Technical Whitepaper Documentation

Company Overview

Perpetuuiti Technosoft PTE is an Intel Venture backed and one of the top 20 most promising Asian software product companies as per CIO Review. Perpetuuiti is focused on developing next generation Business Continuity and Disaster Recovery software solutions. Perpetuuiti's flagship product Continuity Platform™ allows Seamless Business Continuity for organizations across People, Process and Technology. One of the key Availability Management challenge is that every platform needs expertise to recover at all levels for the organization. Continuity Platform™ provides Visibility, Availability, and Manageability through Mobility for Business Continuity Assurance.

IT Disaster Recovery Management

Product Overview

Continuity Patrol™ is a completely automated, end-to-end IT Disaster Recovery Management Suite. Centralized approach towards providing Business Continuity in a simplified, efficient manner. Continuity Patrol™ also has the multi-tenant capability to cater to cloud customers with different portfolio of configuration.

To maintain DR environment of complex IT infrastructure, many set of procedures and processes required to be followed at various layers of infrastructure such as OS, DB, Storage, Application, etc. Such task needs to be performed well within time and without any error to meet RTO and RPO timelines; during Data Synchronization phase, DR Drills and in actual DR situation.

Continuity Patrol™ integrates all these layers and creates workflows to perform task quickly and without any error. Apart from performing tasks Continuity Patrol™ provide reports, which are helpful for management to access DR readiness and helpful for DR execution decision making. Continuity Patrol™ also monitors DR IT infrastructure and take actions if any of the layer / component is not working properly to ensure DR environment is always up-to-date and ready.

Supports integrations with all popular 3rd party replications tools such as Zerto, Carbonite, vSphere, Replica, Veritas Replication - DB native replication tools such as ODG, SQL NLS, Mirroring, Always-On, DB2 HADR, MySQL Master-Slave, PostgreSQL native, Sybase SRS & all Storage replication technologies including IBM, HP, Hitachi, DELL, NetApp & EMC
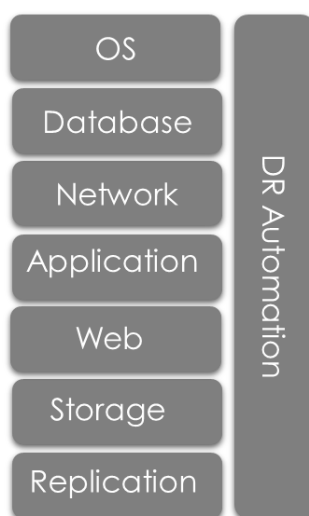
Continuity Patrol™ automates testing of the DR environment (Planned and Unplanned failover) that gives confidence to customers on their DR readiness, it provides DR compliance records and reports to meet the regulatory requirements. Reports can be pulled out and submitted for Auditing purpose.

Continuity Patrol™ provides capability of One Click Disaster Recovery which supports multiple application tiers including OS / DB / Storage / Replication / Application / Middleware. Continuity Patrol™ supports recovering single application OR multiple applications in one-go.

Continuity Patrol™ extends comprehensive capability to monitor MTPOD, RPO for complex Applications and Databases in line with ISO 22301 Standards and guidelines with automated alerts information on any deviation. It provides real time view of recovery process activities so that administrators can control the DR process execution if required. Continuity Patrol™ administrators have a single view across all the application and sites configured in Continuity Patrol™ and can monitor the status for all the groups. Continuity Patrol™ improves the probability of recovery when compared to point-in-time DR testing methods in use.

Continuity Patrol™ supports popular Mobile platforms such as Apple iOS, Google Android, Microsoft Windows, to be able to trigger the DR activities remotely from anywhere seamlessly.

Introduction

Perpetuuiti is the innovation leader for automated Business Continuity and Disaster Recovery Enterprise Software *including* Disaster Recovery as a Service (DRaaS). Through our award winning flagship product Business Continuity Management System (BCMS), Perpetuuiti provides the full automation of the work flow activities that enables what our competitors can't … a one button click DR solution! That means a guaranteed switch-over / switch-back and fail-over / fail-back solution without human intervention. Its Single dashboard provides 'C' level executives with the complete health of the DR environment and services, including physical and Virtual Environments.

Disaster Recovery refers to the ability of IT and hence the business, to recover from a catastrophic failure to the primary data center due to a disaster or disruption. Disaster Recovery solution involves making available a set of hardware, software, data and operations at a remote site, in such a way that the remote site can take over the responsibilities of providing core business services in case of a disaster at the Primary Site.

Continuity Patrol™ is a Hybrid DR framework designed to support multiple replication and DB technologies integrated to provide complete DR solution with automation. Perpetuuiti services ensure best cost of acquisition and ownership of solutions. These services are tailored to meet the growing needs of application availability at the time of Disaster. Perpetuuiti Continuity Patrol™ Solution supports all platforms and integrates with most of the databases and applications without changing or reconfiguring anything in the environment. **Continuity Patrol™ integrates seamlessly with the existing setup without the need to reconfigure or remove existing application setup including clusters.**
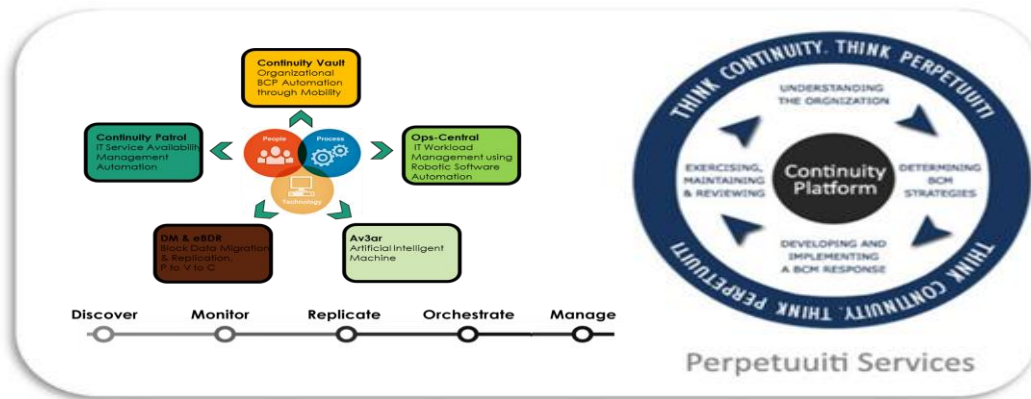
Benefits

1. Allows IT Disaster recovery processes to be built on a reliable, consistent recovery time.

2. Reduces infrastructure management cost and staffing skills.

3. Reduces or eliminates human error during the recovery process at time of disaster.

4. Facilitates regular testing to help ensure repeatable, reliable, scalable IT Disaster recovery.

5. Notification using SMS and email and support for notification lists to handle different stake-holders, groups, DR Admin users.

6. Monitoring and management capability for remote management.

7. Infrastructure/application based and role based access control to users

8. Create and manage user list that are to receive notification via email

9. Support for physical and virtual servers across primary and DR sites without any restrictions.

10. For the configuration part, users will be enabled with online help & step-by-step help wizards during the implementation phase.

11. Continuity Patrol maintains a small asset Inventory to maintain the metadata of configurations performed at Primary and DR entities, same can be made available in a form of report as well at any given point in time.

12. Continuity Patrol is capable of automating different environment including Web/GUI/CLI

13. Supports underlying pre-configured Sync and Async replication at file and block level, Two Site, three site and one to many topologies.

Product Architecture

Continuity Patrol™ is an end-to-end DR Management software that gets installed on one of the Windows servers in IT DR solution environment. This server always resides at DR site / Data Center. This ensures that during disaster situation Continuity Patrol™ is able to communicate with all servers and devices required to make Business Service available from IT point of view. It is recommended to use two identical Continuity Patrol™ servers on both, Production and DR site. This provides high availability for the Continuity Patrol™ solution during normal operation / situation. Continuity Patrol™ can be installed on Virtual or Physical Servers. No Production down time is required for Installation/integration/configuration.
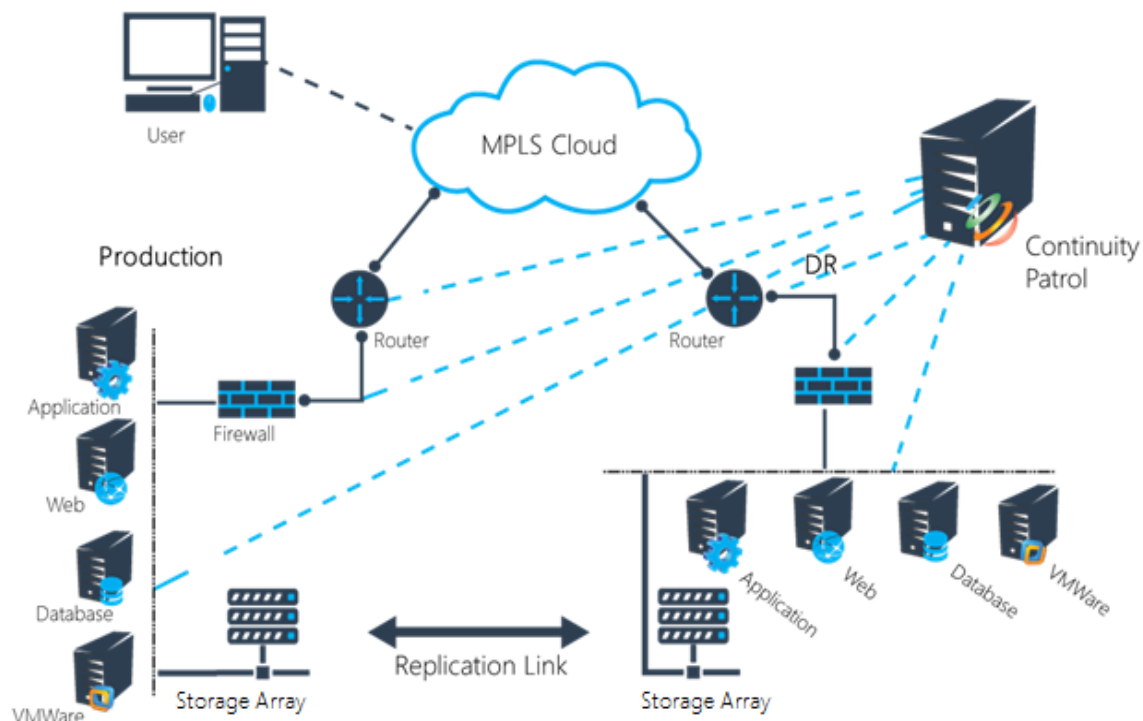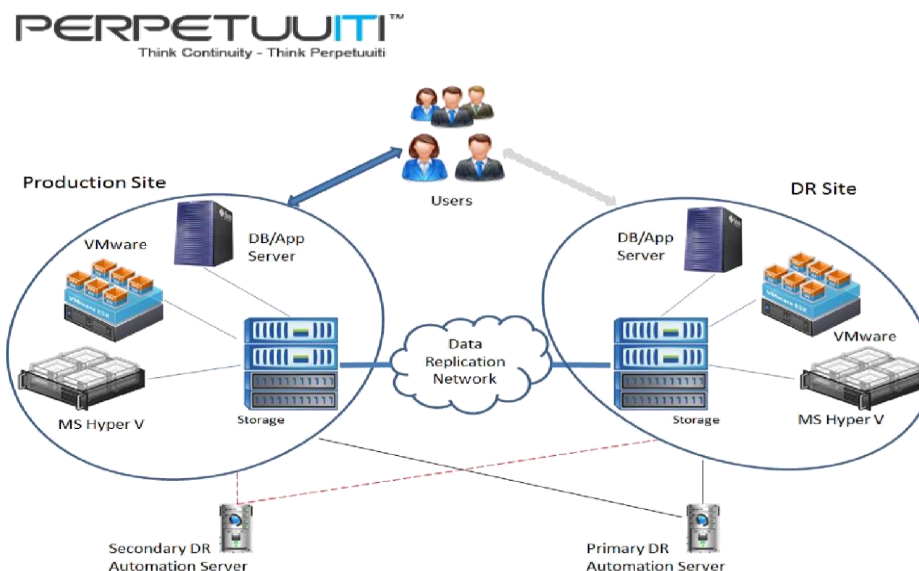
Figure 1 – High Level implementation architecture of Continuity Patrol™ Solution

