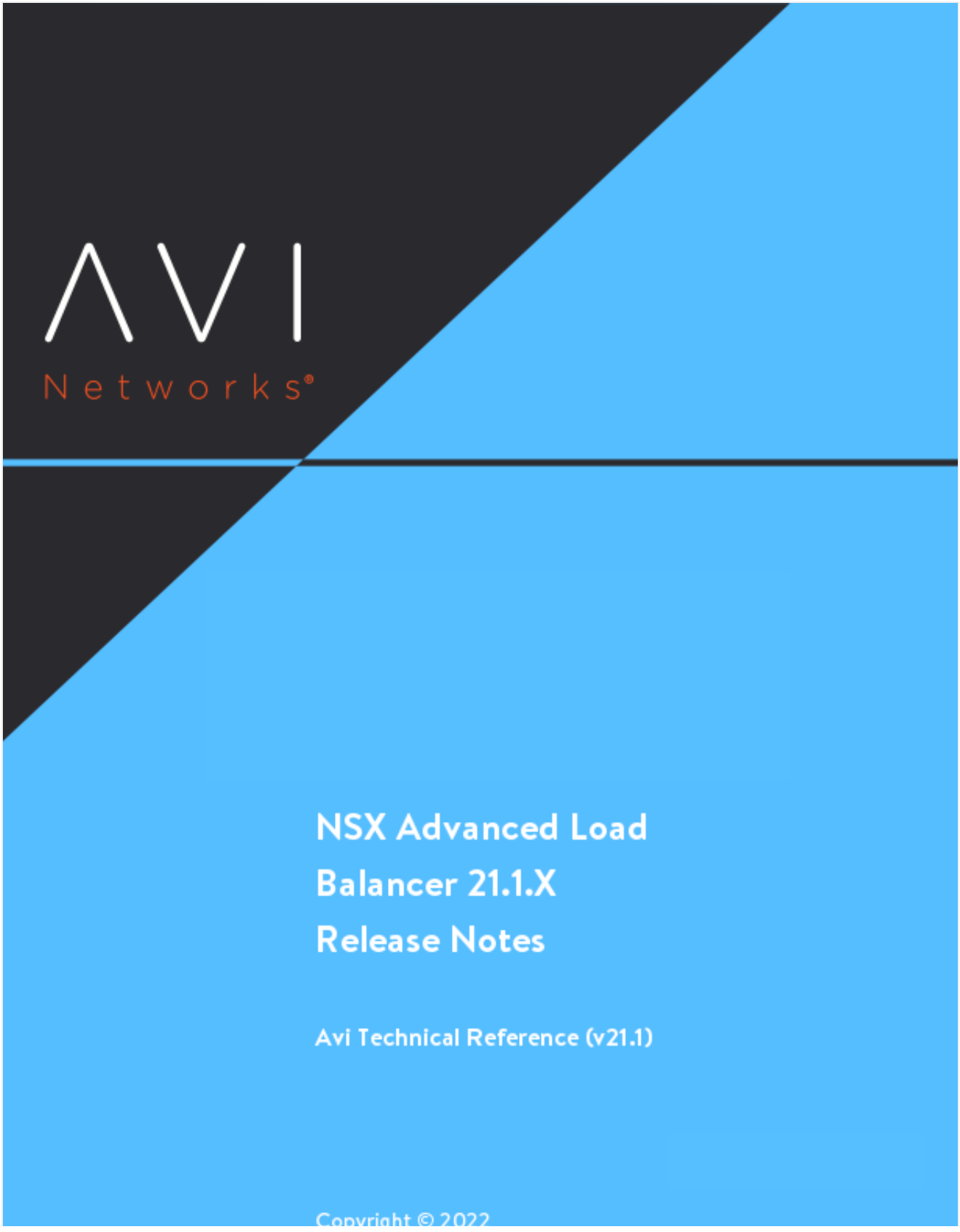

NSX Advanced Load Balancer 21.1.X Release Notes

Avi Technical Reference (v21.1)

NSX Advanced Load Balancer 21.1.X Release Notes

view online

Issues Resolved in 21.1.4 Patch Releases

What's New in 21.1.4-2p4

Release Date: 16 June 2022
* AV-145542: Experimental limited ENS backend support for full access deployments (Tech preview) ### Issues Resolved in 21.1.4-2p4 * AV-146188: Deleting an FQDN from a VSVIP deletes all the FQDNs of a VIP on AWS * AV-145696: Route53 DNS records are not deleted when the VSVIP is deleted from the Controller * AV-144971: Updating large `IpAddrGroups` can fail with a Service Timeout * AV-144544: API timeouts on OpenStack environment when VSVIP objects are created or deleted in bulk * AV-140287: When sending RST packets, longstanding flows during upgrade leads to longer timeouts. * AV-137080: BFD echo mode does not work with NSX Advanced Load Balancer * AV-136469: Fixes error when adding a GSLB pool member for a site with a parent/child VSThe error VirtualService object not found! is displayed when adding a GSLB pool member for a site with a parent or child virtual services

Issues Resolved in 21.1.4-2p3

Release Date: 27 May 2022
* 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-143198: Service Engine may fail if the L7 virtual service listening service is configured with L4 app profile using `override_application_profile` and is followed by the virtual service's network profile update * AV-144235: Packet capture is not working on a virtual service when dedicated dispatcher is enabled on the SE * AV-144468: Upgrade failure in `WaitUntilClusterReadyLocally` task due to timeout on waiting for the `image_manager` queue * AV-144621: vCenter cloud discovery might fail with inventory state "VCENTER_INVENTORY_RETRIEVING_DC" in vCenter cloud version 7.0 an higher * AV-144790: Do not throttle the logs in SE when client log settings are set to unlimited * AV-145264: `HealthMonitorChecks` panicked while creating DNS type `healthmonitor` without `dns_monitor` * AV-145541: Service Engine failure when client resets the connection on an HTTP /2 request

Issues Resolved in 21.1.4-2p2

Release Date: 12 May April 2022
* AV-144262: Unable to create/update `IpAddrGroups`, when any group UUID is present in `ApiAccess`/`SshAccess` in system configuration * AV-143988: Macro API containing GSLB objects errors out * AV-143897: Added support for kernel version 4.18.0-305.34.2.el8_4.x86_64 * AV-143099: SSL certificate generation using control scripts for flows trying to connect to external SSL certificate authority(for example, Let's Encrypt, Venafi, Sectigo) may fail

What's New in 21.1.4-2p1

Release Date: 05 May April 2022
* Support for real-time Prometheus API

Issue Resolved in 21.1.4-2p1

- AV-143825: Real-time metrics API response is missing data for some virtual services in random fashion.

What's New in 21.1.4

Release Date: 07 April 2022
To refer to the upgrade checklist, click here.

