-117141: Configuring the PKI Profile object fails, when using Avi Vantage version 20.1.3 as x-avi-version, if the field Labels is a part of the configuration because the field Labels is deprecated and is no longer valid.
- AV-111669: In LSC clouds, with underlying host running cgroup v1, SE processes can be stuck in deactivating state due to SE failure or reboot.

Issues Resolved in 20.1.5-2p3

- AV-113939: Service Engine fails when an HTTP/2 POST request is sent to a virtual service and all servers in the pool are down.
- AV-113532: Log indexer fails due to segment fault consistently when initializing. The UI is unable to load any logs and events.

Issues Resolved in 20.1.5-2p2

- AV-114228: Unable to load vCenter datastore in SE Group NSX-T cloud
- AV-114367: In AWS deployments with DPDK mode and MTU greater than 1500, whenever the packet received from the driver is greater than 2048 (which is the mbuf data buffer length), the packet length of the chained packets are not getting updated right in ENA driver.

What's New in 20.1.5-2p1

- CLI support for triggering renewal for SSL certificates

Issues Resolved in 20.1.5-2p1

- AV-111556: Upgrade to 20.1.4 on Oracle Enterprise Linus (OEL)-based LSC cloud system fails due to port conflict with Oracle agent running on that host.
- AV-111655: In the Essentials License tier, creating and editing SSL certificates via the UI is not allowed
- AV-111857: ECMP hash change for a multi-homed BGP virtual service can cause SE failure.
- AV-111864: The number of virtual services per SE is limited to 1000, even for a use case where there are a few parents and hundreds of child virtual services
- AV-111940: An environment with tunnel mode on may fail if the virtual service receives a packet while the virtual service is down.
- AV-113786: Azure: Echo server cannot handle multiple connections. This causes the SE to be falsely marked down from the NSX Advanced Load Balancer
- AV-112003: NSX-T (VLAN Management): The SE is not connecting to the Controller in static mode if not L2 adjacent.
- AV-112114: The eBGP multi-hop peering does not work with default routes.
- AV-112139: In FIPS mode, SSH Rekeying is not enforced to be triggered every one hour.
- AV-112191: Both response signing and assertion signing are required from the IDP side for successful SAML authentication after 20.1.1 Controller version.
- AV-112248: SE.pkg is not signed with the correct Secure Channel Certificate when upgraded from a version less than 18.2.6 (V1 to V2 upgrade).
- AV-112284: GSLB Service updates from the follower node print the site configuration including the user credentials.
- AV-112512: Creating the Analytics Profile using the pre-20.1.3 version API client on a Controller of version higher than 20.1.3, the configuration fields like `disable_se_analytics`, `disable_ondemand_metrics` and `disable_vs_analytics` are updated incorrectly.
- AV-113341: Objects are not filtered according to RBAC markers when queried with uuid in URL.

What's New in 20.1.5

Release date: 16 April 2021
To refer to the upgrade checklist, click here.

Analytics

- Health Monitor: Support for mail protocols: POP3, IMAP, SMTP

DNS

- DNS resolution on the Service Engine

Ecosystem

- LSC: Support for Ubuntu 18.04 and 20.04 as host OS

GSLB

- Support to enable/ disable GSLB pool members from any site
- UI support to select a DNS virtual service defined in other tenants in the GSLB site configuration

IPv6

- Proxy Protocol: IPv6 support

Licensing

- Introduction of Essentials Controller (4 core / 12 GB RAM) for Avi Essentials Edition

Networking

- BGP: UI for Support for BGP AS-Path Prepend and Local Preference
- BGP: Selective VIP advertisement
- Wildcard VIP: Placement support for LSC/No Access clouds for multi-vnic

Public/ Private Cloud

- OpenStack: Support for OpenStack Victoria
- NSX-T: VLAN logical support for SE's management network.
  Note: VLAN logical support for Data network is also available in the tech preview mode and should be used only for POC/ testing.

Security

- WAF: Application Rules support
- UI support for IP Reputation Database
- HSM: Support for Thales Luna 7.3.3
- HSM: Dedicated interface for HSM on Service Engine for a no-orchestrator environment

System

- FIPS 140-2 support for Avi Vantage
- Support for field level RBAC for specific objects

- Enhancements to the Granular RBAC feature

Issues Resolved in 20.1.5

- AV-98217: Unable to create service engines when the vCenter 7.0 and vSAN datastore combination is used in NSX-T
- AV-100302: VIP advertisement for a BGP virtual service may fail after the virtual service is flapped by its health monitor if the virtual service shares its pool with the other virtual services
- AV-102065: SSL secure renegotiation is enabled on Avi. This allows clients to do secure renegotiation which is not intended and should not be allowed.
- AV-102957: Email messages configured to be sent as part of an alert action may error out and remain unsent
- AV-103912: Service Engine self election does not work properly when Infoblox IPAM is configured in a no access, vCenter, or Linux Server Cloud
- AV-104019: Import of certificates failed if the key is of type EC and is encrypted using des or aes256
- AV-104715: Service engine failed to detect link state change for vmxnet3 NIC in vCenter
- AV-104837: Health monitor response is not parsed correctly if the content length header is not present
- AV-105461: UI shows SE state as `Pending` even after the SE is disabled
- AV-105629: Linux Server Cloud: Attach IP timed out is displayed on a shared VIP-virtual service after SE reboot
- AV-106057: If a pool is configured with a file larger than 16K to be sent as local response in case the pool is down, the response recieved by the client is partial
- AV-106147: Syslog messages are displayed incorrectly with an extra character (b)
- AV-106169: Port-channel initialisation might fail in service engine running on CSP
- AV-106265: When RBAC is used, the error Unauthorized (403) is displayed when:
  - changing the fields for a labelled object
  - request for Patch of a labelled object
- AV-106362: Updating a DNS policy with site selection having a fall back site, may result in SE failure
- AV-106363: If the SEs are running older versions and the Controller is running version 20.1.3, the virtual service logs may not be indexed if the log contains non utf-8 characters
- AV-106432: Data from the socket was not drained when RST and the data were processed/received at the same time on the SE. This results in partial data being delivered to the client from the server
- AV-106907: LDAP auth does not work if `ignore_referrals` is set to *true* in LDAP settings
- AV-106917: Remote backup fails if cloud connector user is created with auto-generated key pair
- AV-107313: SE might fail due to incorrect route label reference
- AV-107491: Sorting by health score is disabled for the virtual service list
- AV-108086: Exception while listing networks/domains in AWS IPAM/DNS Profile
- AV-108224: When editing an IP address group that is used in ssh access list, the error message Not allowed to remove controller ips when associated with ssh access listis displayed
- AV-108237: Avihost service fails to start if the executive path is not absolute
- AV-108371: When exporting all pages under logs for a virtual service from the UI, the error `identified_ciphers` is displayed
- AV-108490: HTTP Response policy matches can cause Service Engine failure, when request is served from the cache
- AV-108983: Zombie processes keep accumulating in the Service Engine
- AV-109358: Virtual service labels are not exported during upgrade
- AV-109440: New Service Engine fails to boot up initially and then boots up fine to connect to the Controller on its own upon reboot
- AV-109441: Unable to add a BGP peer in the network belonging to the admin's global VRF when using per tenant VRF in vCenter
- AV-109728: L7 VS: When server sends a non-compliant response without a status line, the client cannot detect the content/payload.
- AV-110167: NSX-T: Virtual service updates (enable/disable) does not result in the removal of virtual service related NSGroups.
- AV-112003: NSX-T: VLAN Management: SE is not connecting to the Controller in static mode if not L2 adjacent

Key Changes in 20.1.5

- NSX-V Cloud Connector is no longer supported
- HTTP requests served from the cache will not have HTTP Response Policies applied to it, if configured.
- In vCenter cloud configuration, support to store only the SE VM?s in the datastore during the inventory discovery process
- The flag `avi.http.get_host_tokens()` is introduced to specify if the original host header tokens have to be returned or the host header tokens
- SSL Secure renegotiation will be disabled on Avi. Avi will respond with a 'no_renegotiation' alert to clients attempting to initiate a secure renegotiation. In cases like TLS persistence, Avi can still initiate secure renegotiation with the client.
- Depending on the role filter, only the VSVIPs that the user has access to are visible
- When using per tenant VRF in vCenter, a BGP peer network belonging to the global VRF configuration can be added.
- Virtual services in the OpenStack cloud may go down if Keystone returns 404 Not Found for a tenant.The Avi Controller will not automatically delete the Avi SE and related resources from OpenStack when project/tenant is deleted from OpenStack. Avi will delete the resources when users delete the virtual service configuration and imported tenant from Avi.
- Only the last 200 alert objects will be exported during a scheduled backup
- The minimum value for X-Avi-Version that can be used when interacting with the Avi Controller is 18.2.6. It is recommended to update the automation assets, as required.

Known Issues in 20.1.5

- AV-111588: System compliancemode initiates FIPS upgrade irrespective of whether FIPS mode is already enabled
- AV-111633: Avi pre-upgrade check might fail for OpenStack releases Ussuri or Victoria if the Glance multi store backend feature is enabled in OpenStack.
- AV-112223: Cloud configuration specific to NSX-T gets reset to null when the NSX-T manager credentials are modified in the Cloud UI.
  Work Around: Use the CLI or navigate to Administration > User Credentials to update the credentials.
- AV-112248: SE.pkg is not signed with correct Secure Channel Certificate when upgraded from a version less than 18.2.6 (V1 to V2 upgrade).
- AV-115513: LSC:
  - Upgrade/patch may not work if the Controller is running as a container on a host running RHEL 8.x, Ubuntu 18.04 or Ubuntu 20.04.
  - Podman version higher than 1.6.4 is not supported.

- AV-142641: Macro API for virtual service deletion does not support API migration below X-Avi-Version 20.1.1. ## Checklist for Upgrade to Avi Vantage Version 20.1.5 Refer to this section before initiating upgrade.

- Upgrading to Avi Vantage version 20.1.5 is supported from any of the following versions:
  - Avi Vantage version 17.2.x
  - 18.2.1 through 18.2.12
  - Avi Vantage version 20.1.x

  Note: Upgrade from 18.2.13 and higher to 20.1.5 is not supported.
  For more information refer to:
  - Upgrade from Avi Vantage release 18.2.6 or higher
  - Upgrade from a version prior to Avi Vantage release 18.2.6

- Starting with Avi Vantage release 20.1.1 as per the HTTP/2 RFC, the cipher suites with TLS 1.2 listed here are not supported. Remove the ciphers before initiating upgrade to Avi Vantage version 20.1.1.