Above diagram, shows typical Continuity Patrol™ solution architecture. Continuity Patrol™ needs identical servers on both the Production and DR site. Production server for Continuity Patrol™ is residing at DR site, while server at production site serves purpose of redundancy and high availability.

Continuity Patrol™ use MSSQL/Oracle/MySQL as a database with 3DES/AES 256 encryption for storing all sensitive information about the IT infrastructure in scope of DR, application details including interdependency, Workflows and procedures to be executed during data synchronization activity, switch-over, switch-back and fail-over activity. Applications configured in Continuity Patrol™ are divided into groups, so that, same can be managed properly. Continuity Patrol™ communicate with most of the infrastructure components over SSH and credentials are passed over secured communication channels.

Continuity Patrol™ deployment is easy from the perspective of DR automation, it requires very less human resources & time to configure the DR automation solution.
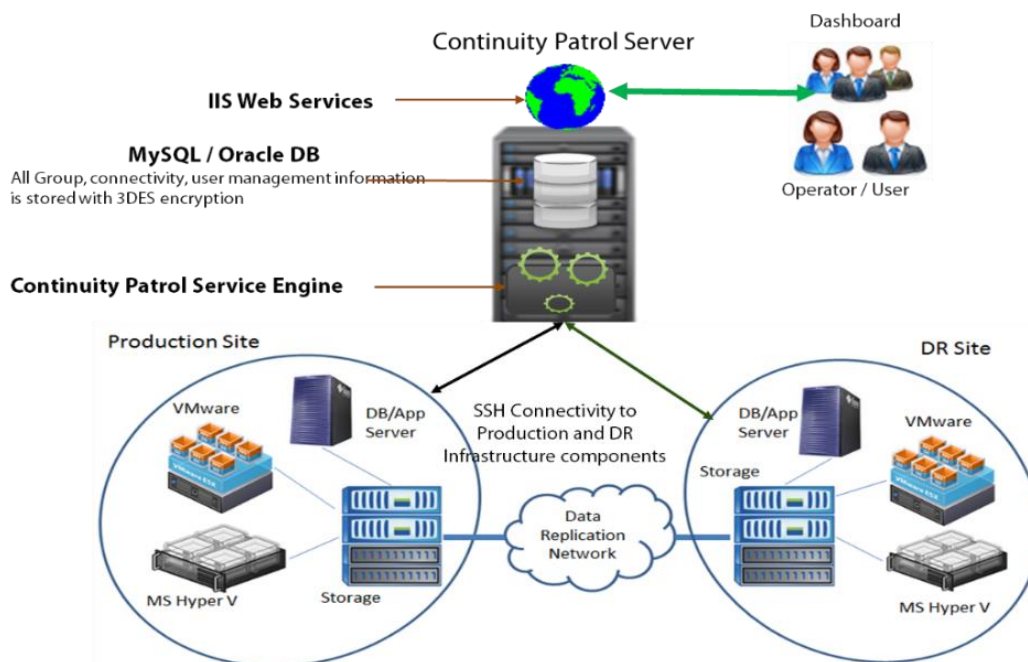
Network, etc. components are tracked and output of same is collected and stored in logs. Using this output results next commands on infra components are executed. Apart from this Continuity Patrol™ can read the logs stored on servers and use these logs or file content to execute the steps. This ensures cross platform activities are performed smoothly and without any problem. It has inbuilt debugging and log capture with facility to view the logs from the web based GUI itself.

Figure 2 –Continuity Patrol™ Solution building block and communication flow

For Data Synchronization between production and DR site various replication technologies can be used such as Storage Array based replication and Database level Replication technology.

Below table gives list of few major replication technologies supported by Continuity Patrol™. The replication of data between Production site and DR site is managed using these technology integrated with Continuity Patrol™ for better management of same.

Interoperability Matrix for Different Replication methods

S. No.	OS Platform	Supported Databases	Supported DB Replication	Supported Storage Replication
1	IBM AIX	Oracle/ DB2/ Sybase	Oracle DG; Sybase SRS; DB2 HADR, DataSync for Oracle	IBM DS/SVC GM/ MGM; EMC SRDF / Mirrorview / Recoverpoint; Hitachi HUR; HP XP/EVA CA / 3PAR remotecopy; NetApp Snapmirrorr; VVR
2	HP-UX	Oracle/ DB2/ Sybase	Oracle DG; Sybase SRS; DB2 HADR, DataSync for Oracle	IBM DS/SVC GM/ MGM; EMC SRDF / Mirrorview / Recoverpoint; Hitachi HUR; HP XP/EVA CA / 3PAR remotecopy; NetApp Snapmirrorr; VVR
3	Solaris	Oracle/ DB2/ Sybase	Oracle DG; Sybase SRS; DB2 HADR, DataSync for Oracle	IBM DS/SVC GM/ MGM; EMC SRDF / Mirrorview / Recoverpoint; Hitachi HUR; HP XP/EVA CA / 3PAR remotecopy; NetApp Snapmirrorr; VVR
4	Windows	Oracle / DB2 / MSSQL / MySQL/PostgreSQL/ MaxDB	Oracle DG; Sybase SRS; DB2 HADR, DataSync for Oracle, MSSQL AlwaysON/ NLS	IBM DS/SVC GM/ MGM; EMC SRDF / Mirrorview / Recoverpoint; Hitachi HUR; HP XP/EVA CA / 3PAR remotecopy; NetApp Snapmirrorr; VVR
5	RHEL	Oracle/ DB2/ MySQL	Oracle DG; Sybase SRS; DB2 HADR, DataSync for Oracle	IBM DS/SVC GM/ MGM; EMC SRDF / Mirrorview / Recoverpoint; Hitachi HUR; HP XP/EVA CA / 3PAR remotecopy; NetApp Snapmirrorr; VVR
6	VMWare / Hyper-V / Citrix Xen / Oracle VM Server / RHEV / PowerVM / HP VPAR / Open Stack	Oracle / DB2 / MSSQL / MySQL	Oracle DG; Sybase SRS; DB2 HADR	IBM DS/SVC GM/ MGM; EMC SRDF / Mirrorview / Recoverpoint; Hitachi HUR; HP XP/EVA CA / 3PAR remotecopy; NetApp Snapmirrorr; VVR

| 7 | AWS/ Azure/ GCP/ OCI | Oracle / DB2 / MSSQL / MySQL | Oracle DG; Sybase SRS; DB2 HADR; MSSQL Always ON/ NLS; ASR; Zerto, Veeam, Carbonite | |

Continuity Patrol integrates with underlying 3rd party replication technologies to provide Delta Sync and resync during DR drills to ensure zero data loss.

DataSync File Replication

DataSync File Replication utility will perform the following functionalities as stated below.

1. File replication over IP networks
2. Replication from multiple sources to multiple destination files/folders
3. Replicate nested files & folders
4. Only replicate files that have changed since last replication instance
5. Preserves file attributes
6. Skip open files
7. Provides log of replicated file names, pending files and number of files to be replicated and statistics on throughput
8. Ability to specify replication from a point-in-time
9. Support replication for Unix symbolic links
10. Restart replication after a break from last successful replicated point
11. Replicate only portions of the file that have changed
12. Specify file/folder names & extensions to include or exclude for replication
13. On-the-fly file compression for reduced bandwidth usage
14. Configurable number of processes to replicate in parallel
15. Existing Scripts and schedules can be called to stop & resume day to day replication operations before and after nightly backup.
16. Existing scripts and schedules can be called to stop day to day replication operations before end-of-day processing.

## DR Dill and DR Execution Activities

Major DR Drill and DR execution activities performed using Continuity Patrol™ are given below:

1. **Switch-Over (Planned DR):** This activity is a planned one and is used to move production environment to DR site in situations such as DR Drill or major planned activity at Production Datacenter which requires significant downtime or major upgradation / changes at Production, in this case customer can use this option to work from DR and data will be replicated from DR to primary.

2. **Switch-Back (Planned Fallback):** This activity is a planned one for the customer to come back to the primary once the activity, DR Drill or upgrade / patch activity is completed.

3. **Fail-Over (Unplanned):** This activity is an unplanned one happens suddenly due to any disaster. To recover critical IT environment at remote site from disaster, this can be initiated.

4. **Fall-Back / Fail-Back (Planned):** This activity is a planned activity happens once the Primary site is ready with resources after disaster.

5. **Non-Intrusive DR Drills (Planned):** Continuity Patrol also is capable of creating workflows for bringing up the applications along with dependencies at DR in an isolated way without pausing/stopping the replication and impacting Production environment.

Note: During DR drills, applications or services which are not part of the DR workflow are not impacted and keep running as usual. Below are the example of such scenarios.

