

parche de Notas de la versión de BPA v4.1.2

Introducción

La automatización de procesos empresariales (BPA) es una solución de automatización y orquestación de varios niveles entre dominios que gestiona el ciclo de vida de los recursos de red en diversas arquitecturas de red, como transporte, Data Center, campus, SD-WAN y seguridad.

BPA ofrece las siguientes funciones:

- Una solución de automatización para gestionar el ciclo de vida de los dispositivos de Cisco y de terceros, con casos prácticos como la incorporación de dispositivos, la gestión de plantillas, la conformidad del software, las actualizaciones y el cumplimiento de la configuración
- Un motor de flujo de trabajo para la integración de servicios integrales y la automatización de procesos operativos y empresariales
- Plantillas de procesos para automatizar procedimientos, Variaciones de mercado para mantener datos de ubicación y Diseñadores de formularios para crear formularios de interfaz de usuario (IU)
- Un marco de adaptador para la integración horizontal con sistemas de soporte de operaciones y sistemas de soporte de negocios

BPA se integra con controladores de Cisco y de terceros:

- Controladores de Cisco
 - Orquestador de servicios de red (NSO)
 - Cisco Catalyst Center
 - Data Center Network Manager (DCNM)
 - Cisco Catalyst SD-WAN Manager (anteriormente Cisco vManage)
 - Umbrella
 - Duo
 - ThousandEyes
 - Controlador de fabric de panel Cisco Nexus (NDFC)
 - Controlador de red Cisco Crosswork (CNC)
 - Cisco Secure Firewall Management Center (FMC)
- Controladores que no son de Cisco
 - Directo al dispositivo
 - Ansible
 - Checkpoint Manager/Smart Console

Con la arquitectura modular de BPA, las integraciones se pueden ampliar a otros controladores de Cisco o de terceros. BPA ofrece ventajas como la reducción del tiempo necesario para prestar nuevos servicios, la reducción de los costes operativos y de capital, la mejora de la disponibilidad, la capacidad y la fiabilidad operativa mediante una configuración de red coherente y automatizada, y la escalabilidad.

Actualización a BPA v4.1.2, parche 7

Para actualizar a BPA v4.1.2, parche 7:

Debido a problemas de vulnerabilidad, la imagen MongoDB se ha actualizado. Debido a que mongo-init es un trabajo y no se soporta la actualización del timón, el grupo de dispositivos mongo-init debe ser eliminado antes de la actualización del parche.

1. Elimine el grupo de dispositivos mongo-init con los siguientes comandos.

```
kubect1 get pod -n bpa-ns -o wide | grep mongo-init  
kubect1 delete pod
```

```
-n bpa-ns
```

2. Después de eliminar mongo-init, consulte la sección Actualización de Parches de la [Guía de Instalación de BPA](#) para obtener más información sobre las actualizaciones de parches.

Qué hay de nuevo

En esta sección se destacan las principales funciones, mejoras y modificaciones introducidas en la versión Cisco BPA v4.1.2.

Actualización de SO

Las mejoras de actualización del sistema operativo (SO) incluyen lo siguiente:

- La actualización en varios pasos ahora incluye compatibilidad con las actualizaciones de mantenimiento de software (SMU) de Bridge como ruta independiente en el proceso de actualización

- Ahora los usuarios pueden ver las reglas y los resultados de la evaluación, junto con la salida del comando de las plantillas anteriores y posteriores a la comprobación en el resumen del trabajo de actualización y el informe PDF de actualización
- Ampliación de la compatibilidad con actualizaciones de software para el controlador vManage v20.12.4

SD-WAN

Se ha agregado compatibilidad con el controlador v20.12.4 de vManage.

Controladores y versiones compatibles

Tipos de controlador	Versiones admitidas
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, 2.2.3.3, 2.3.4, 2.3.5
DCNM	11.5
vManage	20.6.3, 20.9.3, 20.9.5 y 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
Directo Al Dispositivo	Se admiten los siguientes tipos de SO: cisco-ios, cisco-iosxr, cisco-asa, arista-eos y juniper-junos
PuntoDeControlFortinet	R77.30, R80.20 Fortigate 3700D - 5.2.4, 6.0.5
Umbrella	Umbrella SIG Advantage + Multi-Org + RBI L3
DUO	D299.18
ThousandEyes	No aplicable

Miscelánea

BPA v4.1.2 se ha validado con la última versión de los navegadores Google Chrome (v126.0.6478.183) y Mozilla Firefox (v128) en el momento del lanzamiento.

