CITRIX SD-WAN 11.0.0 Release Notes

Copyright and Trademark Notice

Citrix Systems assumes no responsibility for errors in this document, and retains the right to make changes at any time, without notice.

Contents

Introduction

This release notes describes fixed issues and known issues applicable to Citrix SD-WAN software release 11.0.0 for the SD-WAN Standard Edition, WANOP, Premium Edition appliances, and SD-WAN Center.

In Citrix SD-WAN release 11.0.0, the underlying OS/kernel for the SD-WAN software is upgraded to a newer version, requiring an automatic reboot to be performed during the upgrade process. As a result, the expected time for upgrading each appliance is increased by approximately 100 seconds. In addition, by including the new OS, the size of the upgrade package transferred to each branch appliance is increased by approximately 90MB.

For information about the previous release versions, see the Citrix SD-WAN documentation.

What's New

Application centric enhancements

Dynamic PAC file customization

With the increase in enterprise adoption of mission-critical SaaS applications and distributed workforce, it becomes highly critical to reduce latency and congestion that are inherent in traditional methods of backhauling traffic through the Data Center. Citrix SD-WAN allows direct internet break out of SaaS applications such as Office 365.

However, if there are explicit web proxies configured on the enterprise deployment all traffic, including SaaS application traffic, are steered to the web proxy making it difficult for classification and direct internet breakout. The solution is to exclude SaaS application traffic from being proxied by customizing the enterprise PAC (Proxy Auto-Config) file.

Citrix SD-WAN 11.0.0 allows proxy bypass and local Internet breakout for Office 365 application traffic by dynamically generating and serving custom PAC file.

LACP for link redundancy

Link aggregation allows you to support port redundancy. In this case, two or more ports can be grouped together to work as a single port to send out the traffic at any given time.

LACP mainly supports **Active** and **Backup**. That means one port always be in active mode and when the current active port goes down, the other port stay up. The active and backup support relaying on the DPDK package for LACP functionality. The LACP feature is available only on DPDK supported platforms except VPX/VPXL.

Standby and Metered Link

Disable if Data Cap reached option is introduced in release 11.0.

- If the **Disable if Data Cap reached** checkbox is selected, then the metered link and all its related paths will be disabled until the next billing cycle, if the data usage reaches the data cap.
- By default, the **Disable if Data Cap reached** checkbox will be unchecked state, where it retains the current mode or state set for the metered link to be continued after data cap is reached until the next billing cycle.

210-SE LTE authentication

A new Authentication input field is introduced in the APN settings form. There are 4 possible values for this new field– None, PAP, CHAP, PAPCHAP.
The authentication field has been added for APN settings in SDWAN Center UI, SDWAN appliance UI and in REST API.

Packet capture

You can use the **Packet Capture** option to intercept the data packet that is traversing over the selected active interfaces present in the selected site.

Active interfaces are available for packet capture in the selected site. Select an interface or add interfaces from the drop-down list. At least one interface needs to be selected to trigger a packet capture.

Note: The ability to run packet capture across all the interfaces at once helps to speed up the troubleshooting task.

In-band management

Citrix SD-WAN allows you to manage the SD-WAN appliance in two ways, out-band management and in-band management. Out-band management allows you to create a management IP using a port reserved for management, which carries management traffic only. In-band management allows you to use the SD-WAN data ports for management, which will carry both data and management traffic, without having to configure an addition management path.

Enable RED for ICA traffic

From 11.0.0 release on wards, the Random Early Detection (RED) is set to ON by default for ICA traffic.

Cloud services

Cloud Direct Service

The Cloud Direct service delivers SD-WAN functionalities as a cloud service through reliable and secure delivery for all internet-bound traffic regardless of the host environment (data center, cloud, and internet). This improves network visibility and management. It enables partners to offer managed SD-WAN services for business critical SaaS applications to their end customers.

Palo Alto Network integration with SD-WAN

Palo Alto networks deliver cloud-based security infrastructure for protecting remote networks. It provides security by allowing organizations to set up regional, cloud-based firewalls that protect the SD-WAN fabric.