Cloud Connector

- AWS: Support for the region `ap-east-1`
- AWS: New flavors introduced to support AWS regions
- NSX-T: Preserve Client IP Support for NSX-T Overlay
- OpenStack: Reduction in the number of API calls to OpenStack Neutron and Nova

Core LB Features

- Generic Routing Encapsulation (GRE) tunnel support for DSR Type L3 (Layer 3)
- Support for BGP peer label-based virtual service placement
- Layer 7: Support for HTTP/2 WebSocket

DNS/IPAM

- Infoblox IPAM: Multi-AZ support for AWS

Issues Resolved in 21.1.4

- AV-129536: vCenter cloud may fail with vCenter 7.0 and higher
- AV-130533: In a VMware cloud deployment with ESX version 7.x, Layer 2 DSR (Direct Server Return), TCP and, HTTP health monitor may fail due to incorrect checksum handling
- AV-131382: OpenStack floating IP subnet is not visible in the VSVIP configuration for an OpenStack cloud
- AV-132841: For HTTP2 connections sending a 307 redirect or local response for client requests, without making an upstream connection can result in a memory leak
- AV-132945: BGP peer configuration with # in the MD5 password might cause configuration failure
- AV-133050: Re-uploading the image may fail if cloud-generated SE files are present only in the leader node but not in the follower nodes
- AV-133110: In the cloud services portal, the used service units for a Controller may be updated with a maximum delay of one hour
- AV-133272: SE fails if a PKI profile having an expired certificate is updated
- AV-133276: SE creation may fail on vCenter cloud
- AV-133339: Azure: After upgrade to NSX Advanced Load Balancer version 21.1.3, virtual services are down due to SE health probe failures

- AV-133349: SSL Profile (UI): The cipher list in NSX Advanced Load Balancer version 21.1.3 displays a limited set of ciphers and erroneously hides the remaining, common ciphers
- AV-133902: When attaching a `.dat` file to the content switch policy, the virtual service fails with the error Out of memory
- AV-135875: Application profile creation is unsuccessful in the license tier ENTERPRISE_WITH_CLOUD_SERVICES
- AV-135894: Connection mirroring fails in multi-core SEs
- AV-136068: Service Engine fails due to a missing check in the memory allocation routine which gets triggered when Service Engine memory consumption goes high
- AV-136203: Upgrade to NSX Advanced Load Balancer version 21.1.3 may fail, if the current version has alerts configured with `se_enable event_id` as trigger/action
- AV-136539: Spinning SEs from Azure Market place does not work. All the offers have been invalidated.
- AV-136694: When importing an EC SSL certificate, and adding a passphrase, the EC encrypted private key is not exported as a string
- AV-136945: Increase in memory consumption in SE DPDK mode leads to SE start-up failure when `extra_shm_cfg_memory_mb` is configured
- AV-137461: If the SE management network is DHCP enabled, but there is an IP address pool configured in this network to use for VIP IPAM (with type static_ips_for_vip), SE creation fails with the error Service Engine management network xxxx configured for static, but no IP addresses available for use
- AV-137544: Custom IPAM assigns VIP only from the first subnet when configured via UI, and excludes the other subnets
- AV-137515: Due to a race condition in the Service Engine bring up sequence, incorrect interface mapping occurs for the HSM interface configured in the CSP environment
- AV-137713: GSLB Pool Member Resolved IP dropdown is not displayed after upgrading to 21.1.3
- AV-138269: Virtual services sharing the same Virtual IP, but asymmetrically placed across the Service Engines of the Service Engine Group (some can be on one single Service Engine) stop working after the Service Engine Group is upgraded
- AV-138278: Under SE group configuration, changes made in Data Store Scope in Service Engine Virtual Machine do not persist after clicking Save, specifically when Shared is selected at first and then changed to Any or Local
- AV-138439: In an over provisioned system, Service Engine failure can occur when 'se_delayed_flow_delete' is set to *True*
- AV-138352: Multiple updates to the enhanced virtual service parent could result in failure when traffic is sent to its child virtual service
- AV-13857: Multiple certificates cannot be linked to EVH parent virtual services in the Basic tier
- AV-138428: When the Service Engine is processing configuration updates, a virtual service can transition into a fault state (due to memory pressure). Disabling or enabling the virtual service may lead to a Service Engine failure

- AV-138717: ControlScripts executed in a Controller in the Docker environment only supports 'overlay2' and 'devicemapper' storage drivers
- AV-138792: Service Engine might fail with the combination of Error page configuration on failed requests and clients sending pipelined HTTP posts on the same frontend TCP connection
- AV-139248: In vCenter clouds, the Controller can add two vNICs on the SE, in the same VRF/network
- AV-139276: When configured via UI, Infoblox IPAM assigns VIP only from the first subnet, excluding the other subnets
- AV-141095: Request timeout on a Virtual Service when the DataScript line `avi.http.response(200)` is called in the response event
- AV-141620: If the Resource Manager process is unable to connect to the Redis instance at port 5001, the process hangs instead of shutting down and restarting
- AV-140442: HTTP policy content switch fails for IPv6 servers

Key Changes in 21.1.4

- Prior to NSX Advanced Load Balancer version 20.1.3, .local domains were resolvable implicitly using the configured DNS server.
  Starting with NSX Advanced Load Balancer version 20.1.3, .local domains are not resolvable by default through the configured DNS server (local domains are not routed to DNS servers). The search domains need to be configured explicitly for ?.local? domains to make lookups work within this DNS domain.
- When certificate sharing is enabled, the Intermediate CA certificate with highest expiry in the current tenant is always selected. If there is no Intermediate CA certificate in the current tenant, then the corresponding Intermediate CA is selected from the admin tenant (if any)
- Search of usable networks in IPAM is now case insensitive
- EVH Parent virtual services in Basic tier can now refer to multiple SSL certificates
- ControlScripts that make API calls back to the Controller API using `localhost` must be updated to use the `DOCKER_GATEWAY` environment variable instead.

You can now apply any VMware NSX Advanced Load Balancer serial key license to the Avi Controllers.

Known Issues in 21.1.4

- AV-141493: When the Controller of version 21.1.3 or higher is configured with the ENTERPRISE_WITH_CLOUD_SERVICES tier, rolling back the Service Engines to a version lower than 21.1.3, results in failure of the corresponding SE.
  Workaround: Change the license tier to ENTERPRISE before rolling back the Service Engines.
- AV-140545: Virtual service goes into Fault state when user-configured object names exceed 256 characters.
  Workaround:
  1. Edit the object name to reduce the number of characters.
  2. Disable and enable the virtual service.
- AV-142641: Macro API for virtual service deletion does not support API migration below X-Avi-Version 20.1.1.