Product Features

Recovery Monitoring and Configuration
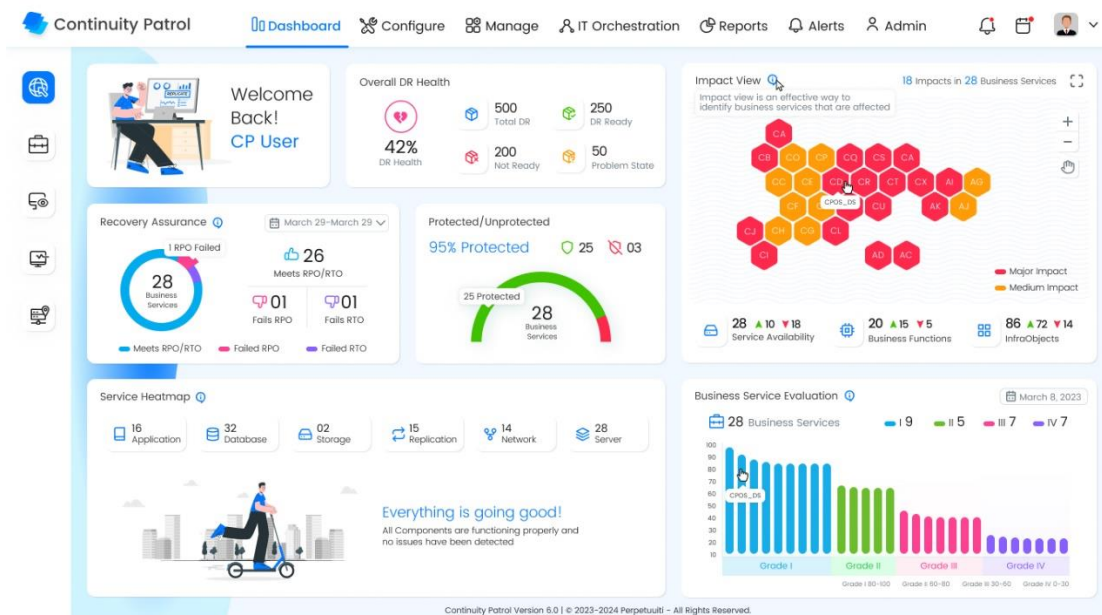
1. Real time monitoring of Business Services, their Functions, dependencies, DR readiness, RPO, RTO, Health at the Business Services level, Services Heat map pointing to root cause of the service degradation.

2. Dashboard provides capability to define services, business functions, IT Components and monitoring of these from availability standpoint.

3. Business-IT relationship to understand how the business services are mapped to the underlying IT Infrastructure components.

4. Provides single dashboard to track DR readiness for all applications tiers configured under IT View 24X7 without any break.

5. Continuity Patrol monitors important health parameters like disk space, password changes, file addition/deletion etc to ensure DR readiness.

6. Continuity Patrol has capability to integrate with underlying Pre-Configured file replication tools which has file system analytics feature to give total file/directory count, typical scan time, number of open files, time of last replication for a file, file size and time stamp.

Events & Notifications

Alerts are provided on event threshold conditions such as RPO deviation, replication status, replication log space full, server up/down status, etc. with event categories such as Incident, critical, normal, and informational. A policy can also be attached to an event to trigger a workflow with defined severity levels.

Events can be customized to,

- Meet end user specific monitoring needs by raising custom events
- Define and register custom event
- Raise custom event based on threshold or state conditions
- Build powerful monitoring and policy response in conjunction with existing BPI
- View and take action on occurred events
- Configure sequence-of-events graph to help root-cause analysis

Recovery Automation
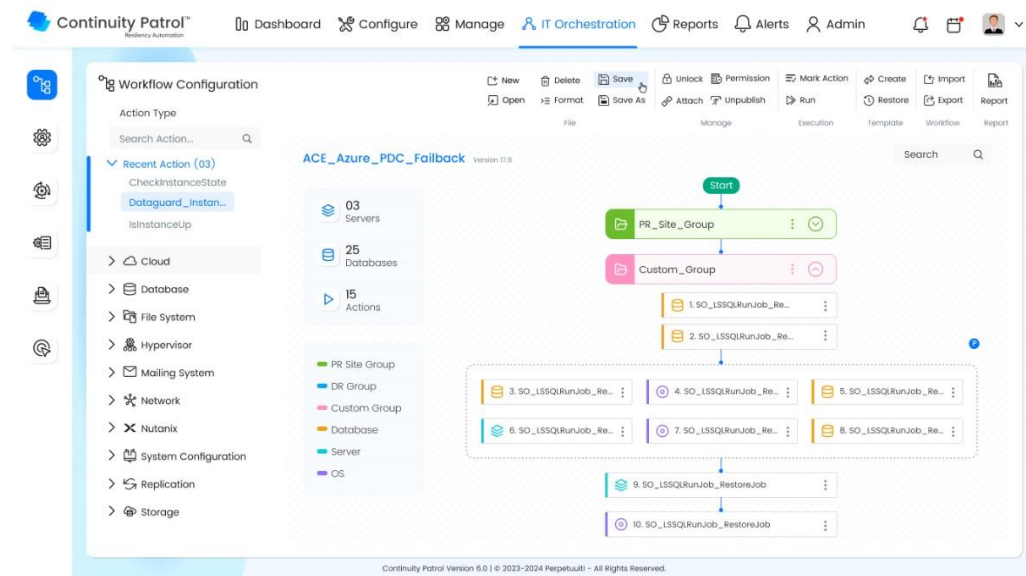
1. Provides central console to start & stop the replication for each application.

2. Continuity Patrol has single console to manage integration of application backup and end-of-day process along with business continuity operations.

3. Workflows can be modified as per the required sequence to get executed, drag-and-drop facility has been enabled for the same.

4. Logical conditions can be introduced in the workflows to control the executions.

5. Extensive Library of actions in terms of all types of OS, DB, Application, Web, Middleware, Storage Array, Network & Replication are available as part of workflow configuration. Custom scripts is supported in "on-demand" basis.

6. Auto discover the configuration details of identified Databases & Storage arrays and map their relationship between Primary and DR components.

7. Provides mapping for interdependencies among 2-tier, 3-tier & 3-tier applications between Primary and DR entities.

Perpetuuiti | Resilience Redefined...

DR Drills

Timeline View   Workflow_ODG_SO

1. DGVerifyModeAndRole_PR_DR
2. DFVerifyMaxSequenceNo_PR_DR
3. DgSwitchLogFile_PR
4. DFVerifyMaxSequenceNo_PR_DR
5. DGCheckUserStatus_PR_DR
6. SwicthOverStatus_PR
7. DGSwitchPrimarytoStandby_PR
8. StartUpNoMount_PR
9. AlterDbMountstandbyDb_PR
10. DGSwitchStandbytoPrimary_DR
11. AlterDatabaseOpen_DR
12. CheckOpenMode_PR
13. CheckOpenMode_DR
14. DGSwitchLogFile_DR

1. Central console to start & stop and track recovery workflows for each application or group of applications.

2. Readymade, automated, out-of-the-box switchover and switchback workflows and also captures start / end timelines, status of activity and execution details.

3. Exportable workflow templates to be re-used for multiple workflows.

4. Pre-flight / dry-run checks to ensure conditions are met to ensure a successful drill such as validation of pre-build equivalent conditions that are required for successful Application recovery at DR. These checks are customizable workflows.

5. Parallel recovery of multiple workflows to reduce the overall RTO window to meet customer's business objectives.

6. Ensures increase in success rate and helps in significantly reducing time to DR drills, with the help of DR readiness checks.

7. With DR readiness module which validates and verifies DC_DR equivalence for OS, DB and applications. This can be configured with out-of-box and custom templates.

Security and User Management in Continuity Patrol™

Below are the important accounts and roles assigned to user accounts.

1. ***SuperAdmin***

    These users can create multiple companies, SuperAdmins, Administrators & Operators. They can manage Administrators, Operators and have full access of entire DR automation tool.

2. ***Administrator***

    These users can create child companies, Administrators, Operators. They can manage Administrators, Operators and have full admin access for child companies.

3. ***Operator***

    These users have view-only access. They can only monitor Continuity-Patrol™ and pull-down relevant reports.

Continuity Patrol™ Application Security:

1. Continuity Patrol™ uses 28 Bit SSL Encryption for Secure Communication

2. Continuity Patrol™ stores *All Sensitive Information* such as User-IDs, IP Addresses, Passwords and all related parameters in 3DES / AES Encrypted format in Application Database. This ensures nothing is visible even user gain access to application database.

3. Continuity Patrol™ integrates with third party authentication protocols like Active Directory Services, CyberArk, LDAP, SAML etc. for secured authentication.

4. Continuity Patrol™ uses secured user / password policies to create and manage users and related passwords.

5. Continuity Patrol™ provides 3 levels of authentication to execute workflows of Critical Processes. Execution of workflows is possible only for Super-Admins and Admins.

6. Continuity Patrol™ provides role-based authentication and user creation to monitor and manage DR infrastructure. E.g. Operator role can be created to access Continuity Patrol™ application in monitor mode.

7. Continuity Patrol integrates with any 3rd party SIEM tools to do log management.

Reporting

Following reports can be pulled out from Continuity Patrol:

1. Readymade reports on Business Service Availability, RPO Deviation, RTO Deviation, Application DR Readiness Status, etc. Details of each recovery workflow execution detail is available in DR Drill report. Reports can be pulled in pdf, CSV, XML formats.

2. Detailed reports for DR drills as per ISO 22301 that covers granular steps involved in recovery of all tiers as per the execution sequence.

3. Standard Monitoring reports including

    i. RPO deviation over time range
    ii. RTO deviation over time range
    iii. Workflow execution time for each step
    iv. WAN utilization over time range
    v. Replication over time range
    vi. Application summary
    vii. Test summary report

4. Ability to create UI based custom reports; data can be exported to popular reporting engines.

Value Proposition

Product Architecture

Agentless

Continuity Patrol™ is basically an Agent Less/Script-less that Manages/Automates Databases, Applications, Network and Change Control for a Heterogeneous Environments of an Enterprise.
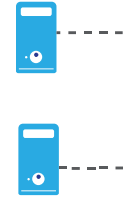
Platform Agnostic

All vendor APIs are available in the product as Libraries, which would make the workflows easy to execute and user-friendly to modify and doesn't require any programming skills or development efforts

End-to-End Automation

Automation Workflows covering end-to-end for the entire layers of IT including - *Operating Systems | Database | Application | Network | Storage | Replication*
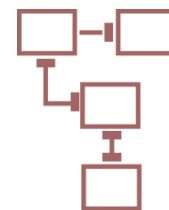
Multi DB support for Metadata

Metadata can be configured to be on MySQL, MS SQL Server and Oracle databases. It also takes care of accidental metadata deletion and recovers and rebuilds the metadata automatically.

Recovery Monitoring

Range with multiple timelines for RPO

Configured applications will be monitored for real-time RPO values for different timelines based on categories like peak-time, lean-time, idle-time, etc.