- An Avi Vantage deployment with FIPS mode enabled prior to 20.1.5, cannot be upgraded to 20.1.5.

- Starting with Avi Vantage 20.1.5, the NSX-V Cloud Connector is no longer supported. NSX-V Cloud was deprecated in version 20.1.3, and is now unsupported. It is recommended to migrate to an NSX-T cloud connector, or switch to no-orchestrator mode with NSX-V.
- Starting with Avi Vantage version 20.1.1, the default disk size for new SEs is now 15 GB.
  For OpenStack deployments, ensure that the disk size for the requisite flavors is increased to a minimum of 15 GB
- Starting with Avi Vantage version 20.1.1, the Avi Controller and Service Engines use Python 3. Refer to the migration notes in the following sections:
  - For ControlScripts
  - For Python-based External Health Monitors
- Licensing Management of the Avi Service Engines has been updated. Refer to the Avi Vantage License Management article for more information.
- Avi Vantage now enforces system limits based on Controller cluster size. Refer to the System Limits article for more information.
- In case of Service Engine upgrade in a Nutanix Acropolis Hypervisor (AHV) environment, refer to the pre-upgrade changes.
- Starting with version 20.1, Avi Vantage has moved from Lua 5.1 to LuaJIT for compiling and running DataScripts. LuaJIT is relatively more restrictive with non-defined escape sequences. Using any escape sequence other than ones supported, (as defined in theLua 5.1 Reference Manual) results in a compile error. Before upgrading to version 20.1 or higher, ensure the DataScripts do not use undefined escape sequences.
  If the DataScripts are not fixed before upgrade, the DataScripts using non-defined escape sequences, which worked earlier will now cause the virtual service to go down.

20.1.4 Patch Releases

Issues Resolved in 20.1.4 Patch Releases

Issues Resolved in 20.1.4-2p26

- AV-143121: Symptoms: With Infoblox IPAM, if an invalid domain is specified in the configuration, host record creation requests result in a timed-out error from Infoblox leading to the leader node UI and CLI getting unresponsive.
- AV-142624: Events and logs are timing out and new events/logs are not visible on the UI/API. When the log manager indexes a file, if the file is corrupted or not able to read the log from the file, the indexer is stuck in loops.
- AV-140278: In setups with GSLB site persistence pools, inventory API calls will fail or time out due to a class name reference error in Network Manager.

Workarounds: Change line 3316: "global_vrf = VrfContext.objects.get(cloud_ref__uuid=cloud_pb.uuid, name='global')" to "global_vrf = models.VrfContext.objects.get(cloud_ref__uuid=cloud_pb.uuid, name='global')" in /opt/avi/python/bin/portal/nonportal/management/commands/network_manager.py. Then perform a controller warmstart.

Issues Resolved in 20.1.4-2p25

- AV-135843: After applying the Controller patch, the indexer service fails.
- AV-133360: `Remote_site_watcher` process can get stuck if there is a GRPC connection failure during the resync process.
- AV-122836: When GSLB leader site is represented with cluster-VIP, configuration replication between sites is not working.

Issues Resolved in 20.1.4-2p24

- AV-117427: Changing `default_minimum_api_timeout` does not reflect in all locations
- AV-100844: Virtual service status is down with the error "Cloud configuration failed"

Issues Resolved in 20.1.4-2p23

- AV-136104: Added support for kernel version 3.10.0-1160.53.1.0.1.el7.x86_64
- AV-136013: Reduce number of API calls to OpenStack Neutron and Nova.
- AV-134455: If a vCenter network name is changed after the Controller has already discovered the network, the name change is not reflected in the corresponding Controller network object.
- AV-131472: Auto-download of CRS via Pulse fails

Issue Resolved in 20.1.4-2p22

- AV-129150: NSX Advanced Load Balancer creates empty storage accounts on Azure cloud.

Issues Resolved in 20.1.4-2p21

- AV-132431: Mitigation for [CVE-2021-44228](CVE-2021-44228).
- AV-131181: On receiving streamed logs, the reported timestamp in the log messages sometimes is displayed as PST time, if the Service Engine of the customers is configured to use PST as the system time zone.
- AV-130174: For logs streaming in Syslog format, at times the Application profile UUID is included as App-name in header instead of the virtual service name.
- AV-127046: WAF tab in the UI is empty for some virtual services. ### Issue Resolved in 20.1.4-2p22
- AV-129150: NSX Advanced Load Balancer creates empty storage accounts on Azure cloud.

Issues Resolved in 20.1.4-2p20

- AV-131448: Added support for Linux kernel 3.10.0-1160.49.1.el7
- AV-128998: The Remote Site Watcher Sync fails if Leader is of version 20.1.1 or above until 20.1.5 and Follower is of version 20.1.5 or above. This is because of uncommon federated objects list. To avoid this scenario, the objects to be synced are considered to be only the common objects between the leader and follower.
- AV-128228: `SE_SYN_TABLE_HIGH` alerts are seen for large number of embryonic connections without necessarily the underlying system under attack or memory stress.
- AV-125592: Controllers do not get license capacity when user uploads NSX serial keys with zero quantity (unlimited licenses). Serial key gets added with zero service cores.
- AV-118134: When a virtual service is configured with `use_vip_as_snat` or effectively using VIP IP as SNAT, consecutive migrations to the same SE may render the virtual service with that VIP inoperative.

What's New in 20.1.4-2p19

- Support to use NSX-DC SP (Base, Advanced, Professional, Enterprise+) serial keys.
- Support for kernel version 3.10.0-1160.45.1.el7.x86_64

Issues Resolved in 20.1.4-2p19

- AV-125824: If a bond exists on the management interface NICs (>=10G), it can be broken while stopping / restarting / upgrading the Service Engines in LSC deployments

- AV-126508: BGP: Virtual service scale in can result in minor traffic disruption.

- AV-127278: Existing static routes are overwritten due to pagination issues on the UI.

Issues Resolved in 20.1.4-2p18

- AV-126389: When RSS is enabled, packet buffers are not freed and eventually lead to connection failures due to a race condition during packet transmission on vNICs that have VLAN configured.
- AV-126153: When a patch is applied to the Controller or the SE, file extraction can fail in some scenarios causing the patch operation to abort.
- AV-126148: The Avi cloud connector fails to sync AWS Auto scaling groups if there are more than 200 servers in the cloud.
- AV-125377: External health monitor is unable to invoke ping and other similar utilities or applications that require raw socket access privileges.

Issue Resolved in 20.1.4-2p17

- AV-125682: GCP cloud is failing to connect to the GCP API servers with `x509.CertificateInvalidError` when `crypto/tls/fipsonly` package is enabled.

Issue Resolved in 20.1.4-2p16

- AV-123972: Scaled out virtual service with an invalid port value of 0 may cause SE failure.

What's New in 20.1.4-2p15

- Support for kernel version 3.10.0-1160.41.1.el7.x86_64

Issues Resolved in 20.1.4-2p15

- AV-124931: Auto-download of CRS fails when proxy is configured
- AV-118269: Network resolution of GSLB site persistence pool fails when using per tenant VRF in vCenter, leading to VS placement failing if site persistence is enabled before the virtual service is placed on all requested number of SEs.
- AV-116516: Graceful disable os server does not work for existing client connections to an L7 virtual service even when connection multiplex is disabled

Issue Resolved in 20.1.4-2p14

- AV-121569: Symptoms: Log file manager didn't clean up event files correctly Workarounds: Changing the logic to filter the possible open file for 'avi-portal' process.

Issue Resolved in 20.1.4-2p13

- AV-119921: In a persistence profile, the `ip_mask` behaves as an inverse CIDR mask and distributes the clients across servers instead of ensuring the clients in the same subnet are connected to the same servers.

Issues Resolved in 20.1.4-2p12

- AV-120947: LSC: Support for base kernel version 3.10.0-1160.36.2.el7
- AV-120542: Virtual Service traffic capture with GRO or TSO enabled system might lead to SE failure.

Issues Resolved in 20.1.4-2p11

- AV-119946: Logs are missing when the query contains a large number of logs and the query timeout has expired.
- AV-119491: Symptoms: When using auto allocation with cloud native IPAM in AWS cloud, a virtual service VIP update which removes the existing VIP level `subnet_uuid` and `ipam_network_subnet` level `network_uuid` and `subnet_uuid` fields while keeping the same `ipam_network_subnet` subnet CIDR will result in the VIP getting a new IP, but the new IP will not be attached in the cloud.

- AV-118802: System generates duplicate diffs for federated objects which can potentially lead to streaming of incorrect config objects to follower sites in a GSLB federation
- AV-117961: Disk clean does not happen if the data is mounted to a different file system.
- AV-116620: In an OpenStack cloud, the Service Engine Group page is inaccessible via the UI.

Issues Resolved in 20.1.4-2p10

- AV-116440: Moving a rule in HTTP policy under Virtual Service >Policies>HTTP Requests>Move To does not work.
- AV-117960: The Avi Controller upgrade with AWS cloud can fail if cloud is in failed state.
- AV-118264: ICMP NAT may lead to SE failure with L4 NAT policy.
- AV-118277: SE might see high disk usage since ip_reputation database files are consuming space.
- AV-111295: Incorrect accounting of half-opened connections in closed TCP Health Monitors lead to reporting of high dropped connections. DSR

Issues Resolved in 20.1.4-2p9

- AV-115729: The SE is not connected to the Controller after the se_dp process is stopped.
- AV-115732: `se_dp` and `se_ns_helper` failure seen after SE reboot
- AV-116043: Cluster events were not getting generated when the leadership changed in the cluster.
- AV-116206: `dhclient` anomaly in SE deployments in LSC deployments
- AV-116243: Avi Controller on AWS EC2 environment fails to create new SEs.
- AV-116327: The System info folder (/var/lib/avi/systeminfo/) becomes larger in size and occupies large disk space.
- AV-116411: Service Engine fails when a HTTP/1.0 request is sent without a Host header to a VS with a pool with both HTTP/2 and SSL enabled.
- AV-116418: Service Engine fails when running the DataScript with the function call avi.http.get_host_tokens ("MODIFIED") over HTTP/1.0 traffic that do not have the Host headers.

Issues Resolved in 20.1.4-2p8

- AV-114660: Reclaimed additional memory used by SE datapath interfaces in non-DPDK mode of operation.
- AV-114426: Undefined behavior when adding a policy match rule for cache-control or Pragma header which may result in a Service Engine failure
- AV-113257: Syslog is sending out duplicate messages for every event
- AV-108371: Exporting all logs via the UI for a virtual service using Export (All Pages) , displays the error "identified_ciphers".
- AV-105629: Symptoms: UI does not show the placement networks from the global VRF when configuring Virtual Service from within a tenant with per-tenant VRF in vCenter cloud.
- AV-105267: CRL refresh could increase memory allocations into SE_MTYPE_OPENSSL_CONN_128 instead of SE_MTYPE_OPENSSL. It is only an issue with memory accounting into incorrect type resulting in connection memory usage instead of config memory.