Checklist for Upgrade to NSX Advanced Load Balancer Version 21.1.4

Refer to this section before initiating upgrade.

- Upgrade to NSX Advanced Load Balancer is only supported from the following versions:
    - Version 18.2.6 through 18.2.13
    - Version 20.1.1 through 20.1.8
    - Version 21.1.1 through 21.1.3
- Ensure the object names are limited to a maximum of 256 characters
- As a part of Ubuntu 20.04 migration, all search domains which need DNS resolution are explicitly specific. This is a deviation from DNS resolver (prior to ubuntu 20.04), where any and all DNS requests were sent to the DNS server. Update the search domain using the CLI if there are not more than one entities.
- NSX Advanced Load Balancer 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 NSX Advanced Load Balancer version 21.1.1, it is recommended to upgrade to a current vCenter version. For more information, refer to the System Requirements article.
- To transition the NSX Advanced Load Balancer Controller to the SaaS edition refer to Getting Started with NSX Advanced Load Balancer Cloud Services.
    - Upgrade Avi Controller cluster to Avi version 21.1.3 (or later)
    - Disable Cloud Services (Pulse) if enabled,
    - Change License Tier from ENTERPRISE to ENTERPRISE_WITH_CLOUD_SERVICES
    - Register with VMware NSX Advanced Load Balancer Cloud Services (Pulse)
- Linux Server Cloud: OEL 6.9 reached the end of support in March 2021. Starting with NSX Advanced Load Balancer version 21.1.3, support for OEL 6.9 will be removed. If you are running OEL 6.9, upgrade to a supported Linux distribution before upgrading to NSX Advanced Load Balancer 21.1.3 or higher.
- vCenter Read Access cloud is deprecated in NSX Advanced Load Balancer 21.1.3 and support for vCenter Read Access will be removed in a future release of NSX Advanced Load Balancer. If you are using vCenter Read Access environment, it is recommended to migrate to vCenter Write Access or vCenter No Access.
- In case of Service Engine upgrade in a Nutanix Acropolis Hypervisor (AHV) environment, refer to the pre-upgrade changes.

Issues Resolved in 21.1.3 Patch Releases

Issues Resolved in 21.1.3-2p10

Release Date: 13 July 2022
* AV-148423: Unable to create that VIP object from the UI in Azure Cloud * AV-147679: Placement network section is not displayed in the NSX-T VIP modal * AV-145954: Clients might still receive OCSP staple status as GOOD even though the certificate has expired * AV-141620: If Resource Manager process is unable to connect to Redis port 5001, it will hang instead of being properly shutdown and restarted * AV-139528: Symptoms: The search filter function for adding usable networks in IPAM profile and for selecting VIP/server placement networks will not work

Issues Resolved in 21.1.3-2p9

Release Date: 22 June 2022
* AV-146188: Deleting an FQDN from a VSVIP deletes all the FQDNs of a VIP on AWS * AV-145696: Route53 DNS records are not deleted when the VSVIP is deleted from the Controller * AV-141435: Shell login fails when the number of `TIMED_WAITING` connections increase on the shell server * AV-140287: When sending RST packets, long-standing flows during upgrade leads to longer timeouts

Key Change in 21.1.3-2p8

Release Date: 02 June 2022
* The capability to enable X-Accel headers to be passed the client is introduced using the flag `pass_through_x_accel_headers`.

Issues Resolved in 21.1.3-2p8

- AV-146000: When sending RST packets, long standing flows beyond 30 seconds during upgrade does not work on multi-core systems
- AV-136469: The error VirtualService object not found! is displayed when adding a GSLB pool member for a site with a parent or child virtual services

Issues Resolved in 21.1.3-2p7

Release Date: 25 May 2022
* AV-138131: `Service Status Updated Object: error:?Access Denied?` on all threat intelligence features (IP Reputation and AppSignature) led to repeated accumulation of large objects in logs as a consequence of repeated upstream sync updates from the portal, eventually causing the Controller to run out of disk space. * AV-144468: Upgrade failure in `WaitUntilClusterReadyLocally` task due to timeout on waiting for `image_manager` queue. * AV-135894: Controllers registered with Avi Pulse, with Application Rules enabled may run out of disk space.

Issue Resolved in 21.1.3-2p6

Release Date: 18 May 2022
* AV-138352: Multiple updates to enhanced virtual service parent could result in a crash when traffic is sent to its child virtual service. * AV-141800: JobManager makes many invalid API queries

Issues Resolved in 21.1.3-2p5

Release Date: 17 May 2022
* AV-140273: Long standing flows are not RST during upgrade leading to longer timeouts * AV-140768: Support for DLF v2 and v3 * AV-142116: When incoming fragmented IPv4 packets (carrying TCP payload) post-reassembly get redirected to SE Linux interface in DPDK mode of operation exhibit issue with IP checksum * AV-142620: VIP retains the old IP address when changing the IP address * 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-142680: Changes to handle remote LDAP user with username only in lowercase

What's New in 21.1.3-2p4

Release Date: 05 April 2022
* Support for vCenter 8.0

Issues Resolved in 21.1.3-2p4

- AV-140505: Virtual service fails after upgrading, if the value of Rules per HTTP Policy (`num_rules_per_http_policy`) exceeds 128
- AV-140442: HTTP policy content switch not fails for IPv6 servers

Issues Resolved in 21.1.3-2p3

Release Date: 20 March 2022
* AV-140366: Mitigation for CVE-2022-0778 * AV-139276: Infoblox IPAM assigns VIP only from the first subnet when configured via UI, it does not consider the other subnets * AV-138357: Multiple certificates cannot be linked to EVH parent virtual services in Basic tier * AV-137713: Dropdown to select resolved IPs is not rendered due to JavaScript Console error * AV-137544: Custom IPAM assigns VIP only from the first subnet when configured via UI, it does not consider the other subnets * AV-135875: User is unable to create an Application Profile due to a side effect from a new licensing tier that was added * AV-135843: After applying the Controller patch, the indexer service fails * AV-133276: SE creation attempt may fail on vCenter cloud * AV-131382: Adds network selection for floating IP subnet in OpenStack cloud virtual service VIP configuration

Issues Resolved in 21.1.3-2p2

Release Date: 09 March 2022

`21.1.3-2p2` is a renumber build for 21.1.3. All features available in 21.1.3 and 21.1.3-2p1 continue to be available, along with the fixes for the issues mentioned here.

Note: We recommend customers who have deployed 21.1.3 with Service Engines in a Linux Service Cloud environment to upgrade to 21.1.3-2p2 since the fix for AV-136945 is available in this build.

While 21.1.3-2p2 follows the patch numbering convention, it is a regular software maintenance build.
To install 21.1.3-2p2 as a new deployment, refer the installation guide for your environment.
To upgrade to 21.1.3-2p2, refer the Upgrade checklist for 21.1.3.

