

Correctif des notes de version du BPA v4.1.2

Introduction

Business Process Automation (BPA) est une solution d'automatisation et d'orchestration multiniveau interdomaine qui gère le cycle de vie des ressources réseau sur diverses architectures réseau telles que le transport, le data center, le campus, le SD-WAN et la sécurité.

Le BPA offre les fonctionnalités suivantes :

- Une solution d'automatisation pour la gestion du cycle de vie des périphériques Cisco et tiers, avec des exemples d'utilisation tels que l'intégration des périphériques, la gestion des modèles, la conformité des logiciels, les mises à niveau et la conformité de la configuration
- Moteur de workflow pour l'intégration de services de bout en bout et l'automatisation des processus métier et opérationnels
- Modèles de processus pour l'automatisation des procédures, écarts de marché pour la mise à jour des données d'emplacement et concepteurs de formulaires pour la création de formulaires d'interface utilisateur
- Structure d'adaptation pour la construction d'une intégration Est-Ouest aux systèmes de support d'exploitation et aux systèmes de support d'entreprise

Le BPA est intégré aux contrôleurs Cisco et non Cisco :

- Contrôleurs Cisco
 - Network Services Orchestrator (NSO)
 - Cisco Catalyst Center
 - Data Center Network Manager (DCNM)
 - Cisco Catalyst SD-WAN Manager (anciennement Cisco vManage)
 - Umbrella
 - Duo
 - ThousandEyes
 - Contrôleur de fabric de tableau de bord Cisco Nexus (NDFC)
 - Contrôleur réseau Cisco Crosswork (CNC)
 - Cisco Secure Firewall Management Center (FMC)
- Contrôleurs non Cisco
 - Direct vers le périphérique
 - Ansible
 - Gestionnaire de points de contrôle/Smart Console

Grâce à l'architecture modulaire du BPA, les intégrations peuvent être étendues à d'autres

contrôleurs Cisco ou tiers. Le BPA offre des avantages tels que la réduction des délais de fourniture de nouveaux services, la réduction des coûts d'investissement et d'exploitation, l'amélioration de la disponibilité, de la capacité et de la fiabilité opérationnelle grâce à une configuration et une évolutivité du réseau cohérentes et automatisées.

Mise à niveau vers BPA v4.1.2 Patch 7

Pour effectuer une mise à niveau vers BPA v4.1.2 Patch 7 :

En raison de problèmes de vulnérabilité, l'image MongoDB a été mise à niveau. Comme mongo-init est un travail et que la mise à niveau helm n'est pas prise en charge, le pod mongo-init doit être supprimé avant la mise à niveau du patch.

1. Supprimez le pod mongo-init à l'aide des commandes suivantes.

```
kubectl get pod -n bpa-ns -o wide | grep mongo-init  
kubectl delete pod
```

```
-n bpa-ns
```

2. Après la suppression de mongo-init, référez-vous à la section Mise à niveau de correctif du [Guide d'installation de BPA](#) pour plus d'informations sur les mises à jour de correctifs.

Nouveautés de Cisco

Cette section présente les principales fonctionnalités, améliorations et modifications introduites dans la version Cisco BPA v4.1.2.

Mise à niveau OS

Les améliorations apportées à la mise à niveau du système d'exploitation sont les suivantes :

- La mise à niveau en plusieurs étapes inclut désormais la prise en charge des mises à jour de maintenance logicielle Bridge (SMU) en tant que chemin distinct dans le processus de mise à niveau
- Les utilisateurs peuvent désormais consulter les règles et les résultats d'évaluation, ainsi

que les résultats des commandes des modèles de pré-vérification et de post-vérification dans le résumé du travail de mise à niveau et le rapport PDF de mise à niveau

- La prise en charge de la mise à niveau logicielle est étendue pour le contrôleur vManage v20.12.4

SD-WAN

La prise en charge du contrôleur vManage v20.12.4 a été ajoutée.

Contrôleurs et versions pris en charge

Types de contrôleurs	Versions prises en charge
NSO	5.5, 5.6, 5.7, 5.8, 6.0, 6.1, 6.2, 6.3
Cisco Catalyst Center	1.3.3, 2.1.2, 2.2.2, 2.2.32.3.3, 2.3.4, 2.3.5
DCNM	11.5
vManage	20.6.3, 20.9.3, 20.9.5, 20.12.4
CNC	4.1, 5.0, 6.0
NDFC	3.0.1(i) Fabric v12.1.2e, 3.0.1(i) Fabric v12.1.3b
FMC	7.2.5
Direct vers le périphérique	Les types de système d'exploitation suivants sont pris en charge : cisco-ios, cisco-iosxr, cisco-asa, arista-eos, juniper-junos
CheckpointFortinet	R77.30, R80.20 Fortigate 3700D - 5.2.4, 6.0.5
Umbrella	Umbrella SIG Advantage + Multi-Org + RBI L3
DUO	D299,18
ThousandEyes	Sans objet

Divers

BPA v4.1.2 a été validé avec la dernière version des navigateurs Google Chrome (v126.0.6478.183) et Mozilla Firefox (v128) au moment de la publication.