What's New in 20.1.4-2p7

- GCP: RSS capability on GCP virtio interfaces in DPDK mode

Issues Resolved in 20.1.4-2p7

- AV-114772: Datapath isolation enabled on a host with hyperthreading, results in incorrect number of non-datapath CPUs in the se_root cpuset. The issue is seen on a host with 2 physical cores i.e. 4 vCPUs (logical cores).
- AV-109476: Increased memory consumption on the Controller after show tech support has been run.

Key Changes in 20.1.4-2p7

AV-109790: SE-DP isolation mode isolates the data path instances from other processes, improving latency and jitter tolerance of the solution.

Issues Resolved in 20.1.4-2p6

- AV-114367: In AWS deployments with DPDK mode and MTU greater than 1500, whenever the packet received from the driver is greater than 2048 (which is the mbuf data buffer length), the packet length of the chained packets are not getting updated right in ENA driver.
- AV-113786: Azure: Echo server cannot handle multiple connections. This can cause SE to be falsely marked down from ALB
- AV-112512: Creating the Analytics Profile using the pre-20.1.3 version API client on a Controller of version higher than 20.1.3, the configuration fields like `disable_se_analytics`, `disable_ondemand_metrics` and `disable_vs_analytics` are updated incorrectly.
- AV-111683: Controller operations such as local configuration backup, scheduler events may fail when remote authentication via TACACS is enabled and the option Allow Local User Login is disabled.
- AV-111556: Upgrade to 20.1.4 on Oracle Enterprise Linux (OEL)-based LSC cloud system fails due to port conflict with Oracle agent running on that host.

Issues Resolved in 20.1.4-2p5

- AV-108871: Virtual service traffic may get affected on missing datapath rules due to race condition in an SE deployed in non-DPDK environments.
- AV-109965: Application Signature fails when the app signature portal URL is not reachable
- AV-112191: Response signing and assertion signing have to be enabled on the IDP for successful SAML authentication after upgrade to 20.1.1 Controller version.
- AV-112114: eBGP multi-hop peering does not work with default routes.
- AV-111940: Environment with tunnel mode on may fail if the virtual service receives a packet while the virtual service is down.
- AV-111857: ECMP hash change for a multi-homed BGP VS might cause SE failure.
- AV-111456: Under heavy load of Events from SE, the redis server memory can increase causing a warm start of the Controller node
- AV-111297: PUT/PATCH requests on `snmptrapprofile` fails with the error that `String field community cannot contain special characters`
- AV-110808: When alert actions are executed in a sequence as specified in the UI, an error in executing one alert action stops triggering the remaining actions in the sequence.
- AV-110784: When configuring the cloud or discovering objects, the cloud configuration was stuck displaying the status *vcenter resyncing in progress.*

Issues Resolved in 20.1.4-2p4

- AV-111436: For clouds with L3-scale-out, heartbeat exchange between SEs fails.
- AV-111120: API calls fail due to high memory usage by reds server
- AV-109873: In case there are Service Engines in lower version, datastore takes a long time to be populated.
- AV-109871: When a cloud object which has hyphens in the prefix name is updated, the error Error in updating cloud NSX-T-Prod: Cloud Object Prefix Name must have only letters, numbers and underscore is displayed.
- AV-107744: Cluster IP configuration for Azure controller does not work with proxy configured
- AV-105638: Linux Server Cloud: Attach IP timed out is displayed on a shared VIP-virtual service after SE reboot

Issues Resolved in 20.1.4-2p3

- AV-108983: Zombie processes keep accumulating in the Service Engine
- AV-108845: `avi.http.get_host_tokens()` always returns the original host header. Any modification done to the host header via HTTP policy actions are not reflected in the value returned by this API.
- AV-108490: HTTP Response policy matches can cause Service Engine failure, when the request is served from the cache.
- AV-107744: Cluster IP configuration for the Azure Controller does not work with proxy configured

Key Changes in 20.1.4-2p3

- AV-102065: SSL Secure renegotiation will be disabled on Avi. Avi will respond with a 'no_renegotiation' alert to clients attempting to initiate a secure renegotiation. In cases like TLS persistence, Avi can still initiate secure renegotiation with the client.

Issues Resolved in 20.1.4-2p2

- AV-109441: When using per tenant VRF in vCenter, it is unable to add a BGP peer in a network belonging to the admin's global VRF
- AV-109440: On Service Engine creation, SE fails initial boot up sequence and recovers on a reboot
- AV-108680: VLAN interface configuration removed from SE after upgrade to Avi Vantage version 20.1.4
- AV-108237: The Avihost service fails to start and displays the error Executable Path is not absolute.
- AV-107491: Sorting by health score is disabled for the virtual service list.
- AV-106265: Unauthorized (403) is displayed when changing fields or requesting for a PATCH of a labelled object
- AV-106147: Syslog messages are displayed incorrectly with an extra character (b)
- AV-100302: VIP advertisement for a BGP virtual service may fail after the virtual service is flapped by its health monitor if the virtual service shares its pool with the other virtual services

Issues Resolved in 20.1.4-2p1

- AV-106917: Remote backup fails if the cloud connector user is created with auto-generated key pair
- AV-106907: LDAP auth does not work if `ignore_referrals` is set to *true* in LDAP settings
- AV-105461: UI shows SE state as *Pending* even after the SE is disabled
- AV-102957: Email messages configured to be sent as part of an Alert action may error out and remain unsent.

What's New in 20.1.4

Release date: 15 February 2021
To refer to the upgrade checklist, click here.

Analytics

- TLS encryption support for application virtual service log streaming

Automation

- The Avi Terraform provider is migrated to HashiCorp's Terraform registry

EDNS

- EDNS support for SE generated responses

WAF

- Consolidation of URI using prefixes to reduce the number of programmed locations

Public Cloud

- AWS: Server Autoscale: During scale in, Avi autoscale ensures balance of servers across different AWS availability zones

Issues Resolved in 20.1.4

- AV-56759: For local entries ECS data not included in response
- AV-88824: After disabling all the policies used by the pool, the pool's oper status shows `oper_inactive` instead of `oper_unknown`
- AV-99447: With RBAC using labels, an object created in Admin tenant is not viewable in other tenants
- AV-99106: The service engine may fail to get configuration updates from the Controller due to error in the GRPC channel
- AV-102318: The Config Migration step in upgrade fails due to exception in `metrics_db` migration
- AV-102822: Granular RBAC configuration in the basic configuration mode of a virtual service breaks the logical workflow
- AV-102892: In a No-Orchestrator deployment, a virtual service using a VLAN interface goes into fault state with reason Failed to add virtual service to the interface
- AV-102954: Real time analytics and non-significant logs are not enabled for 30 minutes when a virtual service is created through the UI
- AV-103171: Under low memory conditions, memory allocation failures can cause an SE failure when HTTP-to-HTTPS redirect is enabled
- AV-103177: The iptables rules are not programmed in LSC PCAP when bonds are present, affecting backend traffic
- AV-103185: Service Engine may fail when Application Cookie persistence is configured
- AV-103394: Unable to upgrade SE groups from the Avi UI via the System Update page since the required images are not displayed
- AV-103495: During IP reputation DB sync cycle, if upgrade is invoked, sync will be partially completed. After upgrade, IP reputation DB sync continues to fail with the error, *File Already Exists*.
- AV-104179: Upgrade may fail in the OpenStack environment due to error in pre-upgrade checks
- AV-104475: API call to `/gslb-inventory` does not provide information in results list, when `X-Avi-Version: 17.2.12` is used in the headers while making the call.
- AV-104692: UI: Valid IPv6 range is not allowed in the static IP pool configuration of a network
- AV-104932: When configuring IPAM profile for Infoblox, the usable network list is not displayed
- AV-105132: Infoblox credentials are logged in plain-text in Controller internal logs

Key Changes in 20.1.4

- AV-102637: The default application profile `System-Secure-HTTP-VDI` has `connection_multiplexing_enabled` set to *FALSE*
- AV-101985: Prior to Avi Vantage version 20.1.4, Avi waited for the default timeouts LDAP (120 seconds) and TACACS (10 seconds) before trying the next server. Starting with Avi Vantage 20.1.4, if an LDAP/TACACS server does not accept connections on the given port, Avi tries to connect to the next server. The timeout for authentication from an LDAP server is modified to be 20 seconds. Currently, multiple LDAP servers are not supported for authentication on Avi Controller.
- AV-102604: Prior to Avi Vantage version 20.1.4, history of the security logs showed fixes done in the last two years. Starting with Avi Vantage version 20.1.4, the security logs display the last security fix done, regardless of the time limit
- AV-103642: Sorting by Health Score is disabled on sets with more than 200 objects

- AV-101985: For Controller authentication, multiple LDAP servers are supported only if they belong to the same cluster. Otherwise, the Controller tries to authenticate with the first reachable server.
- AV-102252: Support for Inter-SE Distributed Object Store: Service Engines can now perform the distribution and synchronization of information without the involvement of the Controller in VMware, LSC and NSX-T clouds (with default port being 9001). Ensure that TCP traffic on the selected port between Service Engine management interfaces is allowed via appropriate firewall rule.
- The minimum value for X-Avi-Version that can be used when interacting with the Avi Controller is 18.2.6. It is recommended to update the automation assets, as required.

Known Issues in 20.1.4

- AV-104715: The service engine does not detect the link status changes of vmxnet3 NICs in vCenter.
- AV-106907: LDAP authentication does not work if `ignore_referrals` is set to *True* in LDAP settings.
- AV-115513: LSC:
    - Upgrade/Patch may not work if the Controller is running as a container on a host running RHEL 8.x.
    - Podman version higher than 1.6.4 is not supported.
- AV-142641: Macro API for virtual service deletion does not support API migration below X-Avi-Version 20.1.1.

## Checklist for Upgrade to Avi Vantage Version 20.1.4 Refer to this section before initiating upgrade.

- Upgrading to Avi Vantage version 20.1.4 is supported from any of the following versions:
    - Avi Vantage version 17.2.x
    - 18.2.1 through 18.2.11
    - Avi Vantage version 20.1.x

  Note: Upgrade from 18.2.12 and higher to 20.1.4 is not supported.
  For more information refer to:
    - Upgrade from Avi Vantage release 18.2.6 or higher
    - Upgrade from a version prior to Avi Vantage release 18.2.6
- Starting with Avi Vantage release 20.1.1 as per the HTTP/2 RFC, the cipher suites with TLS 1.2 listed here are not supported. Remove the ciphers before initiating upgrade to Avi Vantage version 20.1.1.