Prisma Access service for remote networks allows you to on-board remote Network locations and deliver security for users. To connect your remote network locations to the Prisma Access service, you can use the Palo Alto Networks next-generation firewall or a third-party, IPsec-compliant device including SD-WAN, which can establish an IPsec tunnel to the service.

Citrix SD-WAN appliances can connect to the Palo Alto cloud service (Prisma Access Service) network through IPsec tunnels from SD-WAN appliances locations with minimal configuration.

Reporting

Reports based on HDX user name

In HDX reporting page**,** you can view the following report types:

- HDX Site Stats
- HDX Summary (applicable for both HDX information channel available and unavailable sessions)
- HDX User Sessions (applicable for only HDX information channel available sessions only)
- HDX Apps (applicable for only HDX information channel available sessions only)

Enable HDX User Reporting option is newly added in the SD-WAN configuration editor. Enabling this option will generate newly added user based reports (HDX Summary, HDX User Sessions and HDX Apps) and these reports will be available in SD-WAN Center. This is not applicable for **HDX Site Stats** report. This option is available at global level as well as site level similar to enable DPI option.

Routing Enhancements

OSPF redistribution tags

You can use OSPF tags to prevent routing loops during mutual redistribution between OSPF and other protocols. Specifying different tags for SD-WAN and BGP learnt routes allows these routes to be installed in the OSPF routing table.

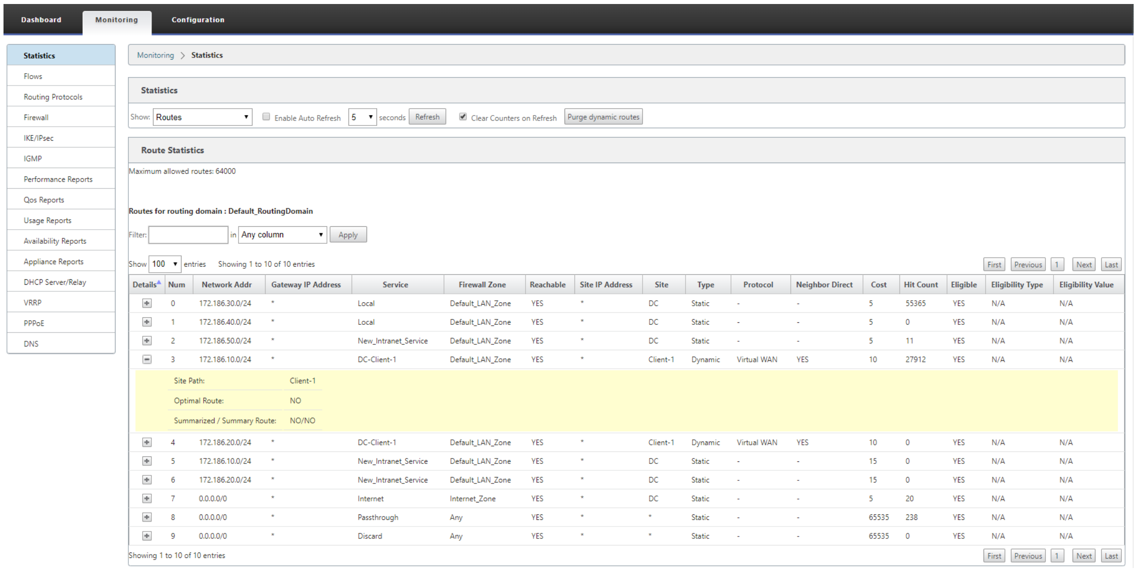
Protocol preference

When Citrix SD-WAN learns a route prefix through virtual paths, OSPF protocol, or BGP protocol, at the same time, the following default preference order is introduced.

- OSPF -150
- BGP – 100
- SD-WAN – 250

Route statistics

Additional details such as **Site Path**, **Optimal Route**, **Summarized / Summary route** are included in Route Statistics report.



