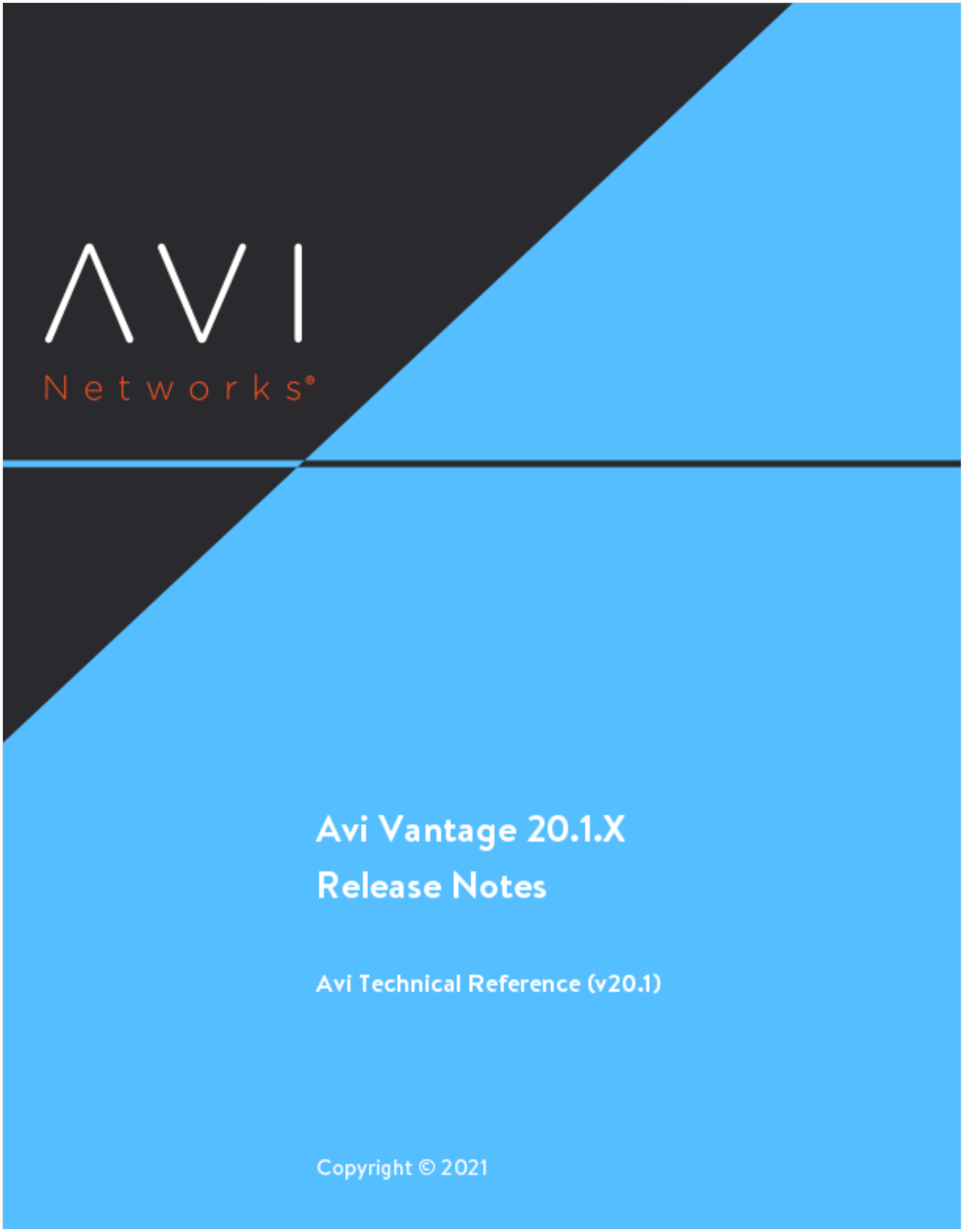


# Avi Vantage 20.1.X
# Release Notes

## Avi Technical Reference (v20.1)

# Avi Vantage 20.1.X Release Notes

view online

## Issues Resolved in 20.1.4 Patch Releases

### 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: Error while sending out email for alerts

## 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

### 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 ## Known Issues in 20.1.4

- AV-104715: The service engine does not detect the link status changes of vmxnet3 NICs in vCenter

## 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 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.

# Issues Resolved in 20.1.3 Patch Releases

## 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

## 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: IPv6 addresses are assigned even though the field ip6_autocfg_enabled is not enabled
- 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 crash 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.

## 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 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.

# 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

## 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 crash 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.

## 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

## 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

- 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.

## Issues Resolved in 20.1.1 Patch Releases

### 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: Symptoms: 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

## Key Changes in 20.1.1

### 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.

### 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.
  Workaround: None

## 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
- 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.

## 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.

## Additional Reading

Protocol Ports Used by Avi Vantage for Management Communication