Starting with Avi Vantage version 20.1.1, the default disk size for new SEs is now 15 GB.
For OpenStack deployments, ensure that the disk size for the requisite flavors is increased to a minimum of 15 GB * Starting with Avi Vantage version 20.1.1, the Avi Controller and Service Engines use Python 3. Refer to the migration notes in the following sections:

```
* [For ControlScripts]({%vpath%}/architectural-overview/templates/scripts/#upgrade-to-python-30)

* [For Python-based External Health Monitors]({%vpath%}/external-health-monitor/#upgrade-to-python-30)
```

- Licensing Management of the Avi Service Engines has been updated. Refer to the Avi Vantage License Management article for more information.

- Avi Vantage now enforces system limits based on Controller cluster size. Refer to the System Limits article for more information.

- In case of Service Engine upgrade in a Nutanix Acropolis Hypervisor (AHV) environment, refer to the pre-upgrade changes.

- Support for Inter-SE Distributed Object Store: Service Engines can now perform the distribution and synchronization of information without the involvement of the Controller in AWS, Azure, GCP, OpenStack clouds (with default port being 4001). Ensure that TCP traffic on the selected port between Service Engine management interfaces is allowed via appropriate firewall rule.

- Starting with version 20.1, Avi Vantage has moved from Lua 5.1 to LuaJIT for compiling and running DataScripts. LuaJIT is relatively more restrictive with non-defined escape sequences. Using any escape sequence other than ones supported, (as defined in the Lua 5.1 Reference Manual) results in a compile error. Before upgrading to version 20.1 or higher, ensure the DataScripts do not use undefined escape sequences.
  If the DataScripts are not fixed before upgrade, the DataScripts using non-defined escape sequences, which worked earlier will now cause the virtual service to go down.

Issues Resolved in 20.1.3 Patch Releases

Issues Resolved in 20.1.3-2p11

- AV-135843: After applying the Controller patch, the indexer service fails.
- AV-133360: Remote_site_watcher process can get stuck if there is a GRPC connection failure during resync process.
- AV-128998: If the leader site is running versions 20.1.1 through 20.1.5 and the follower is running versions > 20.1.5, the Remote Site Watcher Sync can fail.
- AV-127046: WAF tab in the UI is empty for some virtual services.
- AV-126389: When RSS is enabled, packet buffers are not freed and eventually lead to connection failures due to a race condition during packet transmission on vNICs that have VLAN configured
- AV-125824: If a bond exists on the management interface NICs (>=10G), it can be broken while stopping / restarting / upgrading the Service Engines in LSC deployments
- AV-125377: External health monitor is unable to invoke ping since it requires raw socket access privileges.
- AV-124931: Auto-download of CRS fails when proxy is configured.
- AV-122836: When GSLB leader site is represented with cluster-VIP, the configuration replication between sites is not working.
- AV-119910: `vcenter_mgr` process may fail when the SE is deleted.

Issue Resolved in 20.1.3-2p10

- AV-114426: Undefined behavior when adding a policy match rule for cache-control or Pragma header which may result in a Service Engine failure

Issues Resolved in 20.1.3-2p9

- AV-114653: Service engine fails when attempting to reuse a connection to the LDAP server that has already been closed.
- AV-108983: Zombie processes keep accumulating in the Service Engine.

Issues Resolved in 20.1.3-2p8

- AV-113786: Azure: Echo server cannot handle multiple connections. This can cause SE to be falsely marked down from ALB
- AV-109476: The Linux du command is causing increase in memory consumption when the Service Engines failed to unmount.
- AV-106375: No events are seen after an event that has very large data
- AV-101871: The IP Reputation functionality might not work correctly if the virtual service is disabled and then immediately enabled.

Issues Resolved in 20.1.3-2p7

- AV-110784: When configuring the cloud or discovering objects, the cloud configuration was stuck displaying the status *vcenter resyncing in progress*.
- AV-109210: Configured remote address is not passed in TACACS authentication request.

Issues Resolved in 20.1.3-2p6

- AV-106363: If the SEs are running older versions and the Controller is running version 20.1.3, the VS logs may not be indexed if the log contains non utf-8 characters
- AV-106432: Data from the socket was not drained when RST and the data was processed/received at the same time on the SE. This results in partial data being delivered to the client from the server
- AV-108086: Exception while listing networks/domains in AWS IPAM/DNS Profile
- AV-108371: UI: Unable to export *All Logs* for VS due to the identified_ciphers error
- AV-109441: Unable to add a BGP peer in the network belonging to the admin?s global VRF when using per tenant VRF in vCenter
  Note: Per-tenant VRF in vCenter Cloud is not a recommended deployment.

Issues Resolved in 20.1.3-2p5

- AV-102525: PFX certificate upload from UI fails with an error
- AV-106057: If a pool is configured with a file larger than 16K to be sent as local response in case the pool is down, the response recieved by the client is partial
- AV-106363: If the SEs are running older versions and the Controller is running version 20.1.3, the VS logs may not be indexed if the log contains non utf-8 characters
- AV-106119: Unable to create PSM Learning Group from WAF policy modal
- AV-107313: SE may fail due to incorrect route label reference, when BGP is configured

Issues Resolved in 20.1.3-2p4

- AV-106362: Updating a DNS policy with site selection having a fall back site may result in SE failure.
- AV-106169: Port-channel initialisation might fail in service engine running on CSP
- AV-106147: Syslog messages are displayed incorrectly with an extra character (b)
- AV-105629: The UI does not show the placement networks from the global VRF when configuring a virtual service from within a tenant with per-tenant VRF in vCenter cloud.
- AV-104837: Health monitor response is not parsed correctly if the content length header is not present.

Issues Resolved in 20.1.3-2p3

- AV-105132: Infoblox credentials are logged in plain text
- AV-104932: The field Usable Networks is not displayed in the UI when configuring Infoblox IPAM due to API timeout fetching networks from Infoblox
- AV-104692: Unable to add a range of IPv6 addresses as a static pool via the Avi UI
- AV-104475: The API call to `/gslb-inventory` does not provide information in the results list when `X-Avi-Version:17.2.12` is used in the headers while making the call.
- AV-104179: Upgrade may fail in the OpenStack environment if the Avi Controller fails to read the OpenStack versions
- AV-103642: Sorting by Health Score is disabled on sets with more than 200 objects.
- AV-103495: During IP reputation DB sync cycle, if upgrade is invoked, sync will be partially completed. After upgrade, IP reputation DB sync continues to fail with the error, *File Already Exists*.

Issue Resolved in 20.1.3-2p2

- AV-102892: A virtual service using a VLAN interface goes into fault state with reason Failed to add VS to the interface if the parent interface's name changes during upgrade.

Issues Resolved in 20.1.3-2p1

- AV-102822: Granular RBAC configuration in basic VS config mode breaks logical workflow
- AV-102889: If the image tag is not prefixed with `avinetworks`, redundant checks lead to error due to tag mismatch in case of SAAS
- AV-102954: Real time analytics is not enabled for 30 minutes when a virtual service is created in the basic mode
- AV-103185: Service Engine may fail when Application Cookie persistence is configured
- AV-103394: Unable to upgrade SE groups from Administrator > Controller > System Update page as the required images are not displayed

What's New in 20.1.3

Release date: 22 December 2020
To refer to the upgrade checklist, click here.

ADC

- Auto detecting NTLM connections and disabling connection multiplexing for the specific connection
- Enhanced virtual hosting (EVH): To enable virtual hosting on virtual services irrespective of SNI
- Support for JWT validation as the client authorization method for secure communication through Avi
- Support for both HTTP v1 and HTTP/2 servers on an SSL enabled pool
- User profile mapping support for remote users

NSX-T Cloud Connector

- The capability for a single Avi Controller to manage multiple NSX-T clouds pointing to same or to different NSX-T Managers
- Automated NSGroup creation to allow securing of client traffic using DFW policies
- Proxy ARP support for VIP on Tier-0 and Tier-1 LRs
- Multiple vCenters per NSX-T cloud enable multi-site deployments

Analytics

- CLI/ API support to configure alerts using any Avi object in the Avi Controller
- Support for the new syslog mode: SYSLOG_RFC5425_ENHANCED

Avi Pulse

- Support for CORS allowlisting via CLI
- Integration with My VMware Portal

DataScripts

- API/CLI support to configure the `VSDataScriptSet` to use `IPReputationDB`
- Out of Band Request Processing via DataScripts

IPAM

- Support for VIP selector using labels/selectors to match a virtual service VIP with a particular set of IPAM networks
- Support for allocating different IPAM ranges for SEs and Virtual IPs

Linux Server Cloud

- Support for RHEL versions 8.1, 8.2, 8.3

Networking

- Support for DHCP on datapath interfaces in LSC in DPDK mode
- The number of VLAN interfaces allowed to be configured on a SE is increased from 224 to 1000 (applicable to VMware No Access clouds)
- Cisco CSP: Support for PF devices to be passed through to Service Engines
- Outbound NAT: Support for ICMP flows

Public Cloud

- GCP: RSS support in DPDK mode

Security

- UI support for OCSP Stapling
- DDoS detection and mitigation enhancements
- Support to select a ControlScript under Certificate Management

WAF

- Support for partial buffering for chunked-encoded payload
- Support to use string groups as match elements
- IPv6 address support for GeoIP transformation
- ICAP support for HTTP requests processing through Avi iWAF
- Support for configuring IP groups in WAF Allow lists
- Layer 7: Support for IP reputation for HTTP Policies

Key Changes in 20.1.3

Feature Behavior Changes

- The following data path heartbeat and IPC encap config fields are moved from `seproperties` to `segroup`:

- dp_hb_frequency
- dp_hb_timeout_count
- dp_aggressive_hb_frequency
- dp_aggressive_hb_timeout_count
- se_ip_encap_ipc

- se_l3_encap_ipc

However, these fields continue to exist in `seproperties` also. Setting these fields in `seproperties` will only affect SEs in SE groups running Avi Vantage version 20.1.2 or earlier. Likewise, SE group-based fields take effect only for the SEs in SE groups running Avi Vantage version 20.1.3 and later.

