Cisco Nexus Dashboard Orchestrator Release Notes, Release 3.7(1)

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Contents

New Software Features 4

New Hardware Features 5

Changes in Behavior 5

Open Issues 7

Resolved Issues 10

Known Issues 12

Compatibility 14

Scalability 14

Related Content 14

Documentation Feedback 15

Legal Information 15

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

This document describes the features, issues, and deployment guidelines for Cisco Nexus Dashboard Orchestrator software.

Cisco Multi-Site is an architecture that allows you to interconnect separate Cisco APIC, Cloud APIC, and DCNM domains (fabrics) each representing a different region. This helps ensure multitenant Layer 2 and Layer 3 network connectivity across sites and extends the policy domain end-to-end across the entire system.

Cisco Nexus Dashboard Orchestrator is the intersite policy manager. It provides single-pane management that enables you to monitor the health of all the interconnected sites. It also allows you to centrally define the intersite configurations and policies that can then be pushed to the different Cisco APIC, Cloud APIC, or DCNM fabrics, which in term deploy them in those fabrics. This provides a high degree of control over when and where to deploy the configurations.

For more information, see the “Related Content” section of this document.

Note: The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Date	Description
February 27, 2023	Additional open issues CSCwe35911, CSCwe27875, CSCwe26871.
January 30, 2023	Additional known issues CSCwc52360 and CSCwa87027.
October 11, 2022	Additional open issue CSCwd22543.
August 9, 2022	Release 3.7(1l) became available. Additional open issues CSCwc41840 and CSCwc56401 in earlier 3.7(1) releases, which are resolved in 3.7(1l).
July 25, 2022	Release 3.7(1k) became available. Additional open issues CSCwc43830, CSCwc12353, CSCwc15163 in earlier 3.7(1) releases, which are resolved in 3.7(1k).
July 18, 2022	Additional open issue CSCwc12353.
May 24, 2022	Release 3.7(1j) became available. Additional open issues CSCwb10342, CSCwb32631, CSCwb33105, CSCwb41977, CSCwb52863, CSCwb57049, CSCwb65482, CSCwb17102, CSCwb85199, and CSCvw03174 in earlier 3.7(1) releases, which are resolved in 3.7(1j).
March 23, 2022	Release 3.7(1g) became available. Additional open issues CSCwb26063 and CSCwb26058 in Release 3.7(1d), which are resolved in 3.7(1g).
March 12, 2022	Release 3.7(1d) became available.

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

New Software Features

This release adds the following new features:

Feature	Description
Support for multiple frontend IP addresses for an internet-facing Azure Network Load Balancer	This release provides support for multiple frontend IP addresses for an internet-facing Azure Network Load Balancer. For additional information, see Configuring Multiple Frontend IP Addresses on Azure Network Load Balancer.
Support for IANA-assigned CloudSec port	You can choose to configure CloudSec encryption to use the IANA-assigned UDP port instead of the default Cisco proprietary port. For additional information, see Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics.
Support for CloudSec Encryption with Intersite L3Out	CloudSec encryption is now supported for intersite L3Out traffic for both use cases of local EPG to remote L3Out commutation and intersite transit routing (local L3Out to remote L3Out traffic. For information on configuring Intersite L3Out, see the Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics
Configuration drifts reconciliation workflow for APIC and NDFC (DCNM) sites	You can now view and resolve policy configuration discrepancies between what you deploy from the Nexus Dashboard Orchestrator and what is actually configured in each managed site. For additional information, see Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics and Cisco Nexus Dashboard Orchestrator Configuration Guide for NDFC (DCNM) Fabrics.
Scalable static port bindings with leaf/port range provisioning	VLAN configuration for switch interfaces can now be done on a range of ports and switches to simplify provisioning of multiple ports. For additional information, see Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics.
Bulk update workflow for template objects	A subset of properties for template objects of the same type can now be updated simultaneously for multiple objects. For additional information, see Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics.
Nexus Dashboard Fabric Controller 12.0(2) support	Sites managed by Cisco Nexus Dashboard Fabric Controller, Release 12.0(2) can now be onboarded to the Nexus Dashboard and managed by the Nexus Dashboard Orchestrator. For additional information, see Cisco Nexus Dashboard Orchestrator Configuration Guide for NDFC (DCNM) Fabrics.
Google Cloud site support	Cisco Cloud APIC managing Google Cloud sites can now be onboarded to the Nexus Dashboard and managed by the Nexus Dashboard Orchestrator. For more information, see Managing Google Cloud Sites Using Nexus Dashboard Orchestrator.
Multi-cloud inter-site connectivity between AWS, Azure, and Google Cloud Sites	For additional information, see the “Day-0 Operations for ACI Fabrics” chapter of the Cisco Nexus Dashboard Orchestrator Deployment Guide or the “Infrastructure Management” chapter of the Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics.