RPO

15 Mins | 30 Mins | 60 Mins

Monitoring Parameters

✓ Real-time monitoring of DB & app-level RPO

✓ Alert when the configured RPO breaches against the benchmark.

Business Impact Analysis [BIA] Module

BIA is a module to calculate the business impact to the organization due to any disruption. The calculation is based on any application downtime, any disruptions to dependencies, RPO deviations, etc. Based on the calculation, the impact will be reported to stake-holders to take decisions on time. BIA showcases the Business service availability and integration with IT in real time hierarchy shown and the cascading impact of disruption on multiple business services along with financial impact.

Recovery Automation

Resource Co-ordination

Resource coordinator feature of continuity Platform performs vital role of resource coordination during DR drill and Actual DR situation. This reduces large amount of human efforts and time required for sending / updating various stake holders and resources for actual recovery process, alerts, information and messages.

Application Awareness

Intelligent built-in logic that understands the interdependencies among all the in-bound and out-bound dependencies among all configured applications and maps them automatically and represents them in a diagrammatic manner. This also helps during failover scenarios to understand the dependencies and also provides inputs to BIA engine.

Web

App

DB

Custom Reports

Reports can be customized as per the expectation of customers including:

- ✓ Business Impact Analysis Report
- ✓ Application Impact Analysis Report
- ✓ Financial Impact Analysis Report

Password Management

A Unique feature that monitors the OS user passwords and forwards alerts to users to take action when they get changed.

DNS/NAT Automation

Automated approach towards DNS and NAT methodologies in both GUI and command-line based interfaces. Global Load Balancer [GSLB] changes will happen from customer side, where a pop-up will be initiated via workflow during a failover execution to re-route the users to the DR site.

Firewall Policy Automation

Automated approach towards firewall policies that are Required to be updated at DR periodically and this also helps during a failover scenario is automatically handled in the workflow without any manual intervention.

Virtualization Aware	
Virtualization Aware Product is fully automated with popular virtualization platforms from the perspective of ✓ Monitoring all the VMs ✓ Management of all VMs for availability ✓ Replication of VM images through incremental block-based replicator ✓ Data Integrity for assured recovery at DR ✓ Powering ON the VMs ✓ Dynamic resource allocation of VMs after DR failover ✓ Bringing up all the DB and App services. ✓ Supported Virtual platforms are VMWare, Microsoft Hyper-V & Xen	

Support for Mainframe

Mainframe environment [AS-400 & ZoS] is fully compatible in terms of Monitoring and Management 24X7 from the perspective of DR. All mainframe related DR activities are automated with built-in Libraries.

Workflow Management: DR aware, flexible and scalable engine to configure, monitor and manage workflows. Has capabilities such as:

Configuration of workflows include,

- ✓ Set environment variables at run-time

- ✓ Loop, delay, skip, forks & manual input options for workflow execution

- ✓ Build/edit workflow using a UI

- ✓ Support for parameter passing between actions and also proper description of operation with settable input parameter values

- ✓ Execute workflow based on user specified schedule/calendar

Continuity Patrol™ Integration with Virtualized Platforms

1. Continuity Patrol provides VM management and DRM solution which will be integrated to meet the requirement and also provides capability to integrate with the underlying Virtualized Platform.

2. Continuity Patrol provides a GUI based DR workflow editor with Wizard based workflow creation tools so that DR workflows can be customized and extended to meet the desired specification.

3. Continuity Patrol supports Real time visibility and status reports into Step By-Step DR execution plans along with Granular controls in the DR workflow editor. It also has the capability to control access to recovery plans with granular role-based access controls to meet the desired specification.

4. Continuity Patrol has the functionality to monitor the availability of remote site and alert users of possible site failures.

Operations to be Performed using Continuity Patrol™

Data Replication: Continuity Patrol™ will monitor on-going data replication between Production & DR sites. Continuity Patrol™ will report any deviation in RPO and RTO via notifications & alerts.

Switch-Over: A switch-over is a planned operation to move from Production site to DR site. It involves following of entire set of required processes with active participation of appropriate stakeholders. Switch-Over will be invoked by using Continuity Patrol™ which will result in role-reversal of involved IT layers residing in Primary and DR sites. Switch-Over does not expect any data-loss as it is a planned activity.

Switch-Back: Switch-Back operation is a planned activity to move from DR site to Production site. Steps involved in Switch-Back are similar to the Switch-Over steps, except that they are in the opposite direction. Similar to Switch-Over, data-loss is not expected during Switch-Back.

Fail-Over: Fail-Over is, usually, an unplanned activity, which is invoked when the Production site experiences a disaster situation. A disaster situation could be any situation, which renders the Production site to become unusable for an extended period of time. An executive decision is typically taken, after a review of the situation (to be considered at disaster) is done with experts, to declare a disaster and to invoke Fail-Over to the DR site. Since invoking Fail-Over is an unplanned activity, data-loss is expected as per the defined RPO.

Fail-Back / Fall-Back: Fail-Back operations are a set of planned activities to move from DR site to Production site and restoration of their original roles of Production and DR site. This entire set of activity will include the following:

1. Restoration of Production environment, which may include procurement and deployment of new HW etc., Restoration of data using backups, etc. from the DR site. This is similar to the building of a DR site from scratch.

2. Re-synchronizing the DR and the Production environments using the replication technologies. This will be done using Continuity Patrol™ similar to how it will be done for the DR setup. This will include reverse replication from the DR to the Production environment.

3. Once the Production and the DR environments are in-sync as required, Fail-Back from DR to Production site can be initiated as a planned activity, which is usually similar to the Switch-Back activities. This will be achieved using Continuity Patrol™.

Application Workflow: Application workflow will be custom stitched with Continuity Patrol™ dynamic workflow creator. This workflow will be used to create application recovery procedure at DR site.

Network Solution for DR Failover: Following activities can be accomplished using Continuity Patrol™:

1. DNS changes required at DR site can also be automated using Continuity Patrol™.

2. Continuity Patrol™ can also perform necessary changes in networking devices using customized workflows during DR drill and DR execution scenarios.

Continuity Patrol Licensing Policy

Licensing is based on

1. Database SIDs

2. IP Addresses for App, MW, Web Servers, Network devices, 3rd party application management consoles

People and Process Management

Product Overview

Brought to you by Perpetuuiti, Continuity Vault intuitive user interface and sophisticated functionality reduces the time and cost of managing resilience plans whatever the size of your organization. So Continuity Vault not only provides return on investment but also is easy to use and user friendly therefore will be well accepted by all the stakeholders in your organization. Continuity Vault facilitates a commonly shared and logistically structured BC process across the organization. Hence there is standardization across the organization.

Continuity Vault has capability to export diverse and intelligent reports. So you are always ready for any audit or management review. These reports also provide statistics that highlight opportunities. What if analysis is one of the unique features of Continuity Vault through which one can identify the impact an incident could have on the organization not only from financial perspective but to extend where the user would be able to identify the number of transaction completed as well as impacted, number of resource impacted, Facilities impacted, dependencies if any.

Continuity Vault defines and documents detailed plan and procedures for all business functions and locations to ensure business continuity which includes following functionalities:

- ➢ Crisis/incident management
- ➢ Business recovery
- ➢ IT disaster recovery and service continuity management
- ➢ Supplier/sub-contractor risk and contingency management
- ➢ Governance and program management

Key features of the Product

Modules as per ISO 22301 standard

Continuity Vault is one of the most comprehensive business continuity tool that allows organizations to effectively command, control and co-ordinate all of their business continuity capabilities in line with ISO standards. Hence complete life cycle of Business Continuity can be managed using Continuity Vault irrespective of which stage of implementation you are in.

This will also ensure central monitoring and management of people, processes and IT systems across multiple locations from a single unified dashboard

1. Organization structure
2. Resource management

3. BIA and dependencies
4. Risk Assessment
5. Risk Mitigation
6. BCM strategy & plan development
7. Incident Management

Plan   **DO**   **Act**   **Check**

12. Audit management

8. Notification (Exercise / Testing / Drills)
9. Reports
10. Performance review
11. Management Review
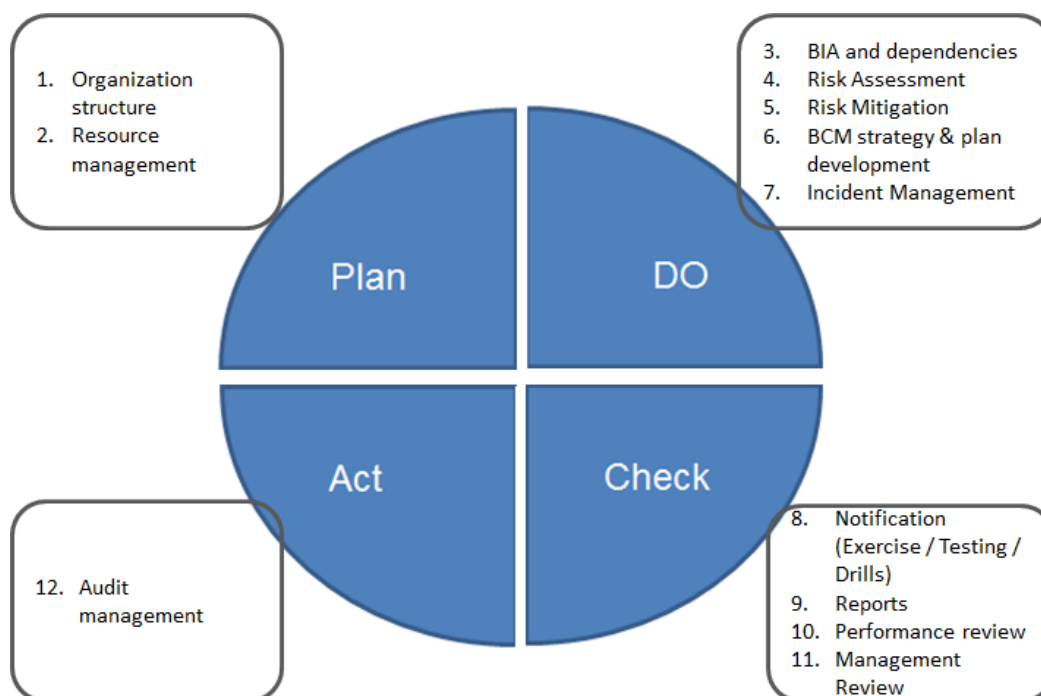
Business Impact Analysis and Risk Assessment

The BIA is the foundation on which the BCM programme is built. It identifies, quantifies and qualifies the impacts in time of a loss, interruption or disruption of business activities on an organization and provides the data from which appropriate continuity strategies can be determined. The BIA identifies the urgency of each business activity undertaken by the organization by assessing the impact over time of an interruption to this activity on the delivery of products and services.