The upgrade from pre-20.1.3 `seproperties` based configuration to version 20.1.3 will automatically migrate the config to SE group as a part of the upgrade migration. * Adding a BGP peer to a VRF context is blocked if the BGP peer belongs to a network which has a different VRF Context. Additionally, if the user attempts to change an existing network's VRF, and there are BGP peers in that network's VRF which belong to this network, then the change will be blocked. * GCP: In DPDK mode, the default descriptor ring size is increased to 2048 for GCP virtIO * The default group `ServiceEngineGroup` object under the Default-Cloud will be reset automatically during a license tier switch to honor the Basic/Essentials license tier restrictions, if it violates the target tier's requirements when there are no virtual services under the SE group. * NSX-T Cloud Connector can be configured on a Avi Controller setup in the Basic edition license tier * Pool and Poolgroup names are not allowed to have '$' character in the Name field * Virtual service VIP objects created via the UI are now prefixed with *vsvip-*. The virtual service VIP object search is enhanced to include search by addr(IP address) along with the existing search by name. * Ciphers arcfour128 and arcfour256 are no longer supported. * Prior to Avi Vantage version 20.1.3, `.local` domains were resolvable using the configured DNS server. Starting with version 20.1.3, `.local` domains are not resolvable by default through the configured DNS server. Explicitly configure the search domain with `.local` sub-domain to allow resolutions for `.local` names. * The minimum value for X-Avi-Version that can be used when interacting with the Avi Controller is 18.2.6. It is recommended to update the automation assets, as required.

Ecosystem Changes

- Controller and Service Engine software updated to Ubuntu 20.04.1

Azure

- Support for Azure IPAM is removed. This was applicable for Kubernetes Cloud Connector, which was deprecated in Avi Vantage version 20.1.1. Click here to know more.

GCP

- Support for GCP IPAM on GCP is removed. This was applicable for Kubernetes Cloud Connector, which was deprecated in Avi Vantage version 20.1.1. Click here to know more.
- Support for Linux Server Cloud in GCP is removed. This has been deprecated in Avi Vantage version 20.1.1.

NSX-V Full Access

- Support for NSX-V full access is deprecated starting with Avi Vantage 20.1.3. NSX-V full access will be removed in the upcoming releases. It is recommended to:
  - Migrate to Avi's NSX-T integration
  - In case NSX-V support is still required, it is recommended to configure Avi with a no-orchestrator cloud.

Issues Resolved in 20.1.3

- AV-63931: If multiple LDAP servers are configured in the Auth profile and the first server times out, the request is closed out, instead of trying other servers configured
- AV-79236: Intermittent "400 bad request" errors displayed when the Avi SE and client/server pod are on the same OpenShift node
- AV-89906: The Avi Service Engine can fail when accessing an invalid connection entry during UDP fast path packet processing
- AV-93539: Geo-location entries are missing on the SE where the DNS virtual services for a site is placed after either of the following triggers:
- SNAT configuration on DNS virtual service
- Disable/ Enable of DNS virtual service
- AV-96887: Static routes on the dedicated management interface are lost when the SE restarts
- AV-97092: ARP cache entry is not cleared for deleted servers, which may cause the SE to send packets to old mac address.

- AV-97564: On upgrading to Avi Vantage version 20.1.1, the Avi Controller wrongly adds extra service cores for the *Trial* license. These extra service cores are removed when the Controller is upgraded to Avi Vantage version 20.1.2 or higher.
- AV-98336: The warning message 'Virtual Service Fault' is displayed when the `vsdatascriptset` command in a non-admin tenant, referring to `IPAddrgroup` or `Stringgroup` in admin tenant, is attached to the virtual service. This happens only when `IPAddrGroups` or `StringGroups` with the same name are configured on both the admin and non-admin tenant.
- AV-98344: In an AWS virtual service, the SE creation failed after the Controller was restarted
- AV-98495: Service Engine failure when the request is served from the cache, while the HTTP response policy or DataScript response header event is configured
- AV-98523: Upgrade fails and rolls back if files were uploaded as case attachments using Avi Pulse prior to the upgrade
- AV-98649: If an SE group has one or more virtual services disabled, and one or more virtual services that are disabled, both pointing to the same virtual service VIP, `auto_rebalance` does not work
- AV-98667: GCP cloud reconcile deletes routes for all virtual services, if a virtual service is disabled in the route-aggregation mode
- AV-98903: The warning message, "Service Time-out" is displayed when the WAF tab was clicked from the virtual service
- AV-98938: If upgrade fails and aborts, in certain cases, the rollback operation may not complete.
- AV-98998: The following virtual service properties are not allowed in the VMware NSX Advanced Load Balancer - Basic Edition and VMware NSX Advanced Load Balancer - Essentials Edition:
  - L4 Policies
  - Remove Listening Port when VS down
  - service_metadata
- AV-99052: App learning and PSM rules are not working. The Learning API returns the message `App not found`
- AV-99127: When an L4 policy rule is deleted, invalid references to the policy can cause the SE to fail
- AV-99172: While updating attributes of an existing SQS queue, a dictionary gets updated during iteration which leads to error in Python 3.0
- AV-100201: Intermittent SE failure on updating IP reputation database
- AV-100240: User creation fails in the VMware NSX Advanced Load Balancer enterprise edition and VMware NSX Advanced Load Balancer basic edition
- AV-100557: `manage.py` process fails and restarts continuously during upgrade from Avi Vantage version 18.2.x to version 20.1.1 while starting the `avicontrollermetrics` process
- AV-100699: Disabling the cloud configuration ip6_autocfg_enabled in the controller CLI removes the auto-configured address from the SE. However, this does not persist across reboots/upgrades.
- AV-100758: Upgrade from Avi Vantage version 18.2.8-2p2 to version 20.1.1-2p4 fails at migrate config
- AV-100892: When VIP is used as SNAT for a virtualservice in a legacy active standby SE group, after a primary switchover, health monitor stops working
- AV-102137: Under low memory conditions, memory allocation failures can cause a failure in the HTTP-to-HTTPS redirect scenarios
- AV-102205: Editing WAF policy in tenant mode triggers the error message, "WAFPolicy object not found!".

Known Issues in 20.1.3

- AV-102057: NSX-T: During VS Scale-in and Scale-out some of the long-standing connections could be dropped.
- AV-102600: If a virtual service which holds a subset of the SEs in a Shared virtual service set is deleted, the capacity of the SEs on which the virtual service was not present is reduced. Those SEs will hold lesser number of virtual service due to an internal accounting error. Do not delete a virtual service if it is Sharing a VIP with other virtual services and the shared virtual service set is asymmetrically Scale-Out.
  First resolve the asymmetric scale-out of the shared virtual services by scaling-out/scaling-in the virtual service and ensure that the shared virtual services are symmetric. Then, delete the desired virtual service.

- AV-102522: When FIPS mode is enabled, the Service Engine may fail if HTTP Security Policy with per_ip + per_uri_path rate limiting rules are configured for a virtual service. Do not use HTTP Security Policy with per_ip + per_uri_path rate limiting rules in FIPS mode
- AV-103185: Service Engine may fail when Application Cookie persistence is configured.
- AV-115513: LSC:
  - Upgrade/Patch may not work if the Controller is running as a container on a host running RHEL 8.x.
  - Podman version higher than 1.6.4 is not supported.
- AV-142641: Macro API for virtual service deletion does not support API migration below X-Avi-Version 20.1.1

## Checklist for Upgrade to Avi Vantage Version 20.1.3 Refer to this section before initiating upgrade.

- Upgrading to Avi Vantage version 20.1.3 is supported from any of the following versions:
  - Avi Vantage version 17.2.x
  - 18.2.1 through 18.2.11
  - Avi Vantage version 20.1.x

  Note: Upgrade from 18.2.12 and higher to 20.1.3 is not supported.
  For more information refer to:
  - Upgrade from Avi Vantage release 18.2.6 or higher
  - Upgrade from a version prior to Avi Vantage release 18.2.6

- Starting with Avi Vantage release 20.1.1 as per the HTTP/2 RFC, the cipher suites with TLS 1.2 listed here are not supported. Remove the ciphers before initiating upgrade to Avi Vantage version 20.1.1.

- Starting with Avi Vantage version 20.1.3, Avi Pulse has been integrated with the My VMware Portal. After upgrading to 20.1.3, it is recommended to re-register the Avi Controllers to Avi Pulse using My VMware credentials. For step-by-step instructions, refer to the Migrating to MyVMware SSO section the Getting Started with Pulse article.

Starting with Avi Vantage version 20.1.1, the default disk size for new SEs is now 15 GB.
For OpenStack deployments, ensure that the disk size for the requisite flavors is increased to a minimum of 15 GB * Starting with Avi Vantage version 20.1.1, the Avi Controller and Service Engines use Python 3. Refer to the migration notes in the following sections:

```
* [For ControlScripts]({%vpath%}/architectural-overview/templates/scripts/#upgrade-to-python-30)

* [For Python-based External Health Monitors]({%vpath%}/external-health-monitor/#upgrade-to-python-30)
```

- Licensing Management of the Avi Service Engines has been updated. Refer to the Avi Vantage License Management article for more information.

- Avi Vantage now enforces system limits based on Controller cluster size. Refer to the System Limits article for more information.

- In case of Service Engine upgrade in a Nutanix Acropolis Hypervisor (AHV) environment, refer to the pre-upgrade changes.

- Starting with version 20.1, Avi Vantage has moved from Lua 5.1 to LuaJIT for compiling and running DataScripts. LuaJIT is relatively more restrictive with non-defined escape sequences. Using any escape sequence other than ones supported, (as defined in the Lua 5.1 Reference Manual) results in a compile error. Before upgrading to version 20.1 or higher, ensure the DataScripts do not use undefined escape sequences.
  If the DataScripts are not fixed before upgrade, the DataScripts using non-defined escape sequences, which worked earlier will now cause the virtual service to go down.

- Explicitly configure the search domain with `.local` sub-domain to allow resolutions for `.local` names.

Issues Resolved in 20.1.2 Patch Releases

Issue Resolved in 20.1.2-3p1

- AV-98230: Support the use of SRIOV PFs in passthrough mode on CSP

Issues Resolved in 20.1.2-2p10

- AV-118134: When a virtual service is configured with `use_vip_as_snat` or effectively using VIP IP as SNAT, consecutive migrations to the same SE may render the virtual service with that VIP inoperative.
- AV-116398: While removing the application domain name from shared virtual service, a random entry from the list is deleted.

Issue Resolved in 20.1.2-2p9

- AV-116157: Traffic logs are not displayed in the Avi UI. On the Controller, no matching log files are synced from the SE. Delayed response to log queries due to timeout on the Controller.