© 2020 Cisco and/or its affiliates. All rights reserved.

Feature	Description
Support for partial mesh connectivity between on-premises and AWS or Azure cloud sites	Intersite connectivity can now be established in a partial mesh configuration where only a subset of all on-premises sites have intersite connectivity to the AWS or Azure clouds sites. For additional information, see the “Day-0 Operations for ACI Fabrics” chapter of the Cisco Nexus Dashboard Orchestrator Deployment Guide or the “Infrastructure Management” chapter of the Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics.
Proxy support for cloud sites	Connectivity to Cisco Cloud APIC sites can be established via a proxy. For more information on enabling proxy when adding sites, see the “Day-0 Operations for ACI Fabrics” chapter of the Cisco Nexus Dashboard Orchestrator Deployment Guide or the “Infrastructure Management” chapter of the Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics. For more information on configuring a proxy in your Nexus Dashboard, see Nexus Dashboard User Guide for your release.
Provisioning connectivity between ACI Data Center Fabrics and Campus Networks (DNAC): • Automation of connectivity between multiple campus VNs and data center VRFs • Automation of Internet access for Campus VNs through ACI fabrics • Visibility of VN-VRF extension and connectivity status	This release of Cisco Nexus Dashboard Orchestrator adds support for Cisco SD-Access and Cisco ACI integration. The purpose of SD-Access and ACI integration is to securely connect the campus-and-branch network to the data center network. For additional information, see the “SD-Access and ACI Integration” chapter of the Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics.

New Hardware Features

There is no new hardware supported in this release.

The complete list of supported hardware is available in the “Deploying Nexus Dashboard Orchestrator” chapter of the Cisco Multi-Site Deployment Guide.

Changes in Behavior

If you are upgrading to this release, you will see the following changes in behavior:

- For all new deployments, you must install the Nexus Dashboard Orchestrator services in Nexus Dashboard release 2.1.1e or later.
- If you are upgrading your existing deployment from a release prior to Release 3.2(1), you must deploy a new Nexus Dashboard cluster and migrate your existing configuration.

  The procedure is described in detail in Cisco Nexus Dashboard Orchestrator Deployment Guide.
- If you deploy in a virtual or cloud Nexus Dashboard, downgrading to releases prior to Release 3.3(1) is not supported.
- If you deploy in a physical Nexus Dashboard cluster, downgrading to releases prior to Release 3.2(1) is not supported.

© 2020 Cisco and/or its affiliates. All rights reserved.

- If you are migrating from a release prior to Release 3.3(1), you may need to resolve any configuration drifts in the object properties that are newly managed by NDO where the default values picked by NDO differ from the custom values set directly in the fabrics' controllers.

  Any time Nexus Dashboard Orchestrator adds support for managing object properties that previously had to be managed directly in the APIC, it sets those properties to some default values for existing objects in NDO Schemas but does not push them to sites.

  To resolve the configuration drifts, you will need to re-import these objects and their properties from the fabrics' Controllers and then re-deploy the templates as described in the Cisco Nexus Dashboard Orchestrator Deployment Guide.

- Site management and on-boarding have moved to a centralized location in the Nexus Dashboard GUI.

  When migrating from a release prior to Release 3.2(1), you will need to on-board the sites using the Nexus Dashboard GUI before restoring existing configuration. The procedure is described in detail in Cisco Nexus Dashboard Orchestrator Deployment Guide.

- User management and authentication have moved to a centralized location in the Nexus Dashboard GUI.

  Existing local users defined in older Orchestrator clusters will be transferred to the Nexus Dashboard during configuration import.

  For existing remote authentication users, you will need to add the remote authentication server to the Nexus Dashboard as described in the Nexus Dashboard User Guide.

- Proxy management has moved to a centralized location in the Nexus Dashboard GUI.

  Any existing proxy configuration done in directly in the Orchestrator GUI in earlier releases will **not** be automatically transferred during the upgrade and must be manually re-added in the Nexus Dashboard as described in the Nexus Dashboard User Guide.