Using Continuity Vault Business Impact Analysis can be performed for the products and services of the organization considering the activities and dependencies that underpin those deliveries.
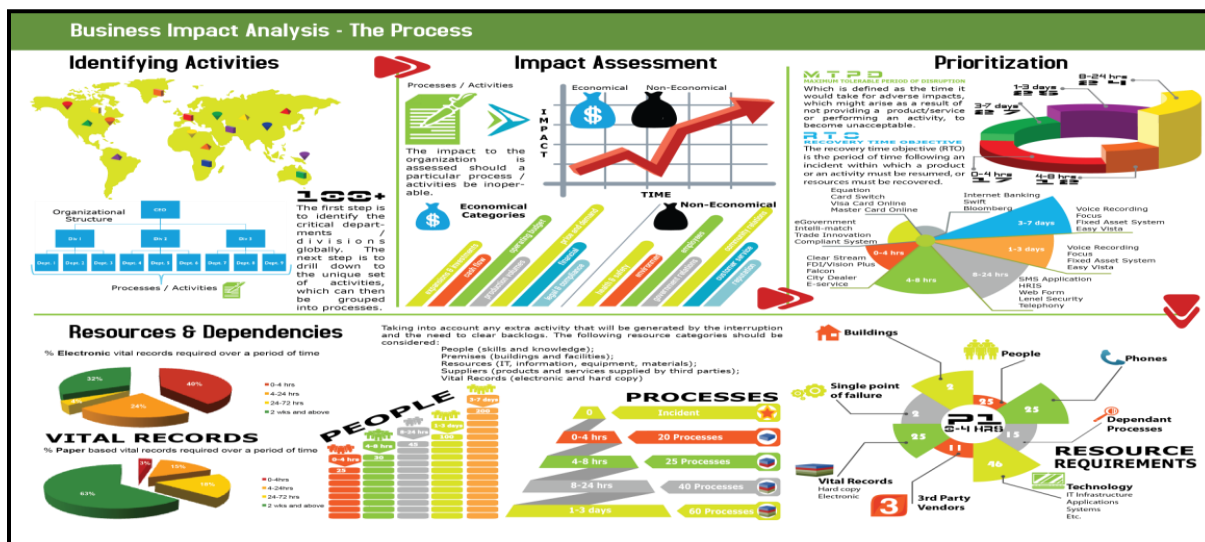
Impact	0 To 2 Hours	2 To 4 Hours	4 To 8 Hours	8 To 12 Hours	12 To 24 Hours	24 To 48 Hours	48 To 72 Hours	72 Hour To 7 Days
ImpactTypeName: Financial Impact								
Competitive advantage	Negligible	Insignificant	Negligible **	Minor	Major	Major	Major	Severe
Penalties /Claims	Negligible	Negligible	Insignificant	Minor	Major	Major	Major	Severe
Productivity Loss	Negligible	Negligible	Insignificant	Minor	Major	Major	Severe	Severe
Brand/Reputation	Negligible	Insignificant	Insignificant	Minor	Minor	Major	Major	Severe
Lost Income/Payments	Negligible	Negligible	Insignificant	Insignificant	Minor	Minor	Major	Severe
Contractual Liability	Negligible	Negligible	Insignificant	Insignificant	Minor	Major	Major	Severe
ImpactTypeName: Operation Impact								
Service Availability	Negligible	Negligible	Negligible	Insignificant	Minor	Major	Major	Severe
Vendor Relationships	Negligible	Negligible	Negligible	Insignificant	Minor	Severe	Severe	Severe
Over All Impact	Negligible	Insignificant	Insignificant	Minor	Major	Severe	Severe	Severe

Calculated RTO	12Hour(s)		Calculated MAO	1Day(s)		IsCritical	No

The overall process of Risk identification, Risk Analysis, and Risk Evaluation is Risk Assessment. From the list of threats that are available in Continuity Vault identify the threats that has potential to the organization's activities and any single points of failure the organization might inherently possess. The results can then be considered to manage the risk by lowering the likelihood or decreasing the impact of disruption or just accepting the risk as is, based on the risk appetite of the organization

Establish the Context: Set internal, external, and risk management context

Identify Risks: What can go wrong

Analysis Risks: Understand the impact

Evaluate: Prioritize risks by risk appetite and tolerance

Treatment Options: Reduce, avoid, transfer or retain
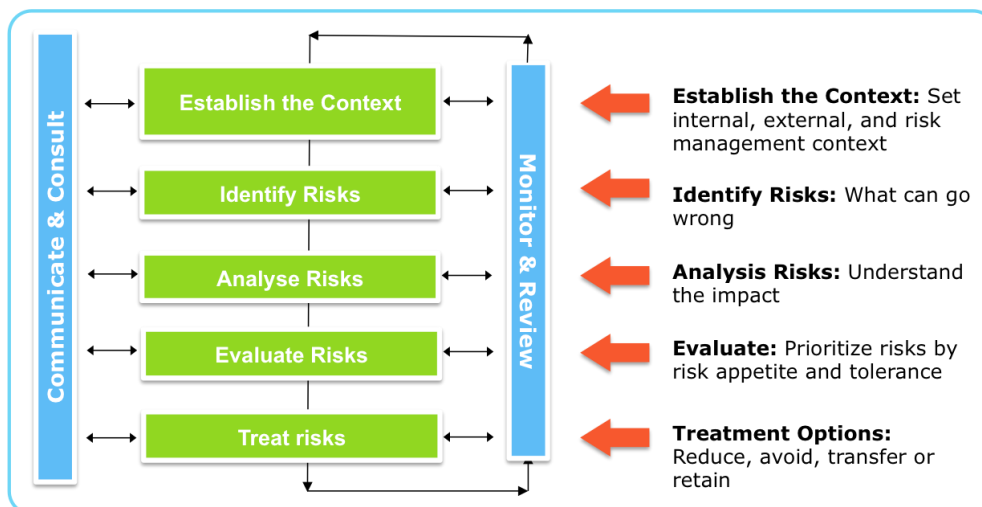
BCM strategies and Continuity Plans

This is the module within which organization identifies and selects appropriate strategies and tactics to determine how continuity and recovery from disruption will be achieved using Continuity Vault. The purpose of designing continuity and recovery strategies and tactics is to set timescales for recovery and identify the means by which those objectives will be best achieved. In CV emergency response plan are segregated from BCM plans and are prepared in a flow chart format with defined steps with owners, contact information, escalation matrix (if the stakeholders are not available), action items etc...

Document management

Document management feature of CV, offers functionalities for not only electronically managing your documents but also creating BCM related document from the application itself.
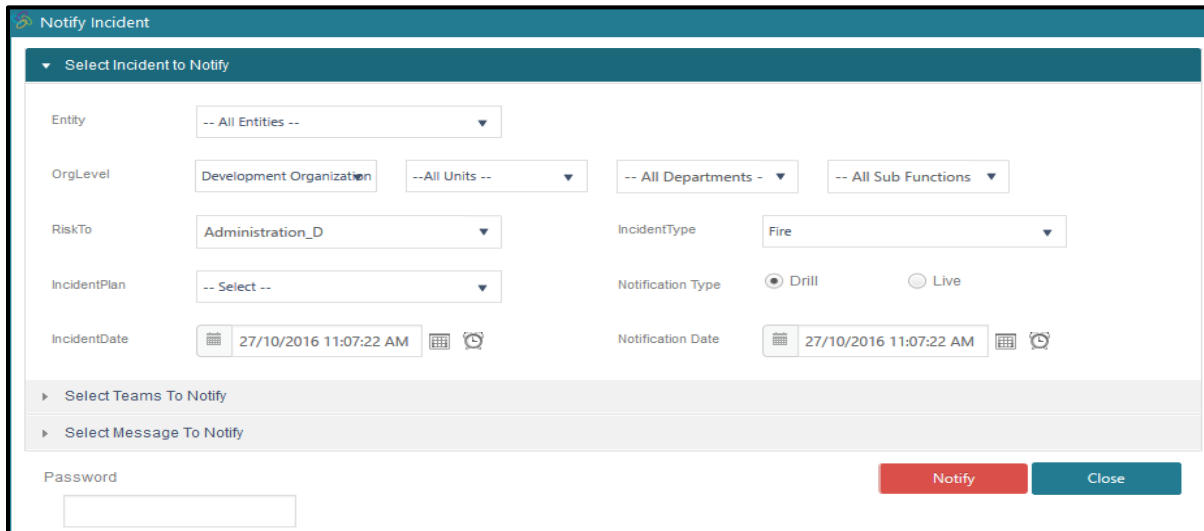
Continuity Vault also offers a repository where your documents such as policies, procedures, guidelines, templates etc.. can be stored and also manage the same as per the document management process with reminders, reviews, approvals and escalation process.

Incident Management

You can design incident response using Continuity Vault to ensure that there is a documented and fully understood mechanism for responding to an incident that has the potential to cause disruption to the organization, regardless of its cause.

Not only design and maintain the Continuity plans but also invoke them at time of crisis using Continuity Vault. Continuity Vault will allow the organization to perform crisis management and sustain critical processes using approved and verified continuity plans.

The same feature can also be used to perform table top simulation tests as well.
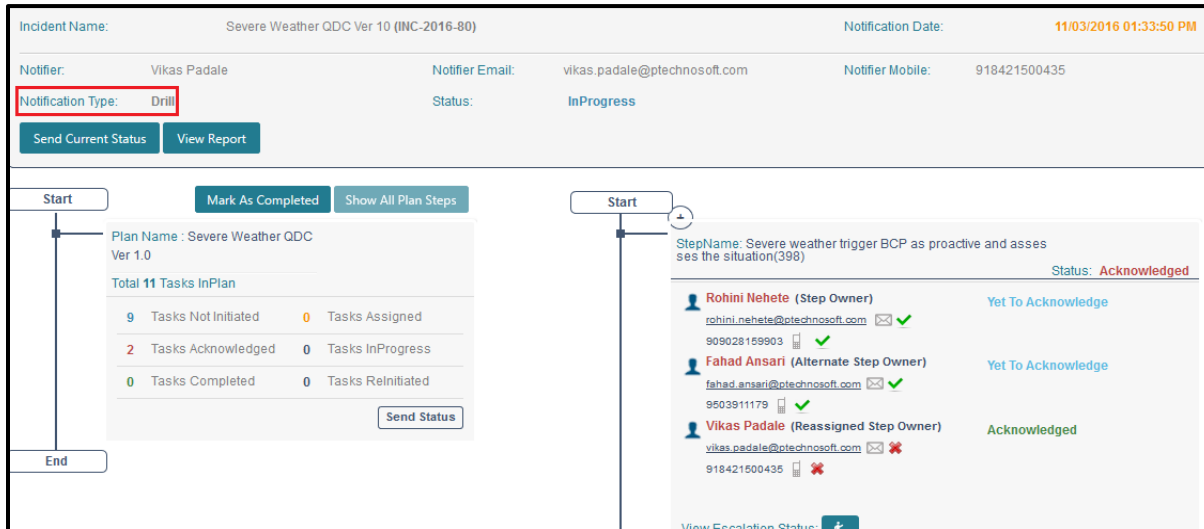
Notification (tests/ drills/ reviews/ escalations)

It is essential to confirm that the BCM meets the objectives set in the BC Policy and that the organization's BCP is fit for purpose. This ensures that the BC capability reflects the nature, scale and complexity of the organization it supports and that it is current, accurate, and complete, and that actions are taken to continually improve organizational resilience.