Statistics

Show: Routes ☐ Enable Auto Refresh 5 seconds ☑ Clear Counters on Refresh

Route Statistics

Maximum allowed routes: 64000

Routes for routing domain : Default_RoutingDomain

Filter: in Any column

Show 100 entries Showing 1 to 10 of 10 entries

Details	Num	Network Addr	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Eligibility Value
⊞	0	172.186.30.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	55365	YES	N/A	N/A
⊞	1	172.186.40.0/24	*	Local	Default_LAN_Zone	YES	*	DC	Static	-	-	5	0	YES	N/A	N/A
⊞	2	172.186.50.0/24	*	New_Intranet_Service	Default_LAN_Zone	YES	*	DC	Static	-	-	5	11	YES	N/A	N/A
⊟	3	172.186.10.0/24	*	DC-Client-1	Default_LAN_Zone	YES	*	Client-1	Dynamic	Virtual WAN	YES	10	27912	YES	N/A	N/A
Site Path: Client-1 Optimal Route: NO Summarized / Summary Route: NO/NO																
⊞	4	172.186.20.0/24	*	DC-Client-1	Default_LAN_Zone	YES	*	Client-1	Dynamic	Virtual WAN	YES	10	0	YES	N/A	N/A
⊞	5	172.186.10.0/24	*	New_Intranet_Service	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
⊞	6	172.186.20.0/24	*	New_Intranet_Service	Default_LAN_Zone	YES	*	DC	Static	-	-	15	0	YES	N/A	N/A
⊞	7	0.0.0.0/0	*	Internet	Internet_Zone	YES	*	DC	Static	-	-	5	20	YES	N/A	N/A
⊞	8	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static	-	-	65535	238	YES	N/A	N/A
⊞	9	0.0.0.0/0	*	Discard	Any	YES	*	*	Static	-	-	65535	0	YES	N/A	N/A

Showing 1 to 10 of 10 entries

AS path length

BGP protocol uses the AS path length attribute to determine the best route. The AS path length indicates the number of autonomous systems traversed in a route. Citrix SD-WAN leverages the BGP AS path length attribute to filter and import routes.

Citrix SD-WAN Center

SD-WAN Center appliance certificate

Previously, a pre-defined appliance certificate was used which was already installed in the SD-WAN Center. With Citrix SD-WAN 11.0.0 release, you can regenerate the appliance certificate on the MCN which will replace the pre-defined certificate and then install on SD-WAN Center.

Security admin role in SD-WAN Center

Security Admin role is added to SD-WAN Center. A Security Administrator has the read-write access only for the firewall and security related settings in configuration editor, while having read-only access to the remaining sections.

Deploy SD-WAN in Azure from SD-WAN Center

You can deploy Citrix SD-WAN on Azure from Citrix SD-WAN Center. Citrix SD-WAN for Azure enables organizations to have a direct secure connection from each branch to the applications hosted in Azure eliminating the need to backhaul cloud bound traffic through a data Center.

Platforms, scalability, and deployments

6K node scale for networks

Citrix SD-WAN 11.0.0 supports a network of up to 6000 sites with a maximum of 128 regions in a tiered network architecture.

SD-WAN SE on Google Cloud Platform

Deploying Citrix SD-WAN SE VPX on Google Cloud Platform (GCP) enables organizations to establish a direct and highly secure connection from each branch to the applications hosted in GCP. This eliminates the need to backhaul cloud bound traffic through the Data Center. The key benefits of using Citrix SD-WAN on GCP are:

- Create direct connections from every branch site to GCP.
- Ensure an always-on connection to GCP.
- Extend your secure perimeter to the cloud.
- Evolve to a simple and easy to manage branch network.

Citrix SD-WAN 1100 - enhancement on SFP to support HA with Y cable

The available Small Form-factor Pluggable (SFP) ports on 1100 appliances can be used with fiber optic Y-Cables to enable high availability feature for Edge Mode deployment. On the 1100 SE/PE appliance the splitter cable split end connects to fiber ports of two 1100 appliances that are configured in high availability pair.