* AV-138428: When SE is processing configuration updates and the virtual service is put into fault state due to the SE being under memory pressure, disable/enable of the virtual service may lead to SE failure. * AV-137515: Incorrect interface mapping with HSM interface configured in CSP environment causes failure in SE upgrade * AV-137080: BFD echo mode does not work with NSX Advanced Load Balancer * AV-136945: Increase in memory consumption in SE DPDK mode leading to SE start-up failure when `extra_shm_cfg_memory_mb` is configured. * AV-136284: `show virtualservice authstats` did not return any output even when an LDAP Auth Profile was attached to the virtual service. * AV-136203: Upgrade to NSX Advanced Load Balancer version 21.1.3 may fail, if the current version has alerts configured with with `se_enable event_id` as trigger/action. * AV-136068: Service Engine failure due to insufficient memory. * AV-135843: After applying the Controller patch, the indexer service fails. * AV-134095: GCP pub/sub topic gets created on cloud reconfiguration even with no autoscaling groups present in Avi pools. * AV-133360: Remote_site_watcher process can get stuck if there is a GRPC connection failure during resync process. * AV-133272: SE fails if a PKI profile having an expired certificate is updated * AV-132841: For HTTP2 connections, sending a 307 redirect or local response for client requests without making an upstream connection can result in a memory leak. * AV-132736: Private keys uploaded as part of Certificate are explicitly moved to avoid disclosure with any GET APIs. * AV-130533: In a VMware cloud deployment with ESX version 7.x, Layer 2 DSR (Direct Server Return), TCP and, HTTP health monitor may fail due to incorrect checksum handling. * AV-126501: If jwt_config is not present in virtual service, it might lead to a config fault state.

Issues Resolved in 21.1.3-2p1

Release Date: 14 January 2022 * AV-131681: If the follower site is being upgraded without putting leader site in maintenance mode, config sync to remote site can fail. * AV-133050: Re-uploading the image may fail if cloud generated SE files are present only in the leader node but not on the follower nodes. * AV-133339: Azure: After upgrade to 21.1.3, Virtual services are down due to ALB-SE health probe failures. * AV-133902: When attaching a .dat extension file to content switch policy, the virtual service goes to failure state with *Out of memory* error.

Known Issue in 21.1.3-2p1

- AV-133349: SSL Profile UI: The Cipher list in NSX Advanced Load Balancer version 21.1.3 displays a limited set of ciphers, and erroneously hides additional, common ciphers. Workaround: Do not modify / update an existing SSL profile post upgrade, via the GUI. Use CLI to modify the Ciphers if required.

What's New in 21.1.3

Release Date: 21 December 2021
To refer to the upgrade checklist, click here.

Application Security

- Detection of DNS NXDOMAIN DDoS Attack
- Support for custom bot classification
- Support for ICAP with HTTP 2.0
- Support for NSX Advanced Load Balancer to act as Client and Resource Server for Open Authentication(OAuth)/ OpenID Connect 1.0 (OIDC)

Avi Cloud Services

- Introducing VMware NSX Advanced Load Balancer with Cloud Services - available through a new License Tier called *Enterprise with Cloud Services.*
  Note: Avi Pulse has been rebranded as *VMware NSX Advanced Load Balancer (Avi) Cloud Services*
- Central Licensing will enable zero-touch capacity management and cloud bursting for globally distributed NSX Advanced Load Balancer deployments

Cloud Connector

- NSX-T: Preserve Client IP Support for NSX-T Overlay

  Note: This feature is currently under tech preview.

Core LB Features

- When vSphere High Availability is enabled, if the Controller detects that a vSphere host failure has occurred, SEs will transition to OPER_PARTITIONED or OPER_DOWN prior to missing six consecutive heartbeat misses.
- Support for True Client IP in Layer 7 security features.
- Enhancements in Content Rewrite Profile.

- Support to configure cookie timeout in GSLB site persistence cookies .
- Support to configure cookie timeout in HTTP persistence cookies.
- Support for LDAP Health monitor.
- Support to monitor the health of the FTP servers configured as pool members using HEALTH_MONITOR_FTP.
- Support to configure DNS resolution on SE.
- Support for active/standby topology at AZ level.
- Support to removes the existing cookie attributes in HTTP response using the DataScript avi.http.remove_cookie_attribute.
- Support to get pool IP and port through DataScript in a response event.
- Support schedule-based scale-out and scale-in of ASG Servers.
- UI support for JSON Web Tokens validation.
- 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.

DNS/ IPAM

- Support to Process DNS Request both on SE and Backend Server in case of partial records.

GSLB

- Support to Adaptive Replication Mode in Replication Policy.

Horizon VDI

- Support for VDI WAF profile.
- Easy configuration and better analytics for UAG load balancing

  Note: This feature is currently under tech preview.

Networking

- Support for DPDK mode on Azure Service Engines.
- Virtual service failover upon BGP Peer failures via BGP peer monitoring.
- Support to show the state of BGP peers' across all the VRFs configured in the SE.

Observability and Monitoring

Application Metrics

- Support to configure custom Controller utilization alert thresholds using CLI.

System

- Controller interface and route management.
- Support for SE Hybrid RSS mode to achieve higher performance on low core SE.
- Support to compare and verify pre/post upgrade operational state.
- Support for multiple queues per dispatcher in SE DPDK mode.

WAF

- Support to mask URI query parameters in Application logs.
- Support for string groups in WAF Allowlist.
- Support for configurable request body processors.
- Support for recommendations to help ascertain and remediate false positives.

Issues Resolved in 21.1.3

- 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-118805: VMXNET3 interface receive stalls due to packet buffer depletion.
- AV-121113: When GeoDB is added with a custom file object having IP Address Mapped to different GEO Attributes in non-ascending order, then rules using country code mapped IP Group in different policies will fail to add the IP Address in GeoDB custom file object into the IP group-generated country code files
- AV-122704: Controller cluster VIP may not be accessible after reboot on Contrail with OpenStack.
- AV-124867: Unable to mask query parameters in application logs
- AV-125094: Scanner Application Profile rate limiter with *Report Only* action was not captured in significant logs.
- 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-126754: Cluster VIP configuration fails in GCP cloud when the Controllers have Public IPs assigned to them.
- 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-127802: Infoblox: When one of the virtual service VIPs is removed, the host record gets removed from the provider, even though there is still one virtual service VIP with that FQDN.
- AV-128044: When streaming request logs over Syslog format, the virtual service name is not included in the streamed logs.