Continuity Vault enables organization to achieve this through this module. Through Continuity Vault organization can effectively demonstrate the organization's operational effectiveness of the BCM Plan.

BCP	Outcome	BCP System Exercise	Type of Exercise	Frequency
Business Continuity Plan I	Validation of roles/ responsibilities and knowledge of procedures/work instructions	BCM arrangements	Walk-through of plan	Quarterly
	Validation of telecommunications recovery time objectives	IT and telecommunications system	Simulation	Annually
	Validation of recovery time objectives for staff relocation	Logistical System	Exercise critical activities	Annually

CV has mass notification capability. CV can be integrated with client's gateways, such as SMS (for messaging services) gateway, SMTP gateway (for email services). PABX gateway (for calling services), whatsapp gateway (for whatsapp messages) etc.. and the notification will be done using these gateways for various activities such as co-ordinating or collaborating with relevant resources or key stake-holders during events, DR drills, simulation table top tests across DC or simple notifications such as review and approval notifications etc... This notification would be two way communication and response from the stakeholders can be tracked on the CV.

CV can be used to perform call tree tests and escalation matrix to the management. CV will also provide you with the report that will highlight any concerns in the contact information or the validity of the stakeholder

Once the test / drills or incidents are invoked, the same can be monitored on the a real time basis and finally CV will provide a actionable report that will highlight any areas of concerns or gaps in the BCP or DRP that was invoked

Reports

It is crucial for an organization to receive intelligent and actionable report to address any anomalies in the system. Continuity Vault provides multiple reports which can also customized to suit the requirement of the user. Reports can be extracted in multiple formats such as PDF, Excel, Crystal etc…

CV has native (in built) reports however we would like to customize the same to suite the requirement of the clients. During the implementation phase we would understand the bespoke requirements and customize CV accordingly.
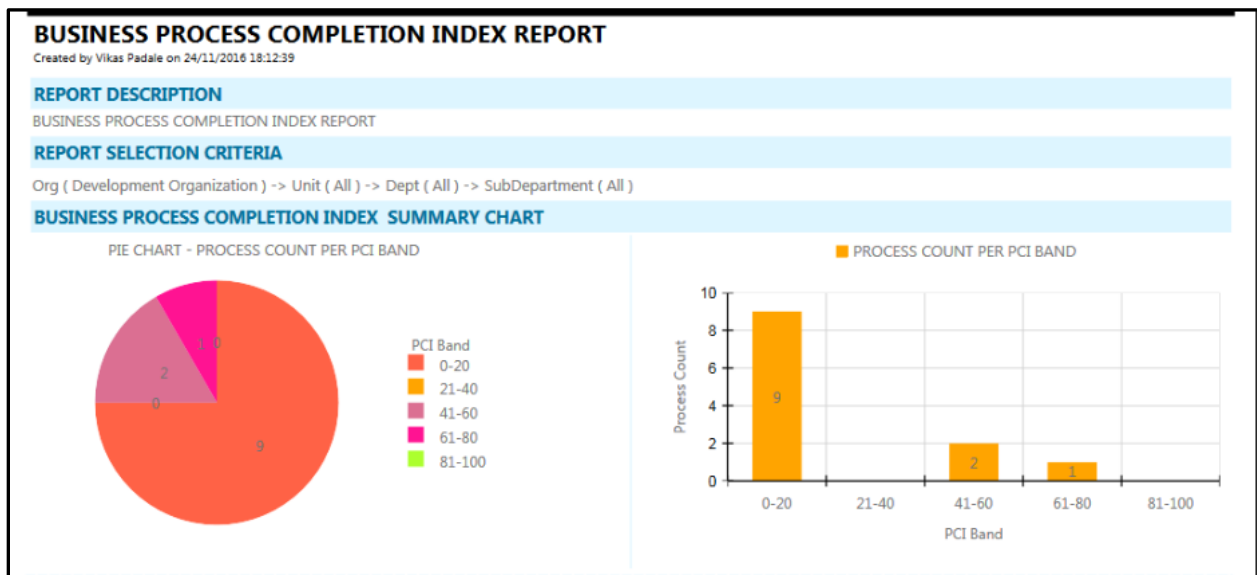
What If Analysis

What if analysis is one of the unique features of Continuity Vault through which one can identify the impact an incident could have on the organization not only from financial perspective but to extend where the user would be able to identify the number of transaction completed as well impacted, number of resource impacted, Facilities impacted, dependencies if any etc.

What is the use of just understanding the impact one would need to also understand what needs to be done to minimize the impact / continue business. What if analysis module of Continuity Vault provides recovery options that have been identified during recovery strategy stage of building BCM. This will let us know number of resources required to manage business continuity, where the resource can be moved to, how much time is required to manage the backlog etc. And as the options are invoked it will show how / to what extend the impact is reducing. CV will show impact of an incident on simulation basis as mentioned in the previous point and not on real time basis.

What IF Analysis

Incident	Fire	Entity Type	Site
Entity	BLR	Incident Time	09/10/2017 02:19:51 PM
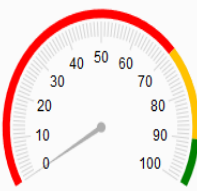
Simulate

Financial Impact Cost
2580
(US $ in Thousands)

Availability 0 %

Organization Impact | **Impacted Processes** | Additional Details

EGSI Skill Center-EDA

0%

Calculate

No. Of Transaction		
400	113 ✓	54 ⚠

Cost (in $)
540

Required	Time(hrs)	Resources
	7 : 40	25

From	To	Resources	Site	Transactions	IsActive
01:00:00	08:00:00	8	BLR	53	No
09:00:00	15:00:00	10	BLR	67	Yes

Parameter Name	Value	Cost	Time	
Move resource to other EGS location (2)				Min ▼
Move resource to other location (3)				Min ▼
People WFH (8)				Min ▼
Increase shift time at DR Site (0)				Min ▼
Move resource to DR (12)				Min ▼

EGSI Skill Center-CBT

BCM calendar

BCM calendar feature of CV will provide the complete information of upcoming and all the other activities scheduled such as Drill, audits, Reviews, Meetings, test and exercises etc... it also has a reminder and escalation process that will alert the stakeholders about upcoming events. if the stakeholder does not take any action within the due date then it can also sent escalations to their managers.
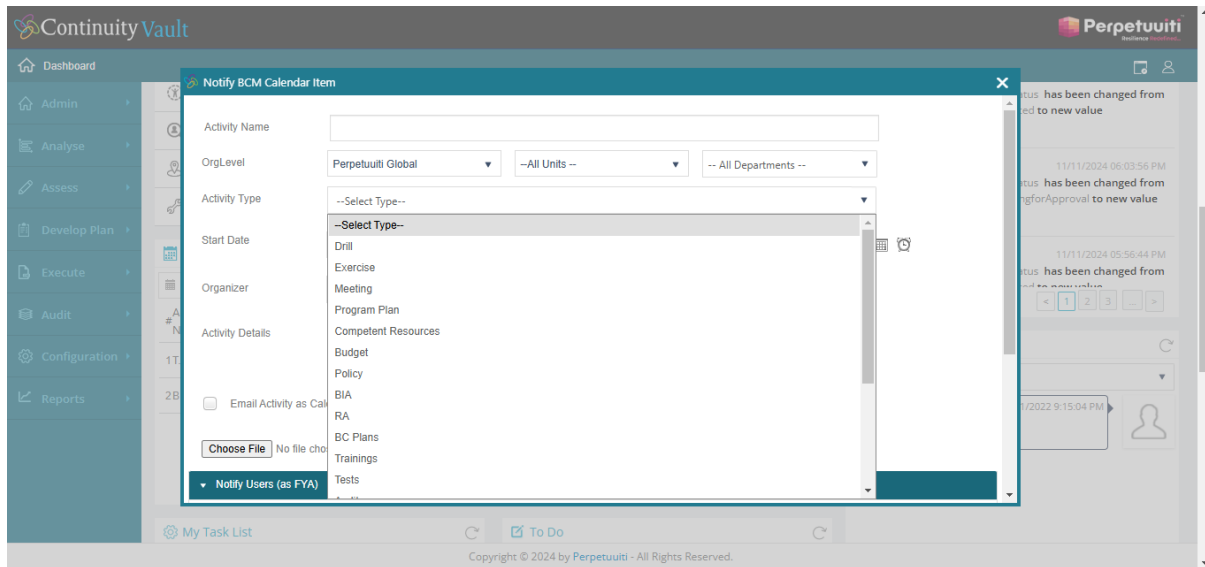
Integrations

CV enables integrations with other applications and streamlines data transfer processes to prevent data silos between teams and / or applications and ensure continuous integration across the enterprise. CV can be integrated with AD for user authenticating, HR database for employee information, with SMS gateway for SMS services. With SMTP gateway for email services etc..

Continuity Vault with AI

AI is everywhere these days, and Business Continuity and disaster recovery is no different. BCM/IT teams can use AI to mitigate, prevent and recover from disruptions faster than traditional methods.

The integration of AI into BCM / IT disaster recovery is not just a trendy addition; it's a significant enhancement that can lead to quicker response times, reduced downtime and overall improved business continuity.

Please meet Susan, our very own bot who is designated as BCM consultant.

Susan encompasses technologies designed to mimic human cognitive functions. At the heart of all these are algorithms enabling Susan to learn from and make forecasts or decisions based on data.

Susan can monitor vast amounts of data from multiple sources in real time, providing businesses with trends and analysis to make informed decisions.

Hosting, Access and Security

CV can be hosted on your premises or on the cloud with PR and DR setup to ensure that CV is available when needed. We prefer to deploy CV on client environment as this will address all the security requirements of the client without additional effort of building the same on cloud. The PR and DR concept of CV can be maintained irrespective of if it is deployed on premises or on cloud.