Problemas resueltos

ID de seguimiento de defectos	Descripción
DAA-91480	El problema de que el proceso de depuración sólo funciona para flujos de trabajo y no para otras aplicaciones se ha resuelto mediante la actualización de las condiciones para devolver una respuesta adecuada.
DAA-90990	Los problemas de vulnerabilidad anteriores en mongol se han resuelto actualizando el shell de Mongo de v506 a v507.
DAA-90878	Los errores que se producen al eliminar una clave de API al seleccionar el icono Eliminar se han resuelto incluyendo una clave en la carga.
DAA-90018	Anteriormente, el parámetro de consulta del adaptador BPA no podía guardar el nombre del campo de clave. Este problema se ha resuelto actualizando la funcionalidad para permitir el nombre del campo clave en los parámetros de la consulta.
DAA-89862	Anteriormente, el proceso de carga fallaba cuando los administradores hacían clic en ver y reclamar tarea. Este problema se ha resuelto corrigiendo un error en la carga de UserTask.
DAA-89754, DAA-89613, DAA-84854	Los usuarios habían recibido previamente un mensaje de "vencimiento de sesión" mientras estaban activos, lo que provocaba cierres de sesión inesperados incluso después de hacer clic en Continuar. Este problema se ha resuelto corrigiendo errores de cálculo en casos de esquina y asegurándose de que el token solo se actualice después del período de tiempo de espera. Nota: Para solucionar este problema en los microservicios personalizados, se debe utilizar jwt_token desde sessionStorage en lugar de localStorage.
DAA-89584	Anteriormente, durante la distribución de plantillas desde el vManage maestro a otras instancias de vManage, se agregaba una etiqueta GR1(Group) duplicada cuando ya había una etiqueta GR en el nombre de la plantilla. Este problema se ha resuelto incrementando la misma etiqueta GR al siguiente número en lugar de agregar una nueva etiqueta GR.
DAA-88969	En versiones anteriores de BPA, la lógica de reintento de flujo de trabajo de actualización del sistema operativo no pudo actualizar la versión predeterminada en vManage y marcar el pedido como completado. Este problema se ha resuelto actualizando la variable de versión predeterminada cuando se observa el problema del token de falsificación de solicitudes entre sitios.
DAA-88778	Anteriormente, cuando los usuarios intentaban iniciar y cerrar sesión en BPA, se les redirigía a direcciones URL incorrectas. Este problema se ha solucionado pasando el indicador de administración correctamente cuando el origen coincide y garantizando la unicidad del grupo de identificadores.
DAA-87879	Anteriormente, los usuarios experimentaban problemas de accesibilidad esporádicos al utilizar direcciones URL guardadas como favoritos sin iniciar sesión. Este problema se ha resuelto agregando lógica para actualizar la página de inicio de sesión para evitar una redirección no válida.
DAA-87822	Anteriormente, la página Pedidos del catálogo de servicios de NextGen se retrasaba cuando los pedidos contenían más datos en la sección hitos. Este problema se ha resuelto excluyendo los campos que no son necesarios en la página Cuadrícula de

ID de seguimiento de defectos	Descripción
	pedidos y haciendo que una llamada de API esté disponible cuando se selecciona un elemento de catálogo.
DAA-87532	Anteriormente, los usuarios no podían obtener archivos de registro pesados con el comando <code>kubect1</code> . Este problema se ha resuelto habilitando los registros en contenedores.
DAA-85007	Anteriormente, cuando se cancelaban manualmente trabajos incompletos en el nivel de aplicación, se producía una cancelación forzada, que dejaba el estado del pedido sin cambios y no permitía deshacer o eliminar los dispositivos del distribuidor asociados. Este problema se ha resuelto mediante la introducción de una tarea de control de errores.
DAA-85003	Anteriormente, el BPA no podía detectar un formato CSV incorrecto, incluidas las columnas que se combinaban incorrectamente, lo que provocaba que el indicador de activación se leyera erróneamente como falso. Este problema se ha resuelto validando el formato CSV al cargar y mostrar mensajes de error para evitar estados de trabajo inactivos.
DAA-84222	Anteriormente, el método criptográfico del script de control de credenciales estaba obsoleto. Este problema se ha resuelto agregando el nuevo método criptográfico para evitar problemas de seguridad.
DAA-83034	Anteriormente, los perfiles de usuario no se creaban en el portal BPA debido a una dirección de correo electrónico vacía del perfil del sistema de control de acceso del controlador de acceso de terminal . Este problema se ha solucionado creando ID de correo electrónico ficticios si no hay ningún correo electrónico disponible en la respuesta. Además, la validación del patrón de correo electrónico se ha actualizado en la interfaz de usuario y la API.
DAA-82449	Anteriormente, los usuarios configuraban los dispositivos sin comprobar que el nuevo dispositivo se encontraba en modo de controlador, lo que podía dar lugar a configuraciones incorrectas. Este problema se ha resuelto mediante la introducción de un mensaje de alerta.
DAA-80340	Anteriormente, BPA tenía problemas de configuración de OAuth. Estos problemas se han resuelto proporcionando actualizaciones de complementos, una reconfiguración del archivo "config.json" y coordinación con los equipos de gestión de productos y cuentas de clientes.
DAA-92291	Anteriormente, el problema de clave de Secure Shell en el informe del controlador del caso no generaba un mensaje de error. Esto se ha resuelto mostrando el estado de ejecución como "Error" junto con el razonamiento correspondiente.
DAA-84221	Anteriormente, durante la instalación de BPA, la implementación del protocolo ligero de acceso a directorios de auth-service importaba una biblioteca obsoleta, lo que suponía un riesgo para la seguridad. Este problema se ha resuelto sustituyendo "pasaporte-ldapauth" por "pasaporte-custom y ldaps package". Nota: En el archivo en ldap auth config.json, "old entry searchBase->"searchBase": "ou=Cisco Users,dc=cisco,dc=com" se ha sustituido por "new searchBase ->"searchBase": "ou=Employees,ou=Cisco Users,dc=cisco,dc=com".

Problemas conocidos

No hay problemas conocidos sobre los que informar como parte de esta versión.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).