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

- AV-128339: If the GSLB site was configured with an FQDN instead of an IP address, the GSLB service page failed to render properly, and the URL to the member site was not generated correctly.
- AV-128707: The SE Agent process may leak an opened file descriptor and consume too much disk space.
- AV-128745: When a GSLB leader site is represented as an FQDN instead of the IP address, the GSLB configuration replication from leader to follower site does not work.
- 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-128928: Server-initiated renegotiation fails for both Pools and HTTPS Health Monitor.
- AV-129063: The GeoDB object and the file objects are not recreated after upgrading to NSX Advanced Load Balancer Enterprise edition.
- AV-129080: NSX Advanced Load Balancer does not sign the SAML authentication requests despite SSL Key and certificate being attached to the SAML virtual service.

Key Changes in 21.1.3

- Avi Cloud Services
  Starting with NSX Advanced Load Balancer 21.1.3, the default license tier on a new Avi Controller deployment will change from ENTERPRISE to ENTERPRISE_WITH_CLOUD_SERVICES.
  To change this, from the NSX Advanced Load Balancer UI, navigate to Administration > Settings > Licensing.

- Installing VMware Serial Key Licenses
- To use VMware Serial Key licenses purchased before December 23, 2021, on a new Avi Controller deployment running version 21.1.3 or later:
    1. Upgrade your VMware Serial Key licenses from the customer connect portal. For more information, refer How to Upgrade License Keys.
    2. Apply the upgraded license keys on the newly deployed Avi Controller.
       Notes:
        - If you run into any issues with applying licenses, reach out to your VMware sales representative and we will provide a license that can be applied on the Avi Controller and fulfil your request.
        - There is no action required on the Avi Controller deployments that are upgraded.
    - To use VMware Serial Key licenses purchased after December 23, 2021, on an existing Avi Controller deployment running version 21.1.2 or earlier:
    1. Downgrade your VMware Serial Key licenses from the customer connect portal. For more information, refer How to Downgrade License Keys.
    2. Apply the downgraded license keys on the newly deployed the Avi Controller.

Installing VMware Serial Key Licenses
To use VMware Serial Key licenses purchased before December 23, 2021, on a new Avi Controller deployment running version 21.1.3 or later: 1. Upgrade your VMware Serial Key licenses from the customer connect portal. For more information, refer How to Upgrade License Keys. 2. Apply the upgraded license keys on the newly deployed Avi Controller.

If you run into any issues applying licenses, reach out to your VMware sales representative and we will provide a license that can be applied on the Avi Controller and fulfil your request.
Note: There is no action required on the Avi Controller deployments that are upgraded.

- FQDNs need to be configured for successful registration of NSX Advanced Load Balancer Controllers with Cloud Services.
- DNS configuration in `systemconfiguration`takes effect even in container-based deployments (Podman/ Docker).
- The Avi server side now allows SSL renegotiation request from the backend server.
- The user-agent check in Bot management allows user-agent strings with an uneven number of single quotes. For instance, Mozilla/5.0 (compatible; Let's Encrypt validation server; +https://www.letsencrypt.org).
- If a user-defined bot mapping is specified in a bot detection policy, the system bot mapping reference can be left empty.
- RBAC: Roles can only be created in admin tenant only.
- On Controller container deployment, the default DNS config from the host is inherited. This can be overridden by user configuration using system configuration.
- If the `admin_auth_profile` is set to LDAP, after upgrading to version 21.1.3 all remote users which are not in lowercase will be removed from the system along with their auth tokens. Going forward, all LDAP users will be created in lowercase instead of being case sensitive.

Ecosystem Changes

- Linux Server Cloud: OEL 6.9 reached end of support in March 2021. Starting with NSX Advanced Load Balancer version 21.1.3, OEL 6.9 is no longer supported. If you are running OEL 6.9, upgrade to a supported Linux distribution before upgrading to NSX Advanced Load Balancer 21.1.3.
- vCenter Read Access cloud is deprecated in NSX Advanced Load Balancer 21.1.3 and support for vCenter Read Access will be removed in a future release of NSX Advanced Load Balancer. If you are using vCenter Read Access environment, it is recommended to migrate to vCenter Write Access or vCenter No Access.

Known Issues in 21.1.3

- The license tier ENTERPRISE_WITH_CLOUD_SERVICES is incompatible with older versions of SEs: If the Controller is on version 21.1.3 or higher and the Service Engines are on versions lower than 21.1.3, this causes Service Engine failure. As a consequence, the virtual services placed on the respective service engines will be down.
  Note: Do not configure ENTERPRISE_WITH_CLOUD_SERVICES if the Service Engines are running versions lower than 21.1.3.
- SSL Profile UI: The Cipher List in NSX Advanced Load Balancer 21.1.3 displays a limited set of ciphers, and erroneously hides the additional, common ciphers.
  Workaround: Do not modify/update an existing SSL profile post upgrade, through the GUI. Use CLI to modify the Ciphers, if required.

- Increase in memory consumption in SE DPDK mode leading to SE start-up failure.
- Macro API for virtual service deletion does not support API migration below X-Avi-Version 20.1.1.

Checklist for Upgrade to NSX Advanced Load Balancer Version 21.1.3

Refer to this section before initiating upgrade.

- Upgrade to NSX Advanced Load Balancer is only supported from the following versions:
    - Version 18.2.6 through 18.2.13
    - Version 20.1.1 through 20.1.7
    - Version 21.1.1 and 21.1.2
- NSX Advanced Load Balancer 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 NSX Advanced Load Balancer version 21.1.1, it is recommended to upgrade to a current vCenter version. For more information, refer to the System Requirements article.
- To transition the NSX Advanced Load Balancer Controller to the SaaS edition refer to Getting Started with NSX Advanced Load Balancer Cloud Services.
    - Upgrade Avi Controller cluster to Avi version 21.1.3 (or later)
    - Disable Cloud Services (Pulse) if enabled,
    - Change License Tier from ENTERPRISE to ENTERPRISE_WITH_CLOUD_SERVICES
    - Register with VMware NSX Advanced Load Balancer Cloud Services (Pulse)
- Linux Server Cloud: OEL 6.9 reached end of support in March 2021. Starting with NSX Advanced Load Balancer version 21.1.3, support for OEL 6.9 will be removed. If you are running OEL 6.9, upgrade to a supported Linux distribution before upgrading to NSX Advanced Load Balancer 21.1.3.
- vCenter Read Access cloud is deprecated in NSX Advanced Load Balancer 21.1.3 and support for vCenter Read Access will be removed in a future release of NSX Advanced Load Balancer. If you are using vCenter Read Access environment, it is recommended to migrate to vCenter Write Access or vCenter No Access.
- In case of Service Engine upgrade in a Nutanix Acropolis Hypervisor (AHV) environment, refer to the pre-upgrade changes.