REST API

The following APIs are introduced:

- Monitoring API for Appliance HA status.
- Mobile Broadband APIs for sim pin summary and sim pin operations.
- Configuration editor APIs for proxy auto configuration file settings and site proxy auto configuration file settings.
- SD-WAN Center reports APIs for HDX apps and HDX sessions.
- SD-WAN Center reports APIs for HDX summary.

Fixed Issues

SDWANHELP-590: Citrix SD-WAN Center security enhancements.

SDWANHELP-594: Virtual paths are marked as DEAD for all the sites when corrupted control packet is processed. If the control packet is malformed it is dropped and paths becomes inactive.

SDWANHELP-600: After a software upgrade from release 9.3.2 to 9.3.5, the post upgrade SNMP System Name shows as the default Virtual WAN, and does not use the device hostname.

SDWANHELP-617: Dynamic Virtual Path is not allocated with required bandwidth when the **Adaptive Bandwidth Detection** feature is enabled on any of the WAN links forming Dynamic Virtual Path.

SDWANHELP-626: Unable to access Citrix SD-WAN Center due to memory outage.

SDWANHELP-649: Excessive Virtual Path packet retransmissions might experience with low bandwidth utilization, high loss or congestion, and less than 20ms RTT times.

SDWANHELP-650: Configuration process such as adding, editing, cloning a site, or performing audit, makes the MCN GUI unresponsive.

SDWANHELP-654: SD-WAN WANOP 4000 appliance might be interrupted while parsing ICA connections.

SDWANHELP-666: PPTP/GRE tunnel over internet service fails to get establish when internet access for all routing domains feature is enabled. The SD-WAN appliance is acting as pass-through and not an endpoint.

SDWANHELP-671: The licensing log files consume large amount of disk space while using remote licensing server.

SDWANHELP-674: On the SD-WAN EE/PE appliance, you need to change the hostname for WANOP communication.

SDWANHELP-676: Domain service automatically re-starts even when domain service occasionally fails.

SDWANHELP-680: Audit configuration gets failed on deleting **Intranet** service in a site, if an **Intranet** service with same name existed in another site.

SDWANHELP-682: The **Site location** field is not saved, while creating a site using basic configuration editor.

SDWANHELP-698: If a Citrix SD-WAN Appliance is deployed in serial high availability (FTW) mode and if a LAN port (in FTB) is defined in high availability interfaces for tracking, then the high availability failover does not happen if the LAN port went down.

SDWANHELP-703: IPSec traffic to Zscaler is impacted when memory usage peaks are observed.

SDWANHELP-712: LTE connected virtual path is reported as DOWN even when the modem is operational on the branch SD-WAN appliance.

SDWANHELP-725: SD-WAN appliance sends the HA virtual path information to SD-WAN Center and it throws statistics error as it is unable to recognize it.

SDWANHELP-734: The default class name does not get updated after changing it.

SDWANHELP-735: The “Active OS partition is completely full…..” alert is observed on the 1100 platform edition configured as PE in releases 10.2.0 and 10.2.1. You need to manually restart the 1100 appliance after upgrading to release 10.2.2.

SDWANHELP-736: SD-WAN service might be interrupted during the configuration change in a two-box deployment mode.

SDWANHELP-742: SD-WAN service might be interrupted during STS bundle collection when the number of Application QoS rules exceeds the IP based QoS rules.

SDWANHELP-746: While creating two different firewall rules, an audit error might occur if an IP address and a port number are same even if the protocols are different.

SDWANHELP-748: The licenses does not get applied on multiple sites.

SDWANHELP-754: When you delete the DHCP configuration, the sub objects such as DHCP relays and DHCP option sets still remain as stale entries. All the child objects need to be deleted when the parent DHCP element is deleted.

SDWANHELP-768: 5100 Premium Edition (PE) virtual WAN service restarts when establishing signalling channel. This occurs due to ephemeral port conflict between multiple WANOP packet engines.

SDWANHELP-795: The path bandwidth test is interrupted, if:

- The path bandwidth test is run on branches that are isolated from MCN due to the virtual path is down/disabled.
- The MCN performs branch WAN link property change, when the branches come up.