- Starting with Release 3.3(1), the following API changes have been implemented:

  PATCH API no longer returns the complete object that was modified, in contrast to prior releases where a complete object (such as schema) was returned by the API.

  Because Site Management and User Management have moved to a central location on Nexus Dashboard, the following API changes have been implemented to the corresponding Nexus Dashboard Orchestrator APIs:

  - User Management API v2 is introduced for querying the new user structures with original API changing to read-only mode (only GET operations are allowed, PUT/POST are removed).

    The issue which caused the User Management API v1 to incorrectly return v2 structures in Release 3.2 has been resolved and the v1 API now returns the correct structure similar to Release 3.1.

  - Site Management API v2 is introduced that allows setting a site to 'managed' or 'unmanaged' in NDO. Previous Site Management APIs are changed to read-only mode (GET operation only). Site onboarding moved to the Nexus Dashboard APIs.

  You can no longer remove DHCP Relay and DHCP Option policies until they have been removed from all associated BDs.

- Starting with Release 3.4(1), local configuration backups have been deprecated.

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

If you are upgrading from a release prior to release 3.4(1) to release 3.4(1) or later, you must download any existing local configuration backups prior to the upgrade. You will then be able to import those configuration backups to a remote backup location you configure in the Nexus Dashboard Orchestrator. For more information, see the “Operations” chapter of the Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics or Cisco Nexus Dashboard Orchestrator Configuration Guide for DCNM Fabrics.

- Cisco Data Center Network Manager (DCNM) service has been renamed to Cisco Nexus Dashboard Fabric Controller (NDFC) starting with Release 12.0.1a.

  Cisco Nexus Dashboard Orchestrator can continue managing Cisco NDFC sites the same way it managed Cisco DCNM sites previously. For a full list of service and fabric compatibility options, see the Nexus Dashboard and Services Compatibility Matrix.

Open Issues

This section lists the open issues. Click the bug ID to access the Bug Search Tool and see additional information about the bug. The " Exists In" column of the table specifies the 3.7(1) releases in which the bug exists. A bug might also exist in releases other than the 3.7(1) releases.

Bug ID	Description	Exists in
CSCwb26063	The on-premises site lose connectivity and NDO is not able to communicate with those sites. The Cloud APIC sites that are connected via proxy continue to operate.	3.7(1d)
CSCwb26058	When usage of proxy is enabled for a site on ND, NDO/MSO does not use the proxy information when contacting sites.	3.7(1d)
CSCwb10342	Audit Log streaming may not work.	3.7(1d) and 3.7(1g)
CSCwb32631	CloudSec key sequence is transiently out of order and can cause brief disruption of traffic on the affected link, but will should be automatically recovered.	3.7(1d) and 3.7(1g)
CSCwb33105	Data fetched from APIC may not match the schema config even though the APIC configuration is identical to NDO schema One of the following four different symptoms can be seen in Reconcile Drift UI: 1. APIC configuration may show a linked reference pointing to an object with the same name but in a different schema/template 2. APIC configuration may not show empty ANP 3. APIC configuration may show svcRuleType as " EPG" even though it should be “VRF” 4. APIC configuration shows VzAnyEnabled but no vzAny contracts	3.7(1d) and 3.7(1g)
CSCwb41977	Upon upgrade of the NDO services, the upgrade may complete successfully but some services may silently remain in a pending state. This will result in various API failures that can be seen in the UI and/or via API invocation from a customer's tooling. The user can detect the issue by looking at the service status summary that is available. Some of the services will be denoted as non-operational.	3.7(1d) and 3.7(1g)

© 2020 Cisco and/or its affiliates. All rights reserved.