CV can be accessed as mobile app for IOS and Android irrespective of it being deployed on premises or on cloud.

Again irrespective or where it is deployed on premises or on cloud, security parameters are address in CV with regular VAPT test being conducted by independent third party. Data is CV stored or transmitted in encrypted format. CV ensure data is stored in 512-bit encrypted format and all data transmitted using 256-bit encryption.

CV Architecture
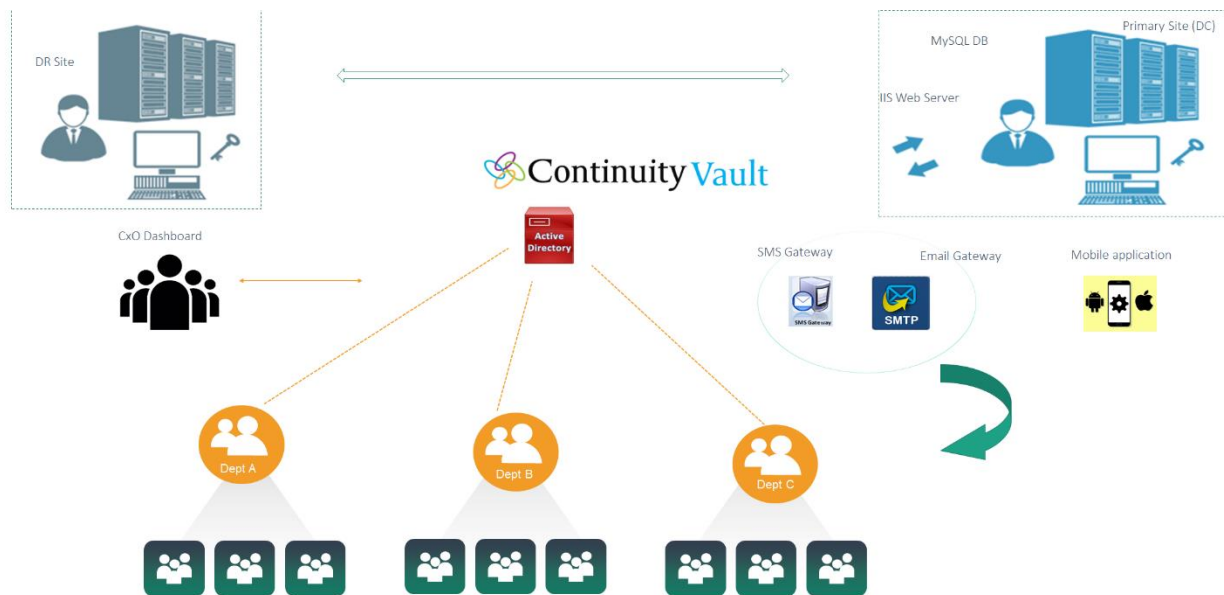
Above architecture represents high level deployment of Continuity Vault. Using Continuity Vault users can conduct BCP DR Drills to test the effectiveness of the BCP on periodic basis. Additional surprise BCP can be carried out at request of ITD in addition to the regular drills using our integrated ITDR Automation Solution Continuity Patrol.

IT Operations and Business Process Management

Product Overview

Why there is a real need for IT Ops today?

Automation is the way ahead in today's world when we are able to leverage software bots to eliminate human intervention and interactions in the entire task / process. This takes the rules based automation to a whole another level. The best bots are able to leverage AI and ML concepts to self-learn and make intelligent decisions that impact the process outcomes without human intervention!

Av3ar IT Ops is the next generation Cognitive computing and Machine Learning system from Perpetuuiti. It is aimed to deliver end-to-end Interactive solutions that dramatically improves the operational efficiencies of customers in the global marketplace. It understands, learns and responds back to customers with emotions like humans.

The product gets plugged into the customer place and absorbs all the data to learn the pattern of the day-to-day tasks and processes. It automates the steps that are required to execute tasks to be carried out daily and solve complex problems that typically takes time to resolve. The built-in Analytics engine is capable of predicting probable issues and breakdowns, decides the approaches to solve them automatically. The compatible platforms includes PC, Tablet or Mobile to view the interface and work on.

Av3ar IT Ops uses **Artificial Intelligence (AI)** and **Machine Learning** algorithms to sense, predict, analyze and solve issues. It provides 360 degree view to customers through the Executive Dashboard on the issues and their status updates like open / resolved tickets, on-going tickets, etc.

It can learn from multiple sources of information like,

- User actions
- Knowledgebase / SoP
- Internet
- Feeds from other related systems

What does Av3ar IT Ops do?

Av3ar IT Ops is a unique type of Virtual Assistant who can absorb, deconstruct and use information like a human being. It has a Self Service portal that understands customer queries and resolve problems without human intervention. It responds to customer chat inputs with voice responses and also read and understand their emails and provide email resolutions, using Artificial Intelligence. Av3ar handles more than 10 Languages to interact with customers across the Globe.

How Av3ar IT Ops works?

Av3ar IT Ops is a Cognitive Framework that uses Natural Language Processing (NLP) technique to interact with customers to provide resolutions within minutes. It uses '**Artificial Intelligence**', '**Machine Learning**' and '**Deep Learning**' algorithms to adopt to the customer environment to quickly takeover the daily operations and start serving customers by itself.

Av3ar resolves issues quickly within minutes and any issues that requires external entities that does not fall under Av3ar's purview will be routed to the next level queue automatically as part of the process. Based on the resolution given by the engineer in the next level, Av3ar learns and adds the learning to its knowledgebase to resolve similar issues in future by itself.

High Level Product Architecture
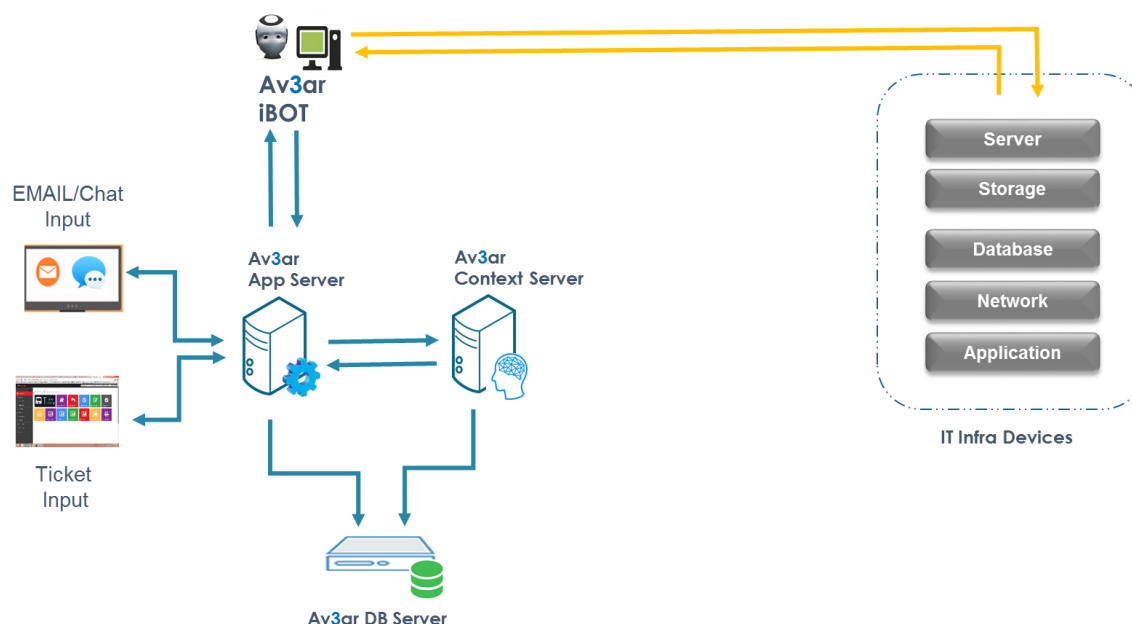
Av3ar IT Ops, as shown in the diagram has the following components as part of its architecture namely,

1. Av3ar Application Server
2. Av3ar Context Server
3. Av3ar iBOTs

These components will work in tandem to cater to requirements of customers. Following sections will discuss the same elaborately.

Av3ar Application Server

Av3ar Application server will receive inputs for the issues from customer in the form of

a. Email messages
b. SR Tickets / Incidents from Ticketing tool
c. Chat messages via Chat Bot interface

Once the messages arrive from any of these channels, the application server passes the extract of the ticket information to the context server to interpret the information or query raised in the ticket, make sense out of it and translates those inputs into action point inputs and get it back to it. The action point input will contain the problem related details, user desktop/server information like hostname, IP address and other network related information to get processed.

At the same time, it also does an acknowledgement back to the customer who sent the service request (SR) to ensure the process is unaffected and customer is kept informed.

Av3ar Context Server

Av3ar's Context server has a huge collection of Library that has resolution actions for various issues from different layers of IT such as OS, DB, Storage, Network, etc. and also has the inputs fed as part of learning from customer SoP/Knowledgebase.

Once it receives the action point input from the application server, context server maps the same against the library actions and passes the information to application server for further resolution execution part of it.

Av3ar iBOT

Av3ar iBOT is a client service that runs on Windows desktop machines and they apply the resolution on the target desktop machine / Server machine. It remotely logs in to the target system and resolves the issue.

After the successful resolution, an acknowledgement goes back to application server to close the SR ticket.

Please Note: In case if Av3ar is unable to resolve the issue, application server moves the issue to the human L2 queue for resolution.

Multiple Input channels can interact with Av3ar to automate the processes, in turn Av3ar IT Ops can perform the automated orchestration of the tasks. Av3ar also integrates with variety of 3rd party tools including Ticketing systems, ERP systems, ITSM tools, etc.

Key Use cases of Av3ar

IT Infrastructure Management

A Virtual System Administrator that understands customer requirement and manages their IT Infrastructure from various perspectives as follows.

- Server Management

- Database Management

- Virtualization and Cloud Management

- Storage / Backup Management

- Network and Security Management

- Windows / Unix / Linux / Mainframe Management

- AD / Exchange Management

Service Desk Management

Av3ar brings advanced artificial intelligence (AI) to Service Desk area and other interactive operations by engaging users in more intuitive and natural conversations through Chat.

Typical Service Desk activities are handled interactively by Av3ar such as,

- Day-to-day mundane tasks that are repetitive by nature with definite rules defined.

- IT Processes that are handled which are having same pattern of activities where there are multiple relative tasks are involved.

- L1 Helpdesk issues that do not require any external entities to get involved.