Issues Resolved in 21.1.2 Patch Releases

Issues Resolved in 21.1.2-2p10

- 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-141620: If Resource Manager process is unable to connect to Redis port 5001, it will hang instead of being properly shutdown and restarted.

Issue Resolved in 21.1.2-2p9

Release Date: 09 June 2022
* AV-136469: The error VirtualService object not found when adding a GSLB pool member for a site with a parent/child virtual service.

Issue Resolved in 21.1.2-2p8

Release Date: 02 June 2022
* AV-136539: Spinning SEs from Azure market place does not work. All the offers have been invalidated.

Issues Resolved in 21.1.2-2p7

Release Date: 22 March 2022
* AV-138352: Multiple updates to enhanced virtual service parent could result in a crash when traffic is sent to its child virtual service. * AV-135843: After applying the Controller patch, the indexer service fails.

Issues Resolved in 21.1.2-2p6

Release Date: 2 March 2022
* AV-136694: When importing an EC SSL certificate, and adding a passphrase, the EC encrypted private key is not exported as a string. * AV-136068: Service Engine failure due to insufficient memory. * AV-135843: After applying the Controller patch the indexer service fails. * AV-132736: Private-keys uploaded as part of Certificate are explicitly moved to avoid disclosure with any GET APIs. * AV-131472: Auto-download of CRS via Pulse fails * AV-130199: GSLB sites go out of sync with "Controller Faults Deprecated API version in use. The minimum api version supported is 18.2.6. Please check events for details."

Issues Resolved in 21.1.2-2p5

Release Date: 22 December 2021
* AV-132122: RSS does not work for Mellanox ConnectX-4 VLAN interfaces

What's New in 21.1.2-2p4

Release Date: 12 December 2021
* RSS support for LSC cloud deployments on VMware virtual machines. ### Issues Resolved in 21.1.2-2p4 * AV-129063: The GeoDB object and file objects are not recreated after upgrade to the Enterprise tier.

- AV-130838: Issue with TCP checksum offload.
- AV-131554: Service Engine failure occurs when a misconfigured SSL profile is attached to a pool.
- AV-130669: Cloud UUID is not populated correctly due to which DNS resolution on SE fails.
- AV-132339: Incorrect accounting of opackets & obytes of interface statistics in non-DPDK mode.
- AV-132431: Mitigation for CVE-2021-44228.

What's New in 21.1.2-2p3

Release Date: 26 November 2021
* AV-130700: LSC DPDK mode support to handle memory fragments for hosts with greater than 256 GB memory.

Issues Resolved in 21.1.2-2p3

- 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-129080: NSX Advanced Load Balancer does not sign the SAML authentication requests despite SSL Key and certificate being attached to the SAML virtual service.
- 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-130327: GSLB configuration sync fails when site is represented by Cluster-VIP/FQDN/public-network address translated IPs.
- 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.

What's New in 21.1.2-2p2

Release Date: 03 November 2021
* AV-128013: Support for kernel version 3.10.0-1160.45.1.el7.x86_64

Issues Resolved in 21.1.2-2p2

- 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-128044: When streaming request logs over Syslog format, the virtual service name is not included in the streamed logs.
- AV-128339: If the GSLB site was configured with an FQDN instead of an IP address, the GSLB service page failed to render properly, and the URL to the member site was not generated correctly.

Key Change in 21.1.2-2p2

- AV-121820: By default faults are not available in the inventory APIs. A query parameter to include faults is introduced in the inventory APIs.

Key Changes in 21.1.2-2p1

Release Date: 22 October 2021
* AV-127130: Support round-robin selection of vCenter rather than random selection in NSX-T cloud with multiple vCenters.

What's New in 21.1.2

Release Date: 14 October 2021
To refer to the upgrade checklist, click here.

Cloud Connector

- GCP: Support to update SE Project ID cloud configuration

- OpenStack: Support for OpenStack Wallaby

Load Balancer Networking

- BGP: BFD support for multi-hop deployments

Issues Resolved in 21.1.2

- AV-116516: Graceful disable of server does not work for existing client connections to an L7 virtual service even when connection multiplex is disabled.
- AV-118269: Network resolution of GSLB site persistence pool fails when using per tenant VRF in vCenter. This can cause the VS placement to fail if the site persistence is enabled before the VS is placed on all requested number of SEs.
- AV-120022: In FIPS mode, TLS persistence on the pool used by the L7 virtual service may not be working as expected.
- AV-120446: HSM: Virtual service with RSA certificates is inaccessible when HSM integration with Thales Luna HSM is enabled, and the Thales Luna HSM has FIPS enabled.
- AV-121761: LSC: On hosts with large memory (>= 256 GB), when the Controller is also running on the same host, the Service Engine may fail due to memory fragmentation.
- AV-122119: NSX-T cloud configuration APIs are failing on the Controller version 21.1.1, with header X-Avi-Version 20.1.6.
- AV-122772: SE fails when auto gateway is enabled and the value of TCP maximum segment size (MSS) is 0 for IPv6 connections.
- AV-122836: When GSLB leader site is represented with cluster VIP, configuration replication between sites is not working.
- 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-124936: GRO in DPDK mode may be impaired for the following NIC families:
  - Virtio
  - ENA
  - VMXNET3
- AV-125098: Upgrade to NSX Advanced Load Balancer fails in the tiers BASIC and ESSENTIALS.
- AV-125377: External health monitor is unable to invoke ping since it requires raw socket access privileges.
- AV-125530: During SE restart, a race condition could potentially result in SE failure.
- AV-125682: GCP cloud fails to connect to the GCP API servers with `x509.CertificateInvalidError`.
- AV-126067: The rollback system fails (`with AttributeError:prev_patch_img_path`) when the previous version has more than two patch versions
- AV-126143: High Latency and reduced throughput may be observed on Service Engines running in the below ecosystems:
  - Linux Server Cloud using NICs apart from Mellanox ConnectX-4 and ConnectX-5 series

    - Cisco CSP
    - OpenStack
    - Google Cloud Platform

- 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, SE may fail due to a race condition during packet transmission on vNICs that have VLAN configured.
- 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

Key Changes in 21.1.2

- `show servicenengine` <se> `cpu` is extended to display cpu set information.
- `X_AVI_VERSION (AVI_API_VERSION)` is removed from the response header.
- As prevention against potential security threats, NSX Advanced Load Balancer version details will now be revealed only to authenticated users at all endpoints like CLI, API, and UI.
  The following endpoints are secured from displaying version related information:

    - initial-data
    - cluster/runtime
    - cluster/status

  To view the version details, ensure your account is authenticated.

  ```
  **Note**:  The version details are permanently removed from the Controller SSH login banner.
  ```

- Starting with NSX Advanced Load Balancer version 21.1.2, roles can only be created in the admin tenants.