Problèmes résolus

ID de suivi des défauts	Description
DAA-91480	Le problème du processus de purge ne fonctionnant que pour les Workflows et non pour les autres applications a été résolu par la mise à jour des conditions pour renvoyer une réponse appropriée.
DAA-90990	Les problèmes de vulnérabilité précédents en mongol ont été résolus en mettant à niveau le shell Mongo de v506 à v507.
DAA-90878	Les erreurs se produisant lors de la suppression d'une clé API en sélectionnant l'icône Delete ont été résolues en incluant une clé dans la charge utile.
DAA-90018	Auparavant, le paramètre de requête de l'adaptateur BPA n'était pas en mesure d'enregistrer le nom du champ clé. Ce problème a été résolu en mettant à jour la fonctionnalité pour autoriser le nom du champ de clé dans les paramètres de requête.
DAA-89862	Auparavant, le processus de chargement échouait lorsque les administrateurs cliquaient sur Afficher et demander une tâche. Ce problème a été résolu en corrigeant un bogue dans la charge utile UserTask.
DAA-89754,	Les utilisateurs ont déjà reçu une invite d'expiration de session alors qu'ils étaient actifs, ce qui a entraîné des déconnexions inattendues même après avoir cliqué sur Continuer.
DAA-89613,	Ce problème a été résolu en corrigeant les erreurs de calcul dans les cases d'angle et en s'assurant que le jeton n'est actualisé qu'après le délai d'expiration.
DAA-84854	Remarque : Pour résoudre ce problème dans les microservices personnalisés, le <code>jwt_token</code> doit être utilisé à partir de <code>sessionStorage</code> au lieu de <code>localStorage</code> .
DAA-89584	Auparavant, lors de la distribution du modèle de la version principale de vManage vers d'autres instances de vManage, une balise GR1(Group) dupliquée était ajoutée lorsqu'une balise GR était déjà présente dans le nom du modèle. Ce problème a été résolu en incrémentant la même balise GR au numéro suivant au lieu d'ajouter une nouvelle balise GR.
DAA-88969	Dans les versions précédentes de BPA, la logique de nouvelle tentative du workflow de mise à niveau du système d'exploitation n'a pas pu mettre à jour la version par défaut dans vManage et marquer la commande comme terminée. Ce problème a été résolu en mettant à jour la variable de version par défaut lorsque le problème de jeton de falsification de requête intersite est observé.
DAA-88778	Auparavant, lorsque les utilisateurs tentaient de se connecter et de se déconnecter de BPA, ils étaient redirigés vers des URL incorrectes. Ce problème a été corrigé en passant correctement l'indicateur d'administration lorsque la source correspond et en assurant l'unicité du groupe de gestion.
DAA-87879	Auparavant, les utilisateurs rencontraient des problèmes d'accessibilité sporadiques lorsqu'ils utilisaient des URL référencées sans se connecter. Ce problème a été résolu en ajoutant une logique pour actualiser la page de connexion afin d'éviter une redirection non valide.
DAA-87822	Précédemment, la page Commandes du catalogue de services de nouvelle génération affichait un décalage lorsque les commandes contenaient plus de données dans la section jalons. Ce problème a été résolu en excluant les champs qui ne sont pas nécessaires dans la page Grille de commandes et en rendant un appel d'API disponible

ID de suivi des défauts	Description
	lorsqu'un élément de catalogue est sélectionné.
DAA-87532	Auparavant, les utilisateurs ne pouvaient pas récupérer des fichiers journaux volumineux avec la commande <code>kubect1</code> . Ce problème a été résolu en activant les journaux en conteneur.
DAA-85007	Auparavant, lorsque des travaux inachevés étaient annulés manuellement au niveau de l'application, une annulation forcée se produisait, laissant l'état de la commande inchangé et ne parvenant pas à restaurer ou supprimer les périphériques du distributeur associés. Ce problème a été résolu par l'introduction d'une tâche de gestion des erreurs.
DAA-85003	Auparavant, BPA n'avait pas détecté un format CSV incorrect, y compris des colonnes qui ont été fusionnées de manière incorrecte, ce qui a entraîné une erreur de lecture de l'indicateur d'activation comme faux. Ce problème a été résolu en validant le format CSV lors du téléchargement et de l'affichage des messages d'erreur afin d'empêcher les états de tâches inactives.
DAA-84222	Auparavant, la méthode de chiffrement du script de gestion des informations d'identification était déconseillée. Ce problème a été résolu en ajoutant la nouvelle méthode de chiffrement pour éviter les problèmes de sécurité.
DAA-83034	Auparavant, les profils utilisateur n'étaient pas créés dans le portail BPA en raison d'une adresse e-mail vide du profil système de contrôle d'accès du contrôleur d'accès aux terminaux. Ce problème a été résolu en créant des ID d'e-mail factices si aucun e-mail n'est disponible dans la réponse. En outre, la validation des modèles d'e-mail a été mise à jour dans l'interface utilisateur et l'API.
DAA-82449	Auparavant, les utilisateurs configuraient les périphériques sans vérifier que le nouveau périphérique était en mode contrôleur, ce qui pouvait entraîner des configurations incorrectes. Ce problème a été résolu par l'introduction d'un message d'alerte.
DAA-80340	Le BPA a précédemment rencontré des problèmes de configuration OAuth. Ces problèmes ont été résolus en fournissant des mises à jour de plug-in, une reconfiguration du fichier « config.json » et une coordination avec les équipes de gestion des comptes clients et des produits.
DAA-92291	Auparavant, le problème de clé Secure Shell dans le rapport du contrôleur de cas ne générait pas de message d'erreur. Cette erreur a été résolue en affichant l'état d'exécution « Failed » avec le raisonnement correspondant.
DAA-84221	Auparavant, lors de l'installation du BPA, l'implémentation du protocole d'accès à l'annuaire léger du service d'authentification importait une bibliothèque obsolète présentant un risque de sécurité. Ce problème a été résolu en remplaçant « passeport-ldapauth » par « passeport-custom and ldaps package ». Remarque : Dans le fichier ldap auth config.json, « old entry searchBase-> »searchBase» : « ou=Cisco Users, dc=cisco, dc=com » a été remplacé par « new searchBase -> »searchBase » : « ou=Employés,ou=Utilisateurs Cisco,dc=cisco,dc=com ».

Problèmes identifiés

Il n'existe aucun problème connu à signaler dans cette version.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.