GUI Management

Any task that requires to be managed through the GUI in any application interface which is part of the task or the use case, Av3ar works like a human being to access the UI to perform the required orchestration without any human intervention. There are different types of interfaces that Av3ar manages such as local Windows application, Web Interface, Windows Farm, etc. Av3ar understands the objects available on the page and manages the orchestration even in situations when the position of objects change or monitor resolution changes intelligently.

Other Interesting Attributes of Av3ar

- Responsive to Human Emotions with an empathy.

- Multiple Av3ar Virtual Assistant personalities with appropriate skill levels.

- Escalations to human agents if a problem is not resolved by itself.

Av3ar Dashboard

The dashboard interface provides a consolidated summary view of all the iBOTs handling different towers and their statistics in ral-time.
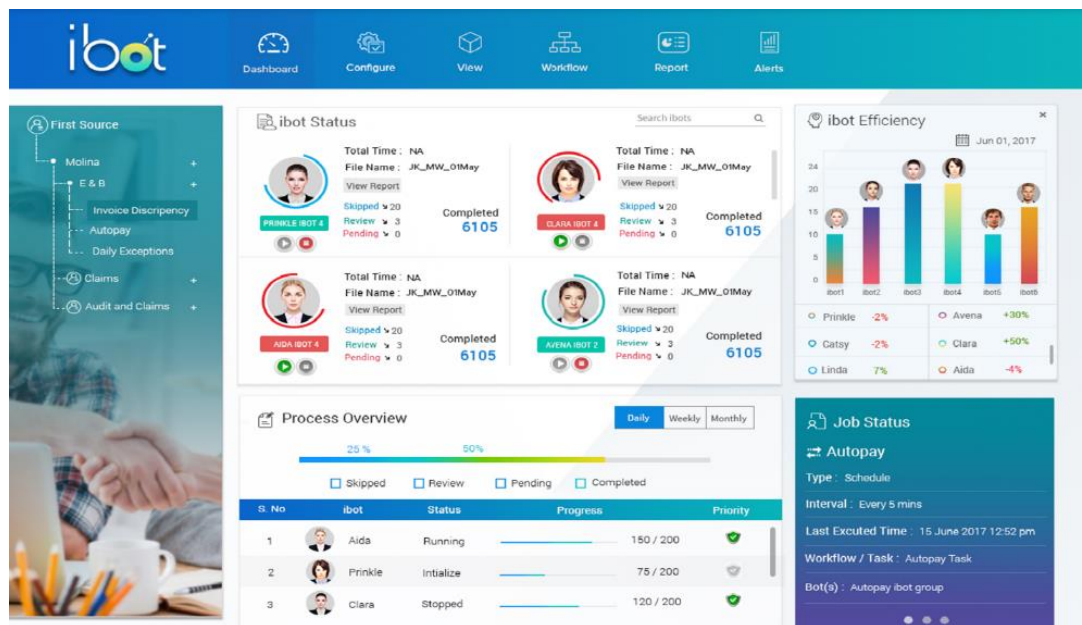
Users can pull out a report from Av3ar IT Ops software for reviews and sharing with different teams for different analytical purposes.

Key Features of Av3ar IT Ops Environment

- Av3ar IT Ops is designed to support multi-environment deployment such as development, testing/staging, Production & DR sites.

- Av3ar IT Ops is capable of supporting centralized release Management process which supports seamless rollback

- Av3ar IT Ops has a design in a non-invasive way & it is code free.

- Av3ar IT Ops has incorporated workflow based orchestration which is re-usable among multiple processes.

- Av3ar IT Ops is able to emulate human behavior such as logging in, working on application, data entry, data uploading, data processing, report generation, report formatting, report/ output data downloading, logging off.

- Av3ar IT Ops is capable of integrating multiple applications in both simultaneous & sequential flow (i.e. Multi-tasking where one or more automations can occur simultaneously with the user performing other tasks. Solution is able to allow the user to work in one application simultaneously with automations running against the same and other applications).

- Av3ar IT Ops is capable of performing Screen Scraping/ Screen emulator to read data from screen (pixel basis or tagging), It also is capable of supporting OCR / QR code to use as input data and convert the same into digital data for further processing and UI automation.

- Av3ar IT Ops has an in-built facility to record each and every step of the process on screen and replay the same like human and should also have the ability to track any dependencies as well.

- Av3ar IT Ops possesses the capability of localizing formats like Date, Time, decimals, currency, number, parameter separators, symbols etc.

- Av3ar IT Ops does have a solution for User Management, Password management, password masking and the complexities for the same is configurable.

- Av3ar IT Ops has mechanisms to connect to various applications using proper user id and passwords for those applications.

- Av3ar IT Ops does have a facility of drag-and-drop based development interface preferred for easy construction of workflows.

- Av3ar IT Ops performs Codeless Application Integration that requires no changes to applications or access to source code.

- Av3ar IT Ops supports Multi-threaded automation engine including scenarios when user is actively interacting with other apps.

- Av3ar IT Ops supports Non-positional, deterministic object matching and should allow flexible, configurable match business rules.

- Av3ar IT Ops supports exception handling i.e. be able to detect that expected objects are missing and take the appropriate action and continue running otherwise.

- Av3ar IT Ops supports web and other applications that can be scrolled and re-sized, or zoom and font sizes can change dynamically.

- Av3ar IT Ops does have the ability to detect radio button and checkbox selections and state changes as well as the current state on an application page where the process is being executed.

- Av3ar IT Ops has the ability to read and manipulate tabular/grid data (i.e. Excel spreadsheets, data grids, web tables), determine number of rows and iterate through the data, providing the ability to both read and update the data cells, accessing both visible and non-visible portions of the grid without having to scroll or block the user from performing other tasks simultaneously.

- Av3ar IT Ops is designed to perform automated orchestration based on event-driven / time-driven alerts including clicking buttons, invoking menu & selection, cursor & mouse selection, use minimal CPU (no impact on performance).

- Av3ar IT Ops does have the capability to perform back office functions for Business Intelligence reports (standard & ad-hoc reports), automate the business process executions for SLR, Trial Balance, Bill Register, E-mail, SMS, RA&FMS and DQ at the DR site.

- Av3ar IT Ops provides high security to ensure that only authenticated and authorized users may use functions they have been authorized for. The solution must fulfill all the security guidelines and mandatory federal data protection guidelines & laws for operating with sensible person related customer data.

- Av3ar IT Ops has the ability to change or move data (i.e. copy/paste) in applications without "pumping keystrokes" into the application or changing focus of where the current user is working. Solution should not work by saving current focus or cursor location, blocking user input while running the automation, then returning focus and mouse to the saved location.

- Av3ar IT Ops does have the ability to detect and log changes to any and all fields of an application without physically defining each field and each position or location of field, and without polling. It automatically detects and react distinctly to many attributes & events.

Av3ar IT Ops deployment Requirements

Infrastructure Hardware Requirements

Av3ar Servers - 3 Nos

- Av3ar Application Server- Qty-1
- Av3ar Context Server- Qty-1
- Av3ar Application Database Server:- Qty-1
- Av3ar iBOT client - 50

Av3ar Application Server

Physical / Virtual Server Machine with following configuration

- 2.4 GHz with Octa Core processors
- 64 Gigabyte RAM
- 500 GB Hard drive.

Software Requirement [on the Application server]

- Windows Server 2012 /2016 Standard/Datacenter Edition
- Mozilla Browser
- .NET Framework 4.5
- IIS server 7.0 or above services installed
- MySQL Workbench 6.16

Av3ar Context Server

- 2.4 GHz with Quad Core processors
- 64 GB RAM
- 100 GB HDD

Software Requirement [on the Context server]

- Ubuntu 14.04 Operating system Standard/Enterprise
- Apache server 2.4
- Python 3

Av3ar Application Database Server:

- GHz with Quad Core processors
- 64 GB RAM
- 100 GB HDD

Database

- Remote My-SQL database version 5.6 with port 3306 enabled
- Should be hosted on separate Windows or Linux Server

Av3ar iBot:

Hardware Configuration

Physical / Virtual desktop with following configuration.

- Dual Core CPU
- 8 GB RAM
- 50 GB HDD

Software Configuration

- Windows 7/8/10 64bit with Sp1 desktop or Windows Server OS
- MS Excel 2010 or above
- .NET 4.5
- MySQL Workbench 6.16 (will be installed and configured by Perpetuuiti)
- Java Runtime 1.7 to run Av3ar Agent on Av3ar Client machines.

The Ports Requirement

The following are the port requirements that need to be opened between Source (Server/Desktop) and Destination (Server/Desktop):

	Source	Target	Port Number	Direction (Uni-Direction / Bi-Direction)
1	Av3ar App Server	Context Server	22, 50000, 50001, 50002, 50003, 50004, 50005, 50006	Bi-Directional
2	Av3ar App Server	Av3ar DB Server	3306	Bi-Directional
3	Av3ar App Server	iBot Client System	80	Bi-Directional
			7222	Bi-Directional
			100	Bi-Directional
4	*Av3ar App Server	Arcos Server	22	
5	Context Server	Av3ar DB Server	3306	Bi-Directional
6	Context Server	Av3ar App Server	50000, 50001, 50002, 50003, 50004, 50005, 50006	Bi-Directional
7	iBot Client System	Remote Desktop/Server	5985	Uni-Directional
			22	Uni-Directional
			8347	Uni-Directional
			100	Uni-Directional

8	iBot Client System	Av3ar DB Server	3306	Bi-Directional
9	Av3ar App Server	ITSM Tool (BMC REMEDY)	443	Bi-Directional
10	Av3ar App Server	Email Server	25	Uni-Directional
11	Av3ar App Server	Remote Desktop/Server	100	Uni-Directional

Product Compatibility

Av3ar IT Ops software supports the following technology tiers to perform automation to manage the IT Infrastructure.

1. Physical platforms including Windows, RHEL, Ubuntu, AIX, Solaris, HP-UX, A400, z/OS.
2. Virtual platforms including VMWare, Hyper-V, KVM
3. CLOUD platforms including AWS, Azure, Google, OCI
4. HCI platforms including CISCO, DELL, HP, Nutanix
5. Microservices platforms including Docker, Kubernetes
6. Databases including Oracle, MSSQL, DB2, MySQL, PostgreSQL, SAP HANA, MongoDB, Sybase, etc.
7. Storage platforms including HP, Hitachi, IBM, EMC/DELL, NetApps
8. Support for Java, .Net, based and also web based applications
9. Support for Application environment like Windows Apps, Java Apps, Web Apps, Enterprise-wide Data Warehouse solutions, SAP CRM, Base24 Switch, Microsoft ADS, CustomerXP FRM solution, MS Office applications (doc, docx, xls, xlsx, ppt, pptx, open format), PDF, MS Outlook/Outlook Web, Databases like Oracle / SQL Server / MySQL etc.