Issue Resolved in 20.1.2-2p7

- AV-104019: Import of certificates failed if the key is of type EC and is encrypted using des or aes256

Issues Resolved in 20.1.2-2p6

- AV-103495: During IP reputation DB sync cycle, if upgrade is invoked, sync will be partially completed. After upgrade, IP reputation DB sync continues to fail with the error, *File Already Exists*.
- AV-99256: Due to slow network, sometimes IP reputation DB sync fails with the *Timeout* error

Issues Resolved in 20.1.2-2p5

- AV-91487: Some DFW rules are not getting created in NSX-V
- AV-98121: Custom DNS does not work.
- AV-98938: If upgrade fails and aborts, in certain cases, the rollback operation may not complete
- AV-98649: Auto rebalance does not work if an SE group has one or more disabled virtual services and one or more enabled virtual services which point to the same virtual service VIP.
- AV-102621: Unable to untar the uploaded tech support from the Controller.

Issues Resolved in 20.1.2-2p4

- AV-98495: Service Engine failure when the request is served from the cache, while the HTTP response policy or DataScript response header event is configured
- AV-98903: The warning message, "Service Time-out" is displayed when the WAF tab was clicked from the virtual service
- AV-100883: The default SE Group object is not handled internally during license tier switch

Issues Resolved in 20.1.2-2p3

- AV-100201: Intermittent SE failure on updating IP reputation database
- AV-100240: User creation fails in the the VMware NSX ALB enterprise edition and VMware NSX Advanced Load Balancer basic edition

Issues Resolved in 20.1.2-2p2

- AV-98523: Upgrade fails and rolls back if files were uploaded as case attachments using Avi Pulse prior to the upgrade
- AV-98854: False positives triggered support case creation. An Avi support case is created for every `SE_DOWN` event. An `SE_DOWN` event can happen during maintenance activities like an upgrade or scaleout
- AV-99052: App learning and PSM rules are not working. The Learning API returns the message `App not found`
- AV-99127: When an L4 policy rule is deleted, invalid references to it can cause the SE to fail

Key Changes in 20.1.2-2p2

- AV-98230: Support for using the SRIOV PFs in passthrough mode on CSP
- AV-99411: The NSX-T cloud type allowed in the Avi Basic license tier

Issues Resolved in 20.1.2-2p1

- AV-98344: In an AWS virtual service, the SE creation failed after the Controller was restarted by Google Kubernetes Engine (GKE)
- AV-98998: The following virtual service properties are not allowed in the VMware NSX Advanced Load Balancer - Basic Edition and VMware NSX Advanced Load Balance - Essentials Edition:
  - L4 Policies
  - Remove Listening Port when VS down
  - `service_metadata`
- AV-99172: While updating the attributes of an existing Amazon Simple Queue Service (SQS) queue, a dictionary gets updated during through its iteration, which leads to error in Python 3.0 and displays the error message `AWS_SQS_ACCESS_FAILURE`

What's New in 20.1.2

Release date: 13 October 2020
To refer to the upgrade checklist, click here.

ADC

- IPAM: Support for user preferred IP with auto allocation (via CLI)
- Granular role-based access control over individual objects via labels
- NSX-T: IPv6 support for NSX-T cloud
- NSX-T: SE group scoping at folder, host, and data store levels

Public Cloud

- GCP: Support for configuring GCP cloud in non-admin tenant
- GCP: Customer Managed Encryption Key (CMEK) support for encrypting Service Engine (SE) disks

Key Changes in 20.1.2

- The Name field is mandatory for DataScript rate limiters. However, the UI does not have the ability to configure the Name field. Use the CLI to configure the Name field for the DataScript rate limiters
- NSX-T: Prior to Avi Vantage release 20.1.2, an NSService for a pool would be created with the default server port, although the pool did not have any servers. In addition, the default server port would be present in the NSService even if no servers used the default server port (all were manually configured). Starting with Avi Vantage 20.1.2, the NSService for the pool will not have a default server port, if no servers are using the default server port.

- VMware: By default, new Controller VMs will have the hardware version set to 10
- NSX-T: A cloud object prefix must have only letters, numbers and underscore.
- The minimum value for X-Avi-Version that can be used when interacting with the Avi Controller is 18.2.6. It is recommended to update the automation assets, as required.

Issues Resolved in 20.1.2

- AV-63931:If multiple LDAP servers are configured in the Auth profile and the first server times out, the request is closed out, instead of trying other servers configured.
- AV-88370: Enabling traffic capture for a virtual service may result in high memory usage on the Controller due to `sshfs` process retaining memory
- AV-87657: NSX-T Cloud: The following have been changed from ID-based configuration to path-based configuration:
    - Cloud Configuration: `transport_zone`, `tier1_lr_id`, and `segment_id`
    - Pool Configuration: `nsx_securitygroup`, and `tier1_lr`
    - Virtual service VIP: `tier1_lr`
- AV-90603: Infoblox: The Usable Subnet field on the Avi UI may not get populated when large number of subnets are configured in Infoblox
- AV-91225: Authorization for TACACS-plus remote auth is unsuccessful stating, "User has no privileges?
- AV-91393: Creating a WAF profile on the Avi Controller version 20.1.1 is not possible on a client with API version prior to 20.1.1. Also, with a client using API version prior to 20.1.1, it is not possible to update and get the WAF profile data except the learning parameters in the WAF profile
- AV-91781: From the Avi UI, in the New Tenant Mapping screen, the drop-downs under User Role and User Tenants were not displayed, unless configured via CLI
- AV-92028: Unable to log in to the Avi Controller using SAML authentication
- AV-92299: Cluster VIP is not included in the ns-groups object for NSX-T
- AV-93632: Failure to import certificates with UTF-8 encoded characters
- AV-93714: In geo-DB files, consecutive creation or deletion operations cause inconsistencies like:
    - The geo-DB files do not get downloaded to the SE
    - The geo-DB files may not get replicated to the followers from the leader
- AV-93792: The rate limit configured for a virtual service using `connections_rate_limit` is not honored
- AV-93954: A Service Engine can fail when a virtual service has traffic consisting of file uploads, with large header files and when all the pool members are down
- AV-94032: If more than 500 AWS autoscale groups (ASG) are configured as pools, frequent updates to the ASGs can cause the pool updates to fail with the error, ?Timedout in executing CloudConnectorService.cc_lookup_nw request_pb?
- AV-94045: Upgrade from Avi Vantage versions 18.2.6 - 18.2.10 to version 18.2.10+ via the application UI is not available
- AV-94608: Unable to create a full access cloud of type GCP via the Avi Controller UI when a proxy is configured on the Avi Controller
- AV-94788: Controller memory usage can increase and cause controller processes to fail due to in-sufficient memory
- AV-94818: Syslog messages from the Avi Controller do not reach the destined syslog server
- AV-96827: Virtual service reports 503 Gateway error when server closes the connection before all the data is sent to client.
- AV-97790: On upgrading to Avi Vantage version 20.1.1, the Avi Controller wrongly adds extra service cores for the *Trial* license. These extra service cores are removed when the Controller is upgraded to Avi Vantage version 20.1.2 or higher.

Known Issues in 20.1.2

- AV-102600: If a virtual service which holds a subset of the SEs in a Shared virtual service set is deleted, the capacity of the SEs on which the virtual service was not present is reduced. Those SEs will hold lesser number of virtual service

due to an internal accounting error. Do not delete a virtual service if it is Sharing a VIP with other virtual services and the shared virtual service set is asymmetrically Scale-Out.
First resolve the asymmetric scale-out of the shared virtual services by scaling-out/scaling-in the virtual service and ensure that the shared virtual services are symmetric. Then, delete the desired virtual service.
- AV-102522: When FIPS mode is enabled, the Service Engine may fail if HTTP Security Policy with per_ip + per_uri_path rate limiting rules are configured for a virtual service. Do not use HTTP Security Policy with per_ip + per_uri_path rate limiting rules in FIPS mode.
- AV-142641: Macro API for virtual service deletion does not support API migration below X-Avi-Version 20.1.1.

## Checklist for Upgrade to Avi Vantage Version 20.1.2 Refer to this section before initiating upgrade.

- Upgrading to Avi Vantage version 20.1.2 is supported from any of the following versions:
  - Avi Vantage version 17.2.x
  - 18.2.1 through 18.2.10

  Note: Upgrade from 18.2.11 and higher to 20.1.2 is not supported.
  For more information refer to:
  - Upgrade from Avi Vantage release 18.2.6 or higher
  - Upgrade from a version prior to Avi Vantage release 18.2.6

- Starting with Avi Vantage release 20.1.1 as per the HTTP/2 RFC, the cipher suites with TLS 1.2 listed here are not supported. Remove the ciphers before initiating upgrade to Avi Vantage version 20.1.1.

- The default disk size for new SEs is now 15 GB.
  For OpenStack deployments, ensure that the disk size for the requisite flavors is increased to a minimum of 15 GB

- Starting with Avi Vantage release 20.1.1, the Avi Controller and Service Engines use Python 3. Refer to the migration notes in the following sections:

  - For ControlScripts

  - For Python-based External Health Monitors

- Licensing Management of the Avi Service Engines has been updated. Refer to the Avi Vantage License Management article for more information.

- Avi Vantage now enforces system limits based on Controller cluster size. Refer to the System Limits article for more information.

- In case of Service Engine upgrade in a Nutanix Acropolis Hypervisor (AHV) environment, refer to the pre-upgrade changes.

- Starting with version 20.1, Avi Vantage has moved from Lua 5.1 to LuaJIT for compiling and running DataScripts. LuaJIT is relatively more restrictive with non-defined escape sequences. Using any escape sequence other than ones supported, (as defined in the Lua 5.1 Reference Manual) results in a compile error. Before upgrading to version 20.1 or higher, ensure the DataScripts do not use undefined escape sequences.
  If the DataScripts are not fixed before upgrade, the DataScripts using non-defined escape sequences, which worked earlier will now cause the virtual service to go down.

