

BPA - Versionshinweise v5.1

- [Einleitung](#)
- [Neuerungen](#)
 - [Kernplattform](#)
 - [BPA-Komponenten](#)
 - [Compliance und Problembehebung](#)
 - [Neuzertifizierung für NDFC v12.2.2](#)
 - [Unterstützung für vManage Controller v20.15 und RBAC](#)
 - [vManagement des Sitzungsmanagements](#)
 - [Migration der klassischen GCT-Anwendung auf die Anwendung der nächsten Generation](#)
 - [Liste der Funktionen für Betriebssystem-Upgrades](#)
 - [Außerbetriebnahme von SASE, Perimeter-Security und TMF](#)
- [Gelöste Probleme](#)
- [Bekannte Probleme](#)

Einleitung

Business Process Automation (BPA) ist eine domänenübergreifende, mehrschichtige Automatisierungs- und Orchestrierungslösung, die den Lebenszyklus von Netzwerkressourcen über verschiedene Netzwerkarchitekturen wie Transport, Rechenzentrum, Campus, Software-Defined Wide Area Network (SD-WAN) und Sicherheit verwaltet. Zu den Vorteilen zählen die Verkürzung der Bereitstellungszeit für neue Services, die Minimierung von Kapital- und Betriebskosten, eine verbesserte Verfügbarkeit, Kapazität und Betriebszuverlässigkeit durch eine konsistente und automatisierte Netzwerkkonfiguration sowie Skalierbarkeit.


BPA bietet folgende Funktionen:

- Eine Automatisierungslösung zur Verwaltung des Lebenszyklus von Geräten von Cisco und Drittanbietern, mit Anwendungsfällen wie Geräteintegration, Vorlagenmanagement, Softwarekonformität, Upgrades und Konfigurationskonformität
- Workflow-Engine für die End-to-End-Service-Integration und Automatisierung von Geschäfts- und Betriebsprozessen
- Prozessvorlagen zur Automatisierung von Prozeduren, Marktvarianzen zur Verwaltung von Standortdaten und Formular-Designer zum Erstellen von Benutzeroberflächenformularen
- Adapter-Framework für die Ost-West-Integration in Operations Support Systems und Business Support Systems

BPA ist in die unten aufgeführten Controller von Cisco und anderen Anbietern integriert. Aufgrund der modularen Architektur von BPA können Integrationen jedoch auch auf andere Controller von


Cisco oder Drittanbietern erweitert werden.

- Cisco Controller
 - Network Services Orchestrator (NSO)
 - Cisco Catalyst Center (ehemals Cisco Digital Network Architecture Center)
 - Data Center Network Manager (DCNM)
 - Cisco Catalyst SD-WAN Manager (ehemals Cisco vManage)
 - Direct-to-Device
 - Cisco Nexus Dashboard Fabric Controller (NDFC)
 - Cisco Crosswork Network Controller (CNC)
 - Cisco Secure Firewall Management Center (FMC)
- Controller anderer Anbieter
 - Ansible

 Anmerkung: Für BPA ist die Verwendung eines Abonnementschlüssels erforderlich, um sicherzustellen, dass BPA-Bereitstellungen für erforderliche Support- und Wartungsservices qualifiziert sind. Um einen Abonnementschlüssel zu erwerben, wenden Sie sich an einen Ansprechpartner bei Cisco, oder senden Sie eine E-Mail an bpa-subscriptions@cisco.com.

Neuerungen

In diesem Abschnitt werden die wichtigsten Funktionen, Verbesserungen und Änderungen der Cisco BPA 5.1-Version vorgestellt.

 Anmerkung: BPA v5.1 wurde mit der neuesten Version von Google Chrome (v139.0.7258.140) und Mozilla Firefox (v142) validiert.

Kernplattform

Zu den Aktualisierungen der Kernplattform gehören:

- Möglichkeit zum Exportieren oder Importieren benutzerdefinierter Rollen oder Berechtigungen
- Unterstützung für Agentenabonnements (alle Agenten verfügen jetzt über Codes und können abonniert werden)
- Hohe Verfügbarkeit für Container mit Open Policy Agent aktiviert
- Unterstützung für die Steuerung des Wechsels zwischen der klassischen und der Portal-Benutzeroberfläche
- Unterstützung für Änderungen von Laufzeitformularen zur einfachen Navigation in der Formularhierarchie

- Unterstützung für vNSO 6.5
- Hinzufügen von Entscheidungsmodell und Notation-UI und UX zur Workflow-Anwendung
- Möglichkeit, die Ablaufverfolgung zu aktivieren oder zu deaktivieren und Ablaufverfolgungen von REST-Anrufen, MongoDB- und Postgres-Datenbankabfragen anzuzeigen (ausgenommen Policy Resolver und NSO)

BPA-Komponenten

Komponentenname	Komponentenversion
Knoten	v22.16.0
Postgres	v17.5.1
Zookeeper	V3.9.3
Patroni	V4.0.6
Camunda	v7.19 (Java 11)
Kafka	Version 4.0.0
MongoDB	v8.0.10
Hongkong	V3.9.0
Elk	v9.0.3
Filebeat	v9.0.3

Compliance und Problembehebung

Aktualisierungen der Konfigurationskonformität und -behebung umfassen:

- Umfassendes Reporting-Dashboard zum Erstellen, Anzeigen und Herunterladen von Compliance-Berichten
- Offline-Konformitätsprüfungen, mit denen Benutzer Gerätekonfigurationen hochladen können, ohne sie in den Asset Manager einbinden zu müssen
- Konfigurierbare Muster in der Blockkonfiguration, um vertrauliche Gerätekonfigurationsdaten zu maskieren
- Möglichkeit zum Exportieren von zusammengefassten Daten zum Richtlinien- und Asset-Compliance-Raster als CSV-Dateien
- Möglichkeit zum Anzeigen und Vergleichen einer generierten Problembehebungskonfiguration mit der aktuellen Konfiguration eines Geräts
- Blockierung von Verbesserungen zur Unterstützung von Verletzungen bei vorhandenen Konfigurationen

Neuzertifizierung für NDFC v12.2.2

Im Rahmen der Neuzertifizierung wurden die folgenden Anwendungen mit dem NDFC-Controller v12.2.2 getestet:

- Kernanwendungen (z. B. Asset Manager, Golden Configuration Template (GCT) und Process Template)
- Geräteaktivierung
- Betriebssystem-Upgrade


Unterstützung für vManage Controller v20.15 und RBAC

Updates für vManage Controller v20.15 und rollenbasierte Zugriffskontrolle (RBAC) umfassen:

- Unterstützung für vManager-Controller v20.15
- RBAC verwendet Bereiche, um nicht administrativen Benutzern Zugriff auf Vorlagen zu gewähren.
- RBAC ermöglicht den Gerätezugriff über Ressourcengruppen
- Die Zugriffsrichtlinie in BPA gewährt nicht administrativen Benutzern Zugriff auf Geräte und Vorlagen.

vManagement des Sitzungsmanagements

Das Sitzungsmanagement wird nun von allen vManage-Controller-Versionen unterstützt. Für jede Anforderung wird eine vorhandene gültige Sitzung verwendet, um eingehende API-Aufrufe auszuführen, anstatt jedes Mal eine neue Sitzung zu erstellen. Wenn die Sitzung abgelaufen ist, wird automatisch eine neue Sitzung erstellt.

 Anmerkung: Das standardmäßige Timeout bei Inaktivität beträgt 30 Minuten, und das Token läuft nach 24 Stunden ab.

Migration der klassischen GCT-Anwendung auf die Anwendung der nächsten Generation

Die klassische GCT-Anwendung wurde auf die GCT-Benutzeroberfläche der nächsten Generation migriert. Die neue Benutzeroberfläche und UX sind auf andere Anwendungen wie Asset Manager abgestimmt, und alle klassischen GCT-Funktionen sind weiterhin verfügbar. Zu den Highlights gehören:

- Verbesserte UI- und API-Leistung
- Einführung des Konzepts der Zuweisungsvariablen beim Erstellen der Vorlage, sodass Bereitstellungsjobs Variablen mit Werten vorfüllen können
- Eine Seite für dedizierte Bereitstellungsaufträge

Liste der Funktionen für Betriebssystem-Upgrades

Zu den Updates für das Betriebssystem-Upgrade gehören:

- Zertifizierung für NDFC-Controller v12.2.2
- Unterstützung für EPLD-Upgrades (Erasable Programmable Logic Device) für Nexus-Switches, die von NDFC-Controllern verwaltet werden. So können Benutzer Konformitätsrichtlinien für EPLD-Pakete definieren, Konformitätsprüfungen durchführen und Ergebnisse anzeigen, die mit Software Maintenance Upgrade vergleichbar sind
- Die Möglichkeit, Software-Upgrades für den gesamten Job, einen bestimmten Batch oder ein oder mehrere Geräte in einem Batch abzubrechen
- Unterstützung von Hinweisen, Bugs und End-of-Life-Details für den Softwaretyp "Internetwork Operating System eXtended Routing"
- Das folgende Framework verbessert die Benutzerfreundlichkeit und das allgemeine Benutzererlebnis:
 - Möglichkeit zum Löschen von Software-Images (im Workflow aktiviert oder deaktiviert) vor der Verteilung und nach der Aktivierung für vom vManager-Controller verwaltete Geräte
 - Automatische Aktualisierung für die Dashboard-Seite für die Softwarekonformität mit Echtzeitaktualisierungen während aktiver Konformitätsrichtlinien
 - Unterstützung von absoluten und relativen Image-Namen in Software-Image-Metadaten für die Flexibilität von Images, die in unterschiedlichen Pfaden auf dem File Transfer Protocol-Server gespeichert sind
 - Software-Konformitätsrichtlinien akzeptieren die für einen Benutzer zulässigen Asset-Gruppen (anstelle von Controller-IDs), wodurch eine größere Genauigkeit ermöglicht wird.

Außerbetriebnahme von SASE, Perimeter-Security und TMF

Die folgenden Anwendungsfälle für BPA 5.1 werden eingestellt und nicht mehr unterstützt:

- Secure Access Service Edge (SASE): Alle SASE-bezogenen Controller, einschließlich Umbrella, Duo und ThousandEyes, und die entsprechenden Anwendungsfälle
- Perimeter-Sicherheit: Alle Anwendungsfälle für die Perimetersicherheit, die Cisco und andere Controller unterstützen
- Übersetzungsmodell-Framework (TMF): TMF Connector-Services und alle TMF 641 Service-Auftragsverwaltungsartefakte

Gelöste Probleme

Es gibt keine behobenen Probleme, die im Rahmen dieser Version gemeldet werden müssen.

Bekannte Probleme

Es sind keine Probleme bekannt, die im Rahmen dieser Version gemeldet werden müssen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.