CAN 5.0

Release Document

AUGUST 11, 2020

AVANSEUS TECHNOLOGUES PVT. LTD.

Table of Contents

General Remarks

CAN 5.0 is one of the bi-annual releases for 2020. At the discretion of delivery team, deployments using CAN 4.0 can be upgraded to CAN 5.0, based on each customer situation, to get the new features. All new deployments must use CAN 5.0.

Please review these release notes to learn what is new in this version as well as important notes concerning known issues, bug fixes for 4.0 and improvements in the existing features.

New Features

- **User interface Revamp** for optimized operations allows users to navigate across different screen very quickly. UI has a consistent and high responsive interface that give quick outputs. UI also has an advanced map view and search parameters which is both captivating and engaging.
- **Integrated Development Environment** is a way to allow users to input custom Java code snippets in a smart coding editor which has syntax highlighting, auto compilation as and when the code has been written in the editor, auto-indent shortcut and provides auto-completion of API's or methods when dot operator is used.
- **Performance Counter Prediction and Health Management** feature enables CAN to do real time as well as forecast tracking of all network performance KPIs in all kinds of network and also correlates performance counter values to the alarms for Performance degrade predictions. This feature reports comprehensive health index of equipment components that show the current and historical health status.
- **Voice Based Interfacing** is a NLP(Natural language processing) enabled engine connected to CAN AI. The AI engine takes voice input as a command and generated aggregated result on the User interface. This feature allows ease of accessibility to results and is time saving which is driven by a comprehensive voice command list dealing with network health status, major faults, priority customer management etc.,
- **Enhanced KPI Reporting** is based on wider requirement criteria of users. Some of such criteria includes location, Cause type, Site profile, Service affecting/Non service affecting etc. Enhanced filtering mechanism makes multiple combination of KPI parameters to overall realistic network performance view.
- **Integration Gateway - BMC remedy** is ticketing/incident management software which allows CAN to book predictive trouble tickets. CAN also allows mapping of essential fields automatically between CAN and BMC gateway with an option to customize extra fields depending on customer requirement.
- **Integration Gateway - Splunk** is a software used to search, monitor and analyse machine generated big data/logs. CAN integration allows flexible and automated extraction of data.
- **Integration Gateway – Weather integration** adds a zone based comprehensive weather forecast to predicted faults up to 5 days with an interval of 3 hours for customers to take better decision on ticket creation.
- **Enhanced Cross Domain Correlation** allows enhanced discovery of topology across multiple domains. In previous CAN release, identification of domains were done with a cluster ID. But in this release, domain details along with list of equipment in the cluster is shown. Eg: Transmission, Access, IP nodes.
- **Containerization for dynamic and scalable deployment** enables CAN compatible to cloud native deployment environments. CAN is compatible to docker which enables automation of

deploying, scaling and management through various orchestration applications like Kubernetes.

- **Web Application Security** is configured into CAN in compliance with OWASP and is duly audited by third party. This reduces risk and security threats to application environment. A brief of all different security features are listed in enhancement section.
- **Knowledge Repository** application is used to share knowledge across CAN applications. This knowledge will be used for fine tuning of predictions, creating synthetic history etc. Periodically CAN applications will share their knowledge information to centralized knowledge repository, later this combined knowledge information will be used by individual CAN applications as per requirement. This increases reliability on CAN predictions there by achieving benchmark prediction KPIs.

Enhancements

- Addition of additional fields in Alarm and Predicted fault data like Service affecting/Non-service affecting, Domain, Network type etc. for more detailed data enrichment.
- Data collection audit under Monitoring now has Data source added based on which data audit would be displayed.
- Notification Handler allows configuration of multiple Email IDs as recipient for system event notifications.
- Prediction assignment policy displays cause names instead of cause IDs from database.
- Priority management screen is developed to set priorities like Critical/Major/Minor for Office code/Site.
- Predicted fault analysis screen has more filters to drill down to view required predictions. Few such new filters are based on Network type, Cause category, Service impact, Cause priority etc.,
- Predicted fault analysis screen feature to download filtered daily report and filtered matching report which is based on all the filters mentioned in previous point.
- Parser screen has a new data source as Splunk to extract data from there.
- Cause management under Settings allows user to configure Domain, Network type, Cause category, Service impact, Cause priority against a cause. These tags help user to filter the predictions in Predicted fault analysis screen.
- Web application security features:
    1. Compliance towards prevention of injection attacks and other vulnerabilities
    2. Compliance of authentication management to prevent unauthorized user access
    3. Protection of sensitive data and prevention of information leakage
    4. Processing of external XML entities
    5. Enhanced access control measures based on roles
    6. Security misconfiguration issues and error handling
    7. Mitigation of cross site scripting related vulnerabilities
    8. Prevent insecure deserialization
    9. Compliance while using components with known vulnerabilities
    10. Compliance in cases insufficient logging and monitoring
- Two factor authentication feature is developed where user is asked to input an OTP which is sent to him over Email after successful login to validate his authenticity.
- Password change needs an OTP based validation where the OTP is sent to the user's Email ID.
- Key based Password encryption feature in both the database and configuration file which is implemented using JASYPT library
- Java security policy is enforced to prevent unauthorized access to external or internal socket ports & files. This is essential as CAN allows users to add custom Java code snippets in the

software and attacker may write a piece of code which can lead to leaking of sensitive information or accessing ports which can download executable virus files in the server.

- In extension to Java security policy, these custom code snippets have been attached timeout values based on the type of activity/feature. These timeouts are essential to prevent attacker code to be executed for a long period of time or to prevent infinite loops.

Removed Features

- Fault analysis screen is removed from CAN 5.0.

Bug Fixes

- SFTP connection hang issue is fixed. This was an issue with JSCH library which is internally being used by Apache VFS. The issue was for larger files, one connection thread was being used to point to source and destination during file transfer. The fix was to create separate connection threads to point source to destination location.
- Security breach error observed for builds from R-4.5. The fix for existing setup is to re-compile all the custom Java code snippets.
- Cluster sheet attachment in daily report was causing a problem. This issue is fixed in the code.
- Priority sequence sorting issue for ROE is fixed by changing the source code to sort the entries in ascending order.
- Data collection performance is improved by fixing an issue where inclusion/exclusion filter was taking time to execute its logic.

Platform Support

- **Client OS & browsers supported**:

OS	Browsers supported
Microsoft Windows 7 & 8	Google chrome 60.0 and above Mozilla Firefox 66.0 and above
Microsoft Windows 10	Google chrome 60.0 and above Mozilla Firefox 66.0 and above Internet Explorer 11 and above
Apple MacOS 10 and above	Google chrome 60.0 and above Mozilla Firefox 66.0 and above
Ubuntu Linux 15.0 and above	Google chrome 60.0 and above Mozilla Firefox 66.0 and above
Fedora Linux 29.0 and above	Google chrome 60.0 and above Mozilla Firefox 66.0 and above

- **OS on deployment server**: RHEL 7.0 & above, CentOS 7 and above

Known Issues

- Although CAN has been configured to support internationalization, it is currently available only in English and the CAN binary is packed with English text only. When there is a

requirement from the Customer to port the application to support some specific language, then it becomes the responsibility of the delivery side developer to map the translations into a file and then pack the binary with that language.