Known Issues in 21.1.2

- AV-127481: Auto-deployment of CRS might fail.
  Workaround: Manually download the CRS and upload it to the system.
- AV-132122: Mellanox NICs [ConnectX-4/ConnectX-4 Lx/ConnectX-5] : RSS with VLAN tagged packets do not work.
- AV-126071: System limit on the number of virtual services that can be created is not honoured. The total virtual service created in the system exceeds the max virtual service limit in the system by 1.
- AV-142641: Macro API for virtual service deletion does not support API migration below X-Avi-Version 20.1.1.

Checklist for Upgrade to NSX Advanced Load Balancer Version 21.1.2 Refer to this section before initiating upgrade.

- Upgrade to NSX Advanced Load Balancer is only supported from the following versions:
  - Version 18.2.6 through 18.2.13
  - Version 20.1.1 through 20.1.7
  - Version 21.1.1
- NSX Advanced Load Balancer 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 NSX Advanced Load Balancer version 21.1.1, it is recommended to upgrade to a current vCenter version. For more information, refer to the System Requirements article.
- Starting with NSX Advanced Load Balancer 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.
- The default disk size for new SEs is 15 GB.
  For OpenStack deployments, ensure that the disk size for the requisite flavors is increased to a minimum of 15 GB
- 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 License Management article for more information.
- NSX Advanced Load Balancer 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.

Issues Resolved in 21.1.1 Patch Releases

Issues Resolved in 21.1.1-2p8

Release Date: 02 June 2021 * AV-142624: Events and logs are timing out and new events anc logs are not visible on the UI or 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-140199: For TLS client, handshake API does not work as expected when connection is terminated after log server restart * AV-139352: Virtual service switchover on ACI based environment can lead to MAC-IP mapping flap eventually leading to blocking of VIP * AV-135843: After applying the Controller patch, the indexer service fails * AV-120370: When configuring the client request data in the HTTP Health monitor with "/r" in the field, '/r' is converted to '/n'

Issues Resolved in 21.1.1-2p7

Release Date: 03 March 2021 * AV-135843: After applying the Controller patch, the indexer service fails. * AV-130533: In a VMware cloud deployment, with ESX version 7.x, L2 DSR TCP and HTTP health monitor may fail due to incorrect csum handling. * AV-129245: In case of CSR (Certificate Signing Request) through the Avi UI, on importing the valid certificate, the Save button in the Edit Certificate screen is greyed out.

Issues Resolved in 21.1.1-2p6

Release Date: 05 February 2021 * AV-136068: Service Engine failure due to insufficient memory. * 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-132122: RSS does not work for Mellanox ConnectX-4 VLAN interfaces. * AV-131472: Auto-download of CRS via Pulse fails

What's New in 21.1.1-2p5

Release Date: 14 December 2021 * AV-132339: Incorrect accounting of opackets & obytes of interface statistics in non-DPDK mode.

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

What's New in 21.1.1-2p4

Release Date: 29 November 2021 * AV-131221: RSS support for LSC cloud deployments on VMware virtual machines.

Issues Resolved in 21.1.1-2p4

- 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.

What's New in 21.1.1-2p3

Release Date: 23 November 2021

- AV-130700: LSC DPDK mode support to handle memory fragments for hosts with greater than 256 GB memory. ### Issues Resolved in 21.1.1-2p3
- 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-128220: Patch install from NSX Advanced Load Balancer version 21.1.1-2p1 to version 21.1.1-2p2 gets stuck at 35%.
- 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-129063: The GeoDB object and file objects are not recreated after upgrade to the Enterprise tier.
- AV-129080: NSX Advanced Load Balancer does not sign the SAML authentication requests despite SSL Key and certificate being attached to the SAML virtual service.
- 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-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.

Issues Resolved in 21.1.1-2p2

- AV-126389: When RSS is enabled, SE may fail 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-126143: High Latency and reduced throughput may be observed on Service Engines running in the below ecosystems:
    - Linux Server Cloud using NICs apart from Mellanox ConnectX-4 and ConnectX-5 series
    - Cisco CSP
    - OpenStack
    - Google Cloud Platform
- AV-126067: From version 21.1.1, the rollback system fails (with AttributeError:prev_patch_img_path) when the previous version has more the two patch versions
- AV-125530: During SE restart, a race condition could potentially result in SE failure.
- AV-125098: Upgrade to version 21.1.1 fails in the license tiers 'BASIC' and 'ESSENTIALS'
- AV-124931: Auto-download of CRS fails when proxy is configured.

Issues Resolved in 21.1.1-2p1

Release date: 24 September 2021
* AV-124931: Auto-download of CRS fails when proxy is configured. * AV-124588: HTTPS requests with chunked transfer encoding might timeout when DataScript or WAF is enabled on the virtual service. * AV-121987: In an Avi Controller with an older Avi API version, `local_file` can not be configured as `fail_action` on pool/pool group * AV-121573: If the Controller does not have access to the internet, creating SE image for vCenter cloud will fail after upgrade. * AV-116516: Graceful disable of server does not work for existing client connections to an L7 virtual service even when connection multiplex is disabled

What's New in 21.1.1

Release date: 12 August 2021
To refer to the upgrade checklist, click here.

Application Security

- DDoS: Detection and mitigation of Layer 7 (DNS) attacks: DNS Amplification Egress and DNS Reflection
- Bot Management: Support to detect, classify and manage bot traffic

  Note: This feature is currently under tech preview.

Automation

- Support for distributing Avi SDK and Config roles as Ansible Collection

Avi Pulse

- Proactive Tech Support Management including:
    - Auto Case Creation On SE Failure
    - Auto Case Creation On System Failure

  Note: This feature is currently under tech preview.

Cloud Connector

- AWS: Support to track Controller and Service Engine upgrade information via the custom tags Current Avi Version and Avi Upgrade Date
- AWS:?Extended support to Gov Cloud US-East region
- GCP: Support for Shared VPC Multi-NIC
- Microsoft Azure: The maximum number of availability zones (AZ) for SEdistribution is increased from two to three
- LSC: Support for base kernel versions 3.10.0-1160.25.1.el7.x86_64 and 3.10.0-1160.31.1.0.1.el7.x86_64
- LSC: Mellanox NICs: Mellanox Technologies MT27800 Family [ConnectX-5]