SDWANHELP-799: The SD-WAN learning OSPF prefixes with cost “AS IS” from neighbor routers and allowing export of these to peer SD-WAN devices. If the redistribution cost is changed externally on the neighbor router (such as, redistributing BGP/RIP into OSPF metric cost change), the newly changed cost is updated only on the immediately connected SD-WAN device but not updated to the peer SD-WAN devices.

SDWANHELP-801: SD-WAN service might be interrupted when processing ICMP packets to its Virtual IP at high rate and configuration update is triggered simultaneously.

SDWANHELP-808: Due to legacy reasons, SD-WAN does not allow few patterns in site configuration. This particular site contains APN in its name. It is misleading only in the SD-WAN GUI and doesn't affect any operation at the site level.

SDWANHELP-812: Provisioning 10.2.x fails on 1100 Premium Edition (PE) platform as it did not create DBC disk.

SDWANHELP-818: Once dynamic routes have learnt and converged, if a configuration update happens that has a cost change performed, post activation the route ID of dynamically learnt routes are reset to '0' instead of staying enumerated causing even optimal routes to be deleted in a route update to the neighbour.

SDWANHELP-819: SD-WAN WANOP Premium Edition (PE) unable to establish secure peering properly.

SDWANHELP-830: The CA certificates used for auto-secure peering in SD-WAN WANOP are getting deleted upon upgrade. This impacts formation of secure peering for any new devices added to the deployment. In this case, it is required to regenerate CA certificates, delete certificates, and cert-key pairs from all sites and re-establish auto-secure peering once again after upgrading to 10.2.3.

SDWANHELP-831: Upon power cycling 210 appliances, FTW relay controller might fail to initialize, which can lead to the relay stay in closed state if configured in serial high availability (FTW) mode.

SDWANHELP-846: SD-WAN service might be interrupted when receiving ICMP packets destined to virtual IP in a multi Routing Domain deployment.

SDWANHELP-854: Under rare circumstances, if invalid packets are received, the system may restart. This issue may occur if path encryption was disabled from its default enabled state.

SDWANHELP-866: SD-WAN drops large packets because of LR0/TSO enabled.

SDWANHELP-914: Unable to apply settings when adding a path to schedule bandwidth tests for it.

SDWANHELP-916: At times, service hangs when the configuration is updated.

NSSDW-16165: Subnet added as part of region definition does not get populated in routes table.

NSSDW-16825: DHCP agent was not able to parse DHCP OFFER packets with additional padding as in case of Satellite modem.

NSSDW-17108: Selecting the first autopath group when configuring WAN Link Templates displays as "no group selected".

NSSDW-18012: At times, the virtual paths go down after configuration update on PPPoE devices.

NSSDW-19233: The Windows Azure agent is filling up with root partition because of few extensions are getting installed by Azure portal.

Known Issues

NSSDW-17238: VPXL does not show more than 4 interfaces when created in XenServer.

Workaround: Set kernel parameter for XenServer as shown below and reboot the XenServer.

/opt/xensource/libexec/xen-cmdline --set-xen gnttab_max_frames=256

NSSDW-19132: In case of HDX MSI sessions, connection state is shown as **INVALID** for some of the IDLE streams in **HDX User Sessions Report** under HDX tab.

NSSDW-20154: On reconnecting to the same session, application related details are not re-sent by Xen Application/Xen Desktop server. Hence, Data in **HDX Apps** report might not be shown for that particular session.

NSSDW-20371: When **Centralized Licensing** is enabled, downgrade to older releases throws an error - *ERROR: Failed to parse license models*.

Workaround: Disable the centralized licensing and proceed with the downgrade. The appliances gets a grace license. After the downgrade is complete, you can re-enable centralized licensing and apply the config through the Change management.

NSSDW-20500: On 5100 PE, when domain join operation is initiated for the first time we may see a warning message stating that WANOP is initializing.

Workaround: Re-join to domain after two mins.

NSSDW-20527: UI allows configuring PPPoE for LTE interface, which is not expected or allowed.