Bug ID	Description	Exists in
CSCwb52863	The Application Profiles (ANPs) may get marked as drifted even though they exist on APIC	3.7(1d) and 3.7(1g)
CSCwb57049	NDO may show wrong serviceGraphContractRelationRef with different service graphs (SGs) mentioned in the same contract. However, serviceGraphContractRelationRef is updated properly, for example, it may show on the NDO side even though it is properly removed from the APIC as expected. This issue is not impacting the traffic on APIC.	3.7(1d) and 3.7(1g)
CSCwb65482	In Reconcile Config Drift workflow for APIC, the External EPG has L3Out reference with only the name and DN.	3.7(1d) and 3.7(1g)
CSCwb17102	Unable to manage a mini ACI fabric in NDO. Error "Unable to determine Site Type" is displayed when attempting to manage the site in the NDO service.	3.7(1d) and 3.7(1g)
CSCwb85199	CloudSec control policy is not created when enabling CloudSec for a site in NDO.	3.7(1d) and 3.7(1g)
CSCvw03174	If an admin user logs in and select an external EPG, they can't see it is associated to any L3Oout. However, if a read-only user logs in, they can see that EPG is associated with some L3Out.	3.7(1d) and 3.7(1g)
CSCwc43830	Duplicate External EPG shadows under different site-local L3Outs causing second update to be blocked and spine switch deleting the old entry.	3.7(1d)-3.7(1j)
CSCwc12353	NDFC throws an error stating that it is being managed with different cluster name.	3.7(1d)-3.7(1j)
CSCwc15163	UI shows an error message if orderID in route maps for multicast is greater than 31.	3.7(1d)-3.7(1j)
CSCwc41840	Unable to configure a scheduled backup on admin account in NDO but able to on other accounts.	3.7(1d)-3.7(1k)
CSCwc56401	Shadow BD's subnet for site local BDs get erroneously deleted from other APIC sites when a template associated to multiple sites is deployed	3.7(1d)-3.7(1k)
CSCvo84218	When service graphs or devices are created on Cloud APIC by using the API and custom names are specified for AbsTermNodeProv and AbsTermNodeCons, a brownfield import to the Nexus Dashboard Orchestrator will fail.	3.7(1d) and later
CSCvo20029	Contract is not created between shadow EPG and on-premises EPG when shared service is configured between Tenants.	3.7(1d) and later
CSCvn98355	Inter-site shared service between VRF instances across different tenants will not work, unless the tenant is stretched explicitly to the cloud site with the correct provider credentials. That is, there will be no implicit tenant stretch by Nexus Dashboard Orchestrator.	3.7(1d) and later
CSCvs99052	Deployment window may show more policies been modified than the actual config changed by the user in the Schema.	3.7(1d) and later

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description	Exists in
CSCvt06351	Deployment window may not show all the service graph related config values that have been modified.	3.7(1d) and later
CSCvt00663	Deployment window may not show all the cloud related config values that have been modified.	3.7(1d) and later
CSCvt41911	After brownfield import, the BD subnets are present in site local and not in the common template config	3.7(1d) and later
CSCvt44081	In shared services use case, if one VRF has preferred group enabled EPGs and another VRF has vzAny contracts, traffic drop is seen.	3.7(1d) and later
CSCvt02480	The REST API call " /api/v1/execute/schema/5e43523f1100007b012b0fcd/template/Template_11?undeploy=all" can fail if the template being deployed has a large object count	3.7(1d) and later
CSCvt15312	Shared service traffic drops from external EPG to EPG in case of EPG provider and L3Out vzAny consumer	3.7(1d) and later
CSCvw31631	When deploying fabric connectivity between on-premises and cloud sites, you may get a validation error stating that l3extSubnet/cloudTemplateBgpEvpn is already attached.	3.7(1d) and later
CSCvw10432	Two cloud sites (with Private IP for CSRs) with the same InfraVNETPool on both sites can be added to NDO without any infraVNETPool validation.	3.7(1d) and later
CSCvy31532	After a site is re-registered, NDO may have connectivity issues with APIC or CAPIC	3.7(1d) and later
CSCvy36810	Multiple Peering connections created for 2 set of cloud sites.	3.7(1d) and later
CSCvz08520	Missing BD1/VRF1 in site S2 will impact the forwarding from EPG1 in site S1 to EPG1/EPG2 in site S2	3.7(1d) and later
CSCvz07639	NSG rules on Cloud EPG are removed right after applying service graph between Cloud EPG and on-premises EPG, which breaks communication between Cloud and on-premises.	3.7(1d) and later
CSCvz77156	Route leak configuration for invalid Subnet may get accepted when Internal VRF is the hosted VRF. There would be fault raised in cAPIC.	3.7(1d) and later
CSCwa47934	Removing site connectivity or changing the protocol is not allowed between two sites.	3.7(1d) and later
CSCwa20994	When downloading external device configuration in Site Connectivity page, all config template files are included instead of only the External Device Config template.	3.7(1d) and later
CSCwa23744	Sometimes during deploy, you may see the following error: invalid configuration CT_IPSEC_TUNNEL_POOL_NAME_NOT_DEFINED	3.7(1d) and later
CSCwa40878	User can not withdraw the hubnetwork from a region if intersite connectivity is deployed.	3.7(1d) and later
CSCwa42346	You may see the following error on Infra template deployment Invalid Configuration CT_PROVIDER_MISMATCH.	3.7(1d) and later
CSCwa42423	Duplicate site entries are sent in the PUT request which is causing mongo DB error.	3.7(1d) and later