Core LB Features

- Persistence: Honor persistence when gracefully disabling a server in a pool
- Pools: L4 and L7 virtual services can use the same pool for backend traffic
- Health Monitoring: Support for External PostgreSQL Health Monitors
- HTTP/2: Support for HTTP/2 upgrade on the client side
- HTTP/2: Support for caching
- SE Time Flow Tracker: Support to track the network characteristics, processing time at key checkpoints and flag queuing delays in a packet journey through the network appliance
- Support to add query in an HTTP request redirect policy
- The flag?`http only`?is introduced in the? HTTP Cookie Persistence Profile ?to set the? HTTP Only?attribute in the cookie. This prevents the client side scripts from accessing this cookie
- For every virtual service, user-configurable default HTML error page profile (Custom-Error-Page-Profile) is available for Avi-generated 4xx and 5xx errors. This feature is available only in the ENTERPRISE license tier
- Support to update the port to the hostname in the host header, in requests to the servers via the field ?Append Port ? during pool configuration
- Support for dynamic modification of the number of `se dps` without rebooting the Service Engine
- Support to configure specific set of signature algorithms for an SSL profile
- Support to configure Elliptic Curve Cryptography (ECC) Cipher Suites in an SSL profile
- Support for Service Engine Datapath Isolation
- Enhancing GeoDB for Layer 7 and network policies (operations like HTTP security policies, and more):
    - Granular GeoDB based on region, city, ASN, ISP, etc.
    - Support to configure user-defined GeoDB mapping attributes

DataScripts

- The support to return all geo information available, including any user mapping matches for a target IP via the flag? *All*? introduced for the DataScript function?`avi.utils.get_geo_from_ip`
- API support to return the total number of open connections per Service Engine attached to the current virtual service
- API support to return the total number of service engines attached to the current virtual service
- API support to modify the existing cookie attributes value in the HTTP response
- Support for SSL events in DataScripts for L7 and L4 SSL virtual services
- Support for STARTTLS : A new DataScript event in L4 SSL (`VS_DATASCRIPT_EVT_TCP_CLIENT_ACCEPT`) and the APIs?`avi.ssl.disable_ssl()`?and?`avi.ssl.enable_ssl()`?are introduced to disable/ enable traffic during SSL respectively
- Support for XML parsing in L7 DataScripts

DNS & IPAM

- Support for third party IPAM providers using respective REST API via Custom IPAM Profile
- DNS Query failed events will be raised as unsuccessful DNS lookup

Networking

- IPv6: Support to deactivate IPv6 learning in SE using the field? `deactivate_ipv6_discovery`?in the Service Engine group properties
- Packet Capture support for NAT flows

Observability and Monitoring

- Monitoring: E-mail Notification timestamp is displayed with the local timezone
- Support to enable/ disable inventory faults per object

Platform

- Tenancy: Granular RBAC support for SE Group objects
- TSO (TCP Segmentation Offload) support in environments where DPDK mode is enabled for packet processing, for deployments where SE routing is enabled
- Migration of Basic Auth to SSO Policy

User Interface

- User Interface Enhancements
- Internationalization (i18n): NSX Advanced *Load* Balancer UI support for Japanese?and?Simplified Chinese

WAF

- ICAP support extended for NSX Defender?s (lastline) ICAP server to prevent malicious file uploads
- Support for XML XPath based exclusion in processing WAF rules

Issues Resolved in 21.1.1

- 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-102522: When FIPS mode is enabled, the Service Engine may fail if a virtual service is configured with the http security policy with the rate limiting rules `per_client_ip and per_uri_path`.
- AV-111140: Unable to search audit logs for usernames containing the special character "."
- 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-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-115797: The `SE_DOWN` event is not displayed under Operations > Events > All Events and user login events are not displayed in the Config Audit Trail.
- AV-116043: Cluster based events are not generated when the Controller cluster leader is restarted.
- AV-116327: High disk usage on the Controller leader node due to excess files in `/var/lib/avi/systeminfo`.
- 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-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-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-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-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-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: ';' 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-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-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-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-122119: NSX-T cloud configuration APIs failing on a Controller with header X-Avi-Version 20.1.6

Key Changes in 21.1.1

- The maximum number of characters in a `vip_id` is limited to 16 characters.
- Launching Bash access in the CLI shell using cli@<controlleriip> is deactivated.
- Prior to NSX Advanced Load Balancer version 21.1.1, 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 21.1.1, 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.
- For pools and pool groups, the special character "$" is not allowed in the field Name.
- After switching to the Basic/ Essentials license tier, the default Error Page Profile reference is removed from the virtual service object.
- The DOS_ATTACK events will be shown on the UI as non-internal events. That is, without clicking on the Internal checkbox, the user can see these events directly on the Controller events UI.
- 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.
- 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.
- LDAP : Support for including exclamation mark (!) in the username for Controller authentication

Known Issues in 21.1.1

- AV-126143: High latency and reduced throughput may be observed on Service Engines running in the below ecosystems:
  - Linux Server Cloud using NICs apart from Mellanox ConnectX-4 and ConnectX-5 series
  - Cisco CSP
  - OpenStack
  - Google Cloud Platform
    Work Around: Disable TSO configuration for each Service Engine Group. For more details on the CLI, refer to Enabling GRO and TSO on an Avi SE.
    Notes:
  - TSO is enabled by default in environments supporting DPDK. Refer to TSO, GRO, RSS, and Blocklist Feature on Avi Vantage for more details.
  - Environments using VMXNET3 (vCenter, NSX-T, VMC on AWS, AVS, GCVE) and ENA (AWS) are not impacted.

- AV-121113: Using GeoDB files that are not sorted in ascending order in the System-GeoDB can result in IP Groups missing entries.
  Workaround: Upload the GeoDB custom file object with IP addresses mapped to different Geo attributes only in ascending order.

- AV-121573: If the Controller does not have access to the internet, creating SE image for vCenter cloud fails after upgrade.

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

- AV-132122: Mellanox NICs [ConnectX-4/ConnectX-4 Lx/ConnectX-5] : RSS with VLAN tagged packets do not work.

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

System Limits Enforced

- System Limits applied for L7 objects:
  - HTTP Policies
  - Caching
  - Compression
- System Limits applied for L4 objects

Checklist for Upgrade to NSX Advanced Load Balancer Version 21.1.1 Refer to this section before initiating upgrade.

- Upgrade to NSX Advanced Load Balancer is only supported from the following versions:
  - Version 18.2.6 through 18.2.12
  - Version 20.1.1 through 20.1.6

- NSX Advanced Load Balancer 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 NSX Advanced Load Balancer version 21.1.1, it is recommended to upgrade to a current vCenter version. For more information, refer to the System Requirements article.

- Starting with NSX Advanced Load Balancer 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.
- The default disk size for new SEs is 15 GB.
  For OpenStack deployments, ensure that the disk size for the requisite flavors is increased to a minimum of 15 GB
- 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 License Management article for more information.
- NSX Advanced Load Balancer 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.

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

- NSX Advanced Load Balancer Installation Guides

Copyrights and Open Source Package Information

For copyright information and packages used, refer to open_source_licenses.pdf.

Additional Reading

Protocol Ports Used by NSX Advanced Load Balancer for Management Communication