Issues Resolved in 20.1.1 Patch Releases

Issue Resolved in 20.1.1-2p10

- AV-98217: Unable to create service engines when the vCenter 7.0 and vSAN datastore combination is used in NSX-T

Issues Resolved in 20.1.1-2p9

- AV-104179: Upgrade may fail in the OpenStack environment if the Avi Controller fails to read the OpenStack versions
- AV-103495: During IP reputation DB sync cycle, if upgrade is invoked, sync will be partially completed. After upgrade, IP reputation DB sync continues to fail with the error, *File Already Exists*.
- AV-102621: The techsupport file uploaded through Avi Pulse is getting corrupted.
- AV-99256: Due to slow network, sometimes IP reputation DB sync fails with the *Timeout* error

Issues Resolved in 20.1.1-2p8

- AV-98938: If upgrade fails and aborts, in certain cases, the rollback operation may not complete
- AV-102137: In low memory conditions, memory allocation failures can cause service engine failure in the HTTP-to-HTTPS redirect scenarios
- AV-102318: Config Migration step in Upgrade fails due to exception in `metrics_db` migration

Issue Resolved in 20.1.1-2p7

- AV-97092: ARP cache entry is not cleared for deleted servers, which may cause the SE to send packets to old mac address

Issues Resolved in 20.1.1-2p6

- AV-100758: Upgrade from Avi Vantage version 18.2.8-2p2 to Avi Vantage version 20.1.1-2p4 failed at migrate config
- AV-100557: `manage.py` process fails and restarts continuously during upgrade to Avi Vantage version 20.1.1 from Avi Vantage version 18.2.x while starting the `avicontrollermetrics` process

Issues Resolved in 20.1.1-2p5

- AV-98523: Upgrade fails and rolls back if files were uploaded as case attachments using Avi Pulse prior to the upgrade
- AV-98854: False positives triggered support case creation. An Avi support case is created for every `SE_DOWN` event. An `SE_DOWN` event can happen during maintenance activities like an upgrade or scaleout

Issues Resolved in 20.1.1-2p3

- AV-92575: A valid Avi user with write access to the Avi DataScript role may be able to gain read/write access to the Controller file system
- AV-93265: A valid Avi user with write access to the Avi DataScript role will be able to execute system commands via the Lua system functions
- AV-93269: Allowing special characters in the protocol parser object filename can lead to security issues
- AV-93303: Allowing special characters in the DataScript filename can lead to security issues
- AV-94608: GCP full access cloud does not work if proxy is configured on the Avi controller
- AV-93632: Import failure of certificates containing data encoded with UTF-8 with characters outside the ASCII set
- AV-94723: GCP full access cloud creation through the Avi Controller web interface does not work if proxy is configured on the Avi Controller
- AV-94788: Controller memory usage can increase and cause controller processes to fail due to insufficient memory
- AV-94818: Syslog messages from the Avi Controller do not reach the destined syslog server

Issues Resolved in 20.1.1-2p2

- AV-91225: User attributes are not set properly. Hence, the user is not being assigned the required privileges. The authorization for TACACS-plus remote auth is unsuccessful stating, "No Privileges".

- AV-91393: Creating a WAF profile on the Avi Controller version 20.1.1 is not possible when a client with API version prior t0 20.1.1 is used. Also, with a client of API version prior to Avi Vantage version 20.1.1, it is not possible to update and get the WAF profile data except the learning parameters in the WAF profile.
- AV-91781: Tenant and role mapping are not working when used from UI
- AV-92028: Unable to log in to the Avi Controller when using SAML authentication
- AV-92400: In GCP environment, the Service Engine upgrade can stop if the UUID ends with the letter 'q'

Issue Resolved in 20.1.1-2p1

- If the Controller is currently in Avi Vantage version 18.2.6 or 18.2.7, with a controller patch, the upgrade to Avi Vantage version 20.1.1 fails.

What's New in 20.1.1

To refer to the upgrade checklist, click here.

ADC

- Write access support for NSX-T
- Support for enabling NTLM and basic authentication in HTTP(S) health monitors
- Rate limiter enhancements for layer-4 and layer-7 virtual services
- Support for HTTP/2 on the server side

Automation

- Java-based plugin for vRealize Orchestrator (vRO)
- APIs: Provide list of available Avi Controller events

Avi Pulse

- Case creation and tech-support addition via Pulse
- IP Reputation case management via Pulse
- Core Ruleset download via Pulse

DataScript

- L7: Ability to retrieve geolocation information for a given IPv4/IPv6 address
- Support for DataScripts to be executed on L4-SSL Response Event

DNS and IPAM

- Support for mail exchanger (MX) records (static records)
- Support for text (TXT) records (static records)
- Infoblox: Support IPv6 subnet allocation

Flexible Upgrades

- UI for Flexible Upgrades
- Ability to apply patches across different patch trains

GSLB

- Support for IPv6 hosts as GSLB pool members
- Support for customized replication policies across GSLB sites

Logging

- Support for VMware Log Insights for Avi Controller events

Networking

- BGP: Support for BGP Learning and advertisement
- BGP: Support for AS-Path prepend and local preference attributes
- BGP: Ability to learn default route from VIP NW router
- BGP: Graceful restart
- Support for wildcard VIP and routing with auto-gateway

Public/ Private Cloud

- AWS: DPDK support for Service Engines
- AWS: Support for C2S Cloud
- Microsoft Azure: Support for server-side disk encryption for Service Engines
- GCP: Full-access, automated support for Avi Service Engine deployment and configuration
    - Autoscale group support
- OpenStack:
    - Support for OpenStack Train
    - Support for Contrail version 19.12
- VMware: Support for VMware vSphere 7.0

Security

- Support for IP Reputation Database
- Authorization policies for SAML authentication to provide granular control
- OCSP Stapling
- WAF: Enhanced allow-lists for WAF traffic
- WAF: Adaptive configuration of WAF learning
- WAF: Support for Core Rule Set (CRS) downloads
- Ability to import DAST scanner results from the following scanners via virtual patching
    - OWASP ZAP Attack Proxy
    - Qualys Web App Scanning

System

- Enforcement of system limits based on Controller size
- Separation of virtual service and the virtual service VIP
- Support for plain-text SMTP relay
- SNMPv3: SHA256 support
- Configuration: Support for pre-defined passphrase for configuration import/export
- Licensing: Support for VMware DLF based license
- Licensing: Support to limit performance and Service Core license consumption of Service Engines
- FIPS 140-2 support for Avi Service Engines
- Support for DRS and vMotion High Availability for Avi Controllers and Service Engines

Feature Behaviour Changes

- Avi Vantage has upgraded to Python 3.0. Python 3.0 is incompatible with the 2.x line of releases.
- The default disk size for new SEs is now 15 GB
- A virtual service with SNAT enabled for L2 or L3 (BGP) in LSC can now also have IP routing enabled

- On a GSLB interaction with Active follower sites, config messages are not prioritized over health status messages
- Pool metrics are no longer supported on virtual service entities. They are supported only on Pool entities.
- Terraform Integration: The environment variable `AVI_SUPPRESS_SENSITIVE_FIELDS_DIFF` is introduced to enable Terraform suppress the difference for sensitive fields during the plan update
- WAF: Learning parameters have been moved from WAF profile to WAF policy object
- WAF: The default version of the WAF CRS changed to CRS-2020-1
- The SAML assertion and response signing are mandatory for successful SAML authentication
- HTTP/2 can now be enabled under virtual service and pool/ pool group configuration. The option Enable HTTP2 is no longer available in the Application Profile configuration.
- The *via* header is removed from the config.restricted_headers field in a WAF profile after upgrade. To retain the old behavior, add "via" into the `config.retricted_headers` field in the WAF policy again after upgrading to version 20.1.2.
- The minimum value for X-Avi-Version that can be used when interacting with the Avi Controller is 18.2.6. It is recommended to update the automation assets, as required.

Licensing

The highlights of licensing in Avi Vantage release 20.1.1 are as below:

- Socket Licenses (for Linux Server Cloud Service Engines) are not supported. On upgrade, existing Service Engines will be migrated to equivalent Service Core licenses.
- The One GB bandwidth license is not supported. On upgrade, existing Service Engines will be migrated to unlimited bandwidth, and require four Service Core licenses.
- Future-dated subscription licenses cannot be issued anymore. All subscription serial keys are valid from the time of issue

For detailed information, refer to the Avi Vantage License Management article.

Ecosystem Changes

OpenStack

Starting with Avi Vantage release 20.1.1, the The following features/ integrations are removed:

- Port-Security as the plugin for standard ML2 and Contrail
- Hypervisor Type option from OpenStack cloud (Default will be only KVM)
- Support for Nuage as the SDN
- Support for ACI as the SDN
- Support for Horizon dashboard
- LBaaSv2 as the deployment mode

Google Cloud

- Support for GCP IPAM (Linux Server Cloud mode of deployment in Google Cloud) is deprecated. We recommend customers to use the GCP Full Access Deployment.

Container Clouds

- Support for OpenShift and Kubernetes cloud mode of deployment is removed. We recommend customers to use Avi Kubernetes Operator (AKO).

Issues Resolved in 20.1.1

- AV-72536: Unauthenticated requests create sessions on the database

- AV-73155: OpenStack: Scale in does not happen for SE during migration
- AV-74434: DNS resolution not working from one of the egress pods because of wrong route entry for source IP egress pod DNS resolution not working from one of the egress pods because of wrong route entry for src ip egress pod
- AV-76098: UI: Non federated persistence profiles are shown for GSLB services
- AV-78741: Content-Type cannot be removed or replaced through the HTTP response policy
- AV-79264: Application profile with client cert validation fails to write headers in other tenants
- AV-79346: Avi-Venafi integration: Certificate is not being renewed in the right tenant
- AV-79847: The health score under the Health tab is marked as NA
- AV-79912: When specifying a port range, the DataScript function avi.vs.port reports the first port in the range specified
- AV-80050: `avi.http.add_header()`, `avi.http.remove_header()`, `avi.http.replace_header()` allow an extra integer argument not shown in existing documentation
- AV-80115: Unable to clean up stale tenants using */api/openstack-cleanup* when the `use_admin_url` config is set to *False* in OpenStack cloud configuration.
- AV-80196: SE failure when passing `avi.HTTP_RESPONSE` as the second argument to the `avi.http.get_cookie()` when it is used in the Request header script.
- AV-80594: Service Engine installed in Nutanix-AHV for versions prior to 20190916.96 fails during initialization
- AV-81373: AWS: Extra VIPs on SE data NICs that belong to a disabled virtual service are not moving to a parking NIC during reconcile
- AV-81374: GSLB Health Monitor fails due to incorrect namespace
- AV-81456: Service Engine issues if a chunked transfer encoding cache entry is hit when `enable_chunk_merge` is configured as *false* with response buffer mode on
- AV-81836: Users with PERMISSION_TRAFFIC_CAPTURE can do 'packet capture' of virtual service but cannot view the captured files
- AV-81908: Some of the GSLB pool members? FQDNs are not resolvable (as they are in a DR site). When DNS refresh interval is set to 5 minutes, this will create excessive CRUD on the system resulting in leader site not being able to send health status probes to the follower sites
- AV-81953: BGP peering is not established on using a VLAN interface that is in a different VRF than the parent interface. External health monitors that use that VLAN interface also do not work
- AV-82284: External AWS DNS profile with AWS cloud does not work if cloud is using cross account-based authentication
- AV-82432: Virtual service is unreachable when placed on Service Engines running in PCAP mode and with BGP Layer 3 scale-out configured
- AV-82459: metrics-mgr process fails repeatedly if an IP Group covering the range 128.0.0.0 to 255.255.255.255, or a subset, is configured on the Controller
- AV-82753: LSC: Virtual service traffic failure when inband management is disabled and DPDK mode is disabled
- AV-82965: WAF admin unable to edit WAF Policy from the UI
- AV-83138: When upgrading with *action_on_error* is *ROLLBACK_UPGRADE_OPS_ON_ERROR*, the SE fails to upgrade and goes to *UPGRADE_FSM_ERROR* state
- AV-83223: Under severe memory pressure, cache processing can fail while parsing response from backend server
- AV-83301: When an interface or its corresponding IP is removed the associated gateway monitor is not disabled. This will cause the gateway monitor to report a GW_DOWN to the Controller
- AV-83367: Controller users logged in via LDAP authentication may be logged out intermittently
- AV-83620: While serving objects from the cache, if the client abruptly closes the connection (or stream in case of HTTP2), the object being served from cache might hold onto the connection resulting in connection memory usage. Many such instances could lead to high connection memory usage
- AV-83643: Service Engine fails when connection multiplexing is disabled, pool group is configured, and pool member goes down between requests on the same connection
- AV-83804: Possible Controller configuration loss due to multiple Controller node failover events involving the same leader node