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description	Exists in
CSCvw10432	Two cloud sites (with Private IP for CSRs) with same InfraVNETPool on both sites get added to NDO without any infraVNETPool validation.	3.7(1d) and later
CSCwa17852	BGP sessions from Google Cloud site to AWS/Azure site may be down due to CSRs being configured with a wrong ASN number.	3.7(1d) and later
CSCwa26712	Existing IPSec tunnel state may be affected after update of connectivity configuration with external device.	3.7(1d) and later
CSCwa37204	Username and password is not set properly in proxy configuration so a component in the container cannot connect properly to any site. In addition, external module pyaci is not handling the web socket configuration properly when user and password are provided for proxy configuration.	3.7(1d) and later
CSCwb03980	For a BD in NDO schema, only the linked L3Out name is populated and the BD's L3Out Ref field remains empty even though the L3Out is managed by NDO. This can be observed in UI when BD L3Out is edited, it does not show the complete path for the existing L3Out in the drop-down list. It can also be observed in the Reconcile Drift UI where the BD's L3Out Ref is missing in the NDO schema tab and only the name is displayed.	3.7(1d) and later
CSCwd22543	The traffic between on-premises InstP and cloudEPGs is affected when a template containing a subnet of cloud EPGs with contract to on-premises InstP is undeployed.	3.7(1d) and later
CSCwe35911	Same EPG may be shown more than once in the drift reconciliation workflow.	3.7(1d) and later
CSCwe27875	When BD DHCP labels with "infra" scope/owner are imported/reconciled into NDO, they will get deployed back to APIC with scope "tenant".	3.7(1d) and later
CSCwe26871	False configuration drift on subnet names and order.	3.7(1d) and later

Resolved Issues

This section lists the resolved issues. Click the bug ID to access the Bug Search tool and see additional information about the issue. The "Fixed In" column of the table specifies whether the bug was resolved in the base release or a patch release.

Bug ID	Description	Fixed in
CSCwa22530	If you have BGP-IPv4 connectivity across the sites and BGP password is different across sites, it should not form BGP sessions. Also, BGP configurationss related to password are not pushed to CSRs on Azure and AWS.	3.7(1d)
CSCwa54416	UI shows "standby service instances" status down	3.7(1d)
CSCvt11713	Intersite L3Out traffic is impacted because of missing import RT for VPN routes	3.7(1d)* *The site must be running Release 5.2(4) or later

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description	Fixed in
CSCwb26063	The on-premises site lose connectivity and NDO is not able to communicate with those sites. The Cloud APIC sites that are connected via proxy continue to operate.	3.7(1g)
CSCwb26058	When usage of proxy is enabled for a site on ND, NDO/MSO does not use the proxy information when contacting sites.	3.7(1g)
CSCwb10342	Audit Log streaming may not work.	3.7(1j)
CSCwb32631	CloudSec key sequence is transiently out of order and can cause brief disruption of traffic on the affected link, but will should be automatically recovered.	3.7(1j)
CSCwb33105	Data fetched from APIC may not match the schema config even though the APIC configuration is identical to NDO schema One of the following four different symptoms can be seen in Reconcile Drift UI: 1. APIC configuration may show a linked reference pointing to an object with the same name but in a different schema/template 2. APIC configuration may not show empty ANP 3. APIC configuration may show svcRuleType as " EPG" even though it should be “VRF” 4. APIC configuration shows VzAnyEnabled but no vzAny contracts	3.7(1j)
CSCwb41977	Upon upgrade of the NDO services, the upgrade may complete successfully but some services may silently remain in a pending state. This will result in various API failures that can be seen in the UI and/or via API invocation from a customer's tooling. The user can detect the issue by looking at the service status summary that is available. Some of the services will be denoted as non-operational.	3.7(1j)
CSCwb52863	The Application Profiles (ANPs) may get marked as drifted even though they exist on APIC	3.7(1j)
CSCwb57049	NDO may show wrong serviceGraphContractRelationRef with different service graphs (SGs) mentioned in the same contract. However, serviceGraphContractRelationRef is updated properly, for example, it may show on the NDO side even though it is properly removed from the APIC as expected. This issue is not impacting the traffic on APIC.	3.7(1j)
CSCwb65482	In Reconcile Config Drift workflow for APIC, the External EPG has L3Out reference with only the name and DN.	3.7(1j)
CSCwb17102	Unable to manage a mini ACI fabric in NDO. Error " Unable to determine Site Type" is displayed when attempting to manage the site in the NDO service.	3.7(1j)
CSCwb85199	CloudSec control policy is not created when enabling CloudSec for a site in NDO.	3.7(1j)
CSCvw03174	If an admin user logs in and select an external EPG, they can't see it is associated to any L3Oout. However, if a read-only user logs in, they can see that EPG is associated with some L3Out.	3.7(1j)

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description	Fixed in
CSCwc43830	Duplicate External EPG shadows under different site-local L3Outs causing second update to be blocked and spine switch deleting the old entry.	3.7(1k)
CSCwc12353	NDFC throws an error stating that it is being managed with different cluster name.	3.7(1k)
CSCwc15163	UI shows an error message if orderID in route maps for multicast is greater than 31.	3.7(1k)
CSCwc41840	Unable to configure a scheduled backup on admin account in NDO but able to on other accounts.	3.7(1l)
CSCwc56401	Shadow BD's subnet for site local BDs get erroneously deleted from other APIC sites when a template associated to multiple sites is deployed	3.7(1l)

Known Issues

This section lists known behaviors. Click the Bug ID to access the Bug Search Tool and see additional information about the issue.

Bug ID	Description
CSCvy67993	NDO will not update or delete VRF vzAny configuration which was directly created on APIC even though the VRF is managed by NDO.
CSCvo82001	Unable to download Nexus Dashboard Orchestrator report and debug logs when database and server logs are selected
CSCvo32313	Unicast traffic flow between Remote Leaf Site1 and Remote Leaf in Site2 may be enabled by default. This feature is not officially supported in this release.
CSCvn38255	After downgrading from 2.1(1), preferred group traffic continues to work. You must disable the preferred group feature before downgrading to an earlier release.
CSCvn90706	No validation is available for shared services scenarios
CSCvo59133	The upstream server may time out when enabling audit log streaming

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCvd59276	For Cisco Multi-Site, Fabric IDs Must be the Same for All Sites, or the Querier IP address Must be Higher on One Site. The Cisco APIC fabric querier functions have a distributed architecture, where each leaf switch acts as a querier, and packets are flooded. A copy is also replicated to the fabric port. There is an Access Control List (ACL) configured on each TOR to drop this query packet coming from the fabric port. If the source MAC address is the fabric MAC address, unique per fabric, then the MAC address is derived from the fabric-id. The fabric ID is configured by users during initial bring up of a pod site. In the Cisco Multi-Site Stretched BD with Layer 2 Broadcast Extension use case, the query packets from each TOR get to the other sites and should be dropped. If the fabric-id is configured differently on the sites, it is not possible to drop them. To avoid this, configure the fabric IDs the same on each site, or the querier IP address on one of the sites should be higher than on the other sites.
CSCvd61787	STP and " Flood in Encapsulation" Option are not Supported with Cisco Multi-Site. In Cisco Multi-Site topologies, regardless of whether EPGs are stretched between sites or localized, STP packets do not reach remote sites. Similarly, the " Flood in Encapsulation" option is not supported across sites. In both cases, packets are encapsulated using an FD VNID (fab-encap) of the access VLAN on the ingress TOR. It is a known issue that there is no capability to translate these IDs on the remote sites.
CSCvi61260	If an infra L3Out that is being managed by Cisco Multi-Site is modified locally in a Cisco APIC, Cisco Multi-Site might delete the objects not managed by Cisco Multi-Site in an L3Out.
CSCvq07769	" Phone Number" field is required in all releases prior to Release 2.2(1). Users with no phone number specified in Release 2.2(1) or later will not be able to log in to the GUI when Orchestrator is downgraded to an earlier release.
CSCvu71584	Routes are not programmed on CSR and the contract config is not pushed to the Cloud site.
CSCvw47022	Shadow of cloud VRF may be unexpectedly created or deleted on the on-premises site.
CSCvt47568	Let's say APIC has EPGs with some contract relationships. If this EPG and the relationships are imported into NDO and then the relationship was removed and deployed to APIC, NDO doesn't delete the contract relationship on the APIC.
CSCwa31774	When creating VRFs in infra tenant on a Google Cloud site, you may see them classified as internal VRF in NDO. If you then import these VRFs in NDO, the allowed routeleak configuration will be determined based on whether the VRF is used for external connectivity (external VRF) or not (internal VRF). This is because on cAPIC, VRFs in infra tenant can fall into 3 categories: internal, external and un-decided. NDO treats infra tenant VRFs as 2 categories for simplicity: internal and external. There is no usecase impacted because of this.
CSCwc52360	When using APIs, template names must not include spaces.