- AV-83807: GCP: Default-cloud cannot be set as GCP full access cloud via UI
- AV-83835: OpenStack: Cannot create/deploy virtual services, if Keystone v2 endpoint is used for integration and admin endpoints of nova, neutron, and glance services are not reachable or if Keystone v3 endpoint is used for integration and public endpoints of nova, neutron, and glance services are not reachable
- AV-83912: Every time image check was invoked, it generated an image uploaded event
- AV-83953: Connection reset in TCP fast path after idle timeout may send the reset with incorrect sequence number
- AV-84035: Postgres database on the follower node does not fully sync with the leader node causing it to leave the cluster and restart the full sync again
- AV-84092: Traffic to GSLB FQDN does not work when GSLB is enabled for OpenShift routes
- AV-84103: While deleting GSLB pool members, the wrong member is getting deleted from the UI
- AV-84247: SE fails when passing the`avi.HTTP_RESPONSE` as the second argument to the DataScript function `avi.http.cookie_exists()` when the said function is used in the request header script.
- AV-84284: L4 DataScript stalls with TCP request event. The virtual service having a TCP request DataScript event rejects requests after 57,000 connections. This is specific to TCP request events only
- AV-84287: OpenStack: SE failure when 25 vNICs are added
- AV-84396: For a virtual service with `traffic_enabled` set to *False* and the option use VIP as SNAT enabled, the SE responds to ARP for the VIP which negates the effect of `traffic_enabled` being set to *False*
- AV-84400: The Avi Controller fails to find the right VIP port to place VIP address on it
- AV-84432: On configuring `use_vip_as_snat` as *False* and snat_ip the same as VIP manually, the SNAT/IP configuration will be ignored
- AV-84678: Virtual services down due to SSL certificate PEM encoding read error when length of line in certificate is a multiple of 254
- AV-84679: Service Engine can fail while deleting a virtual service after it has been in fault state
- AV-85207: Clients proxying through Avi virtual service of Layer 4 SSL application type might experience intermittent TCP connection errors
- AV-85218: Same vLAN / vNIC IPs allowed in other SEs, VIP, Floating Interface IPs and sNAT IP
- AV-85647: Memory leak when creating HTTP policy configuration fails
- AV-85680: Service Engine processes may hold up freed memory that may cause memory being unavailable for other system process leading to Service Engine fail
- AV-85800: Service Engine can fail when requests with cookies with no spaces in between or large cookies use the avi.http.remove_cookie or avi.http.replace_cookie API
- AV-86092: TCP DNS queries over IPv6 network incorrectly load balanced
- AV-86518: Service Engine becomes unresponsive when time is set backwards on the SE by a large range of hours
- AV-86782: SE initialization fails if the data path interfaces are not released back to Linux successfully when SE is restarted
- AV-86871: Upgrade from Avi Vantage version 17.2.x to 18.2.x or higher can result in the metrics manager using a lot of memory after upgrade (more than 50,000 backend servers. This can happen at a lower scale if the pools are shared across many virtual services.
- AV-86953: IPv6 GeoDB may contain duplicate entries depending on the order of the DB entry creation
- AV-86955: DNS policy using client IP match / Geo location match behavior is not behaving as expected, impacting the DNS policies Match client location (use_edns_client_subnet_ip enabled), Match client location (use_edns_client_subnet_ip not enabled), Match client IP (use_edns_client_subnet_ip enabled)
- AV-87502: Service Engine failure when Auth Profile is disabled while still processing HTTP traffic is sent on old connections
- AV-87505: Service Engine failure due to a double close of LDAP connection
- AV-88094: Service Engine on Azure could fail if the NIC's link flaps
- AV-88267: Requests sent to virtual services with incorrect DataScripts in the LB Done event sends a 200 OK response instead of responding with a server error
- AV-88692: Service Engine can fail due to incorrect rate limiter configuration in a network security policy
- AV-88795: SE Group or SE upgrade initiated when the Controller is upgraded at the system level in case of software or patch update

- AV-89227: Requests resulting in a SAML authentication loop
- AV-89246: Python exception in `pci_unbind.py` during SE initialization
- AV-89946: HTTP Policy port match always matches to the first port in port range instead of the service port the request arrived on

Known Issues in 20.1.1

- AV-90364: NSX-T: When a Virtual Service is placed in a different Service Engine Group, duplicate static route entries with same network but with different next hop can cause traffic failure.
- AV-90949: NSX-T: After changing the NSX-T Manager password provided to the Avi Controller,the NSX-T account may get locked temporarily due to excessive login attempts by the Avi Controller with the old password.
- AV-91264: WAF: Configuring WAf profile containing `learning_params` through API versions prior to 20.1 is not supported and can cause the Avi Controller to enter bad state. Warm reboot to fix this bad state.
- AV-94788: Processes that are consuming memory beyond their threshold are not automatically restarted. This can cause the Controller processes to fail due to insufficient memory. Manually restart the Controller processes with high memory usage.
- AV-97790: On upgrading to Avi Vantage version 20.1.1, the Avi Controller wrongly adds extra service cores for the *Trial* license. These extra service cores are removed when the Controller is upgraded to Avi Vantage version 20.1.2 or higher.
- AV-101464: A version incompatibility is causing Thales Luna HSM (formerly SafeNet Luna HSM) and AWS CloudHSMv2 interoperability to fail for Avi versions 20.1.1 and onwards.
- AV-142641: Macro API for virtual service deletion does not support API migration below X-Avi-Version 20.1.1.

Checklist for Upgrade to Avi Vantage Version 20.1.1

Refer to this section before initiating upgrade to Avi Vantage release 20.1.1:

- Upgrading to Avi Vantage version 20.1.1 is supported from any of the following versions:

  - Avi Vantage version 17.2.x

  - Avi Vantage versions 18.2.1 through 18.2.9

  Note: Upgrade from 18.2.10 and higher to 20.1.1 is not supported.
  For more information refer to:
  - Upgrade from Avi Vantage release 18.2.6 or higher
  - Upgrade from a version prior to Avi Vantage release 18.2.6

- Starting with Avi Vantage release 20.1.1 as per the HTTP/2 RFC, the cipher suites with TLS 1.2 listed here are not supported. Remove the ciphers before initiating upgrade to Avi Vantage version 20.1.1.

- The default disk size for new SEs is now 15 GB.
  For OpenStack deployments, ensure that the disk size for the requisite flavors is increased to a minimum of 15 GB

- Starting with Avi Vantage release 20.1.1, the Avi Controller and Service Engines use Python 3. Refer to the migration notes in the following sections:

  - For ControlScripts

  - For Python-based External Health Monitors

- Licensing Management of the Avi Service Engines has been updated. Refer to the Avi Vantage License Management article for more information.

- Avi Vantage now enforces system limits based on Controller cluster size. Refer to the System Limits article for more information.
- In case of Service Engine upgrade in a Nutanix Acropolis Hypervisor (AHV) environment, refer to the pre-upgrade changes.
- Starting with version 20.1, Avi Vantage has moved from Lua 5.1 to LuaJIT for compiling and running DataScripts.
  - LuaJIT is relatively more restrictive with non-defined escape sequences. Using any escape sequence other than ones supported, (as defined in the Lua 5.1 Reference Manual) results in a compile error. Before upgrading to version 20.1 or higher, ensure the DataScripts do not use undefined escape sequences. The escape sequences supported are:
    - Literal strings can be delimited by matching single or double quotes, and can contain the following C-like escape sequences: '' (bell), '' (backspace), '' (form feed), '' (newline), '' (carriage return), '' (horizontal tab), '' (vertical tab), '\\' (backslash), '"' (quotation mark [double quote]), and ''' (apostrophe [single quote]).
    - A character in a string can also be specified by its numerical value using the escape sequence , where ddd is a sequence of up to three decimal digits. (Note that if a numerical escape is to be followed by a digit, it must be expressed using exactly three digits.)
Before upgrading to version 20.1 or higher, ensure the DataScripts do not use undefined escape sequences.
If the DataScripts are not fixed before upgrade, the DataScripts using non-defined escape sequences, which worked earlier will now cause the virtual service to go down.
  - Uninitialized variables are not scoped to only the current request and could carry over values between requests causing unintended behavior.

Supported Platforms

Refer to System Requirements: Ecosystem

Product Documentation

For more information, please see the following documents, also available within this Knowledge Base.

Installation Guides

- Avi Vantage Installation Guides

Copyrights and Open Source Package Information

For copyright information and packages used, refer to https://aviopensource.s3.amazonaws.com/20.1/open_source_licenses.pdf.

Avi Networks software, Copyright ? 2015-2021 by Avi Networks, Inc. All rights reserved. The copyrights to certain works contained in this software are owned by other third parties and used and distributed under license. Certain components of this software are licensed under the GNU General Public License (GPL) version 2.0 or the GNU Lesser General Public License (LGPL) Version 2.1. A copy of each such license is available at http://www.opensource.org/licenses/gpl-2.0.php and http://www.opensource.org/licenses/lgpl-2.1.php

Additional Reading

Protocol Ports Used by Avi Vantage for Management Communication