© 2020 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Bug ID	Description
CSCwa87027	After unmanaging an external fabric that contains route-servers, Infra Connectivity page in NDO still shows the route-servers. Since the route-servers are still maintained, the overlay IFC from the route-servers to any BGW devices in the DCNM are not removed.

Compatibility

This release supports the hardware listed in the “Prerequisites” section of the Cisco Nexus Dashboard Orchestrator Deployment Guide.

This release supports Nexus Dashboard Orchestrator deployments in Cisco Nexus Dashboard only.

Cisco Nexus Dashboard Orchestrator can be cohosted with other services in the same cluster. For cluster sizing guidelines and services compatibility information see the Nexus Dashboard Cluster Sizing tool and Nexus Dashboard and Services Compatibility Matrix.

When managing Cloud APIC sites, this Nexus Dashboard Orchestrator release supports Cisco Cloud APIC, Release 5.2(1) or later only.

When managing on-premises fabrics, this Nexus Dashboard Orchestrator release supports any on-premises Cisco APIC release that can be on-boarded to the Nexus Dashboard. For more information, see the Interoperability Support section in the “Infrastructure Management” chapter of the Cisco Nexus Dashboard Orchestrator Deployment Guide.

Scalability

For Nexus Dashboard Orchestrator verified scalability limits, see Cisco Nexus Dashboard Orchestrator Verified Scalability Guide.

For Cisco ACI fabrics verified scalability limits, see Cisco ACI Verified Scalability Guides.

For Cisco NDFC (DCNM) fabrics verified scalability limits, see Cisco NDFC (DCNM) Verified Scalability Guides.

Related Content

For NDFC (DCNM) fabrics, see the Cisco Nexus Dashboard Fabric Controller documentation page.

For ACI fabrics, see the Cisco Application Policy Infrastructure Controller (APIC) documentation page. On that page, you can use the " Choose a topic" and " Choose a document type” fields to narrow down the displayed documentation list and find a specific document.

The following table describes the core Nexus Dashboard Orchestrator documentation.

Document	Description
Cisco Nexus Dashboard Orchestrator Release Notes	Provides release information for the Cisco Nexus Dashboard Orchestrator product.
Cisco Nexus Dashboard Orchestrator Deployment Guide	Describes how to install Cisco Nexus Dashboard Orchestrator and perform day-0 operations.

© 2020 Cisco and/or its affiliates. All rights reserved.

Document	Description
Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics	Describes Cisco Nexus Dashboard Orchestrator configuration options and procedures for fabrics managed by Cisco APIC.
Cisco Nexus Dashboard Orchestrator Configuration Guide for NDFC (DCNM) Fabrics	Describes Cisco Nexus Dashboard Orchestrator configuration options and procedures for fabrics managed by Cisco DCNM.
Cisco Nexus Dashboard Orchestrator Verified Scalability Guide	Contains the maximum verified scalability limits for this release of Cisco Nexus Dashboard Orchestrator.
Cisco ACI Verified Scalability Guides	Contains the maximum verified scalability limits for Cisco ACI fabrics.
Cisco NDFC (DCNM) Verified Scalability Guides	Contains the maximum verified scalability limits for Cisco NDFC (DCNM) fabrics.
Cisco ACI YouTube channel	Contains videos that demonstrate how to perform specific tasks in the Cisco Nexus Dashboard Orchestrator.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, send your comments to mailto:apic-docfeedback@cisco.com. We appreciate your feedback.

Legal Information

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2022 Cisco Systems, Inc. All rights reserved.