Data Center Automation

Accelerate cost-efficient, secure IT infrastructure services with out-of-the-box Automated, consistent, and secure—patching, regulatory compliance, and provisioning on a modern containerized infrastructure. Proven capability managing enterprise scale infrastructure of more than 100k nodes across multi-vendor physical and virtual servers, databases, and middleware.

Key Features

For a complete list of supported devices, systems, and applications please visit:
Data Center Automation Documentation

Policy-Based Patching of Servers, Databases, and Middleware

Dynamic Patching with Exception Management. Unlike static patching, dynamic patching is an implicit list of patches based on vendor recommendations. Vendor recommended patches are always changing. Dynamic patch policies are much easier to maintain compared to manually creating explicit lists of static patches. Patching dynamically ensures you are always patching based on the latest needed patches. DCA queries the vendor specific update utilities on the target resource to determine which patches should be applied. Patch exceptions can be configured to ignore desired patches, e.g., low risk patches on critical infrastructure. Service Level Objectives and maintenance schedules ensure patches are applied within a defined frequency and occur within scheduled maintenance windows.

Patch Operating System (OS). Individual patches can be downloaded directly from the vendor or imported in multiple formats e.g. exe, tar, zip, and more. Create custom patch policies of various types e.g. recommended, critical, etc. for various operating systems such as Windows, RHEL, SOLARIS, and more. Attach desired patches to the policy and assign policies to individual resources or resource groups. Patch remediation can be scheduled with ongoing Service Level Objectives (SLO) or run ad hoc. View a full patch history for resources by policy or individual patches applied.

Patch Database (DB) and Middleware (MW). OOTB workflows for patching of DB and MW e.g. Oracle, JBoss, Apache, etc. can be customized with the workflow design studio. Patch deployment can be scheduled with Service Level Objectives (SLO) or run ad hoc. Patches may also be rolled back using orchestration workflows.

Risk Dashboard. The risk dashboard uses Common Vulnerability Exposure (CVE) data imported from the NVD database to identify patching vulnerabilities across the IT infrastructure. Resources are evaluated for exposure to all known CVEs and results are displayed on the dashboard in various sections. The dashboard can be customized to show statistics including weekly impact trends and number of affected resources for vulnerabilities of particular interest. Other areas show key information such as most recent vulnerabilities and affected resources, overall resource count by vulnerability status, resource type and count by CVE severity e.g. 55 critical CVEs on RHEL resources, and vulnerabilities by age e.g. 14 resources have had an ongoing critical exposure for a period greater than one year.

Agent and agentless operation. Patch resources using agent or agentless based communication.

Key Benefits

- Automate cross-silo, patching, compliance, and provisioning to achieve high-quality, repeatable and reliable processes; eliminate errors and hand-offs between technology silos
- Detect and remediate vulnerability and compliance risks proactively across the data center; eliminate inconsistent patching, intermittent compliance, and meet Service Level Objectives
- Standardize provisioning across multi-vendor servers and application infrastructure; eliminate error prone manual tasks
- Business value: reduce cost of IT operations, accelerate service delivery, reduce risk

Ongoing Policy Based Regulatory Compliance Audit and Remediation for Servers, Databases, and Middleware

Ongoing, policy based compliance. Service level objectives (SLO) are defined for each compliance policy. SLO sets a frequency objective for audit and/or remediation jobs e.g. daily, weekly, or monthly. Maintenance schedules are created for resource groups to establish the time period in which these jobs will be run i.e. Sunday between 12:00am and 6:00am.

Out-of-the-box (OOTB) compliance audit and remediation content. Pre-built compliance content e.g. (CIS, PCI, DSS, SOX, ISO 27001, FISMA, HIPAA, NERC, and DISA), compliant deployment templates, and remediation content. Create custom benchmarks and policies or modify existing content. Policies can contain benchmarks for mixed resource types (e.g. OS, databases, and middleware) and can be applied to a resource group containing multiple resource types.

Compliant deployments. Deploy compliant resources e.g. CIS compliant RHEL, Oracle, and more. Resources are provisioned with OS or Database templates designed to be compliant at time of deployment.

Puppet integration. DCA discovers Puppet managed nodes by communicating with a Puppet Master. Once Puppet nodes are discovered, DCA discovers OS, DB, and MW resources on the nodes. Compliance and patching can be performed on these resources, leveraging the full capability of DCA. Quickly identify Puppet managed resources on DCA dashboards and resource lists.

Compliance reporting. Obtain compliance reports via dashboards available for resource groups, individual resources, and policies. Observe key details on compliance such as compliance status (within or outside of SLO) and identification of failed benchmarks by severity. Overall Infrastructure compliance statistics and metrics are available from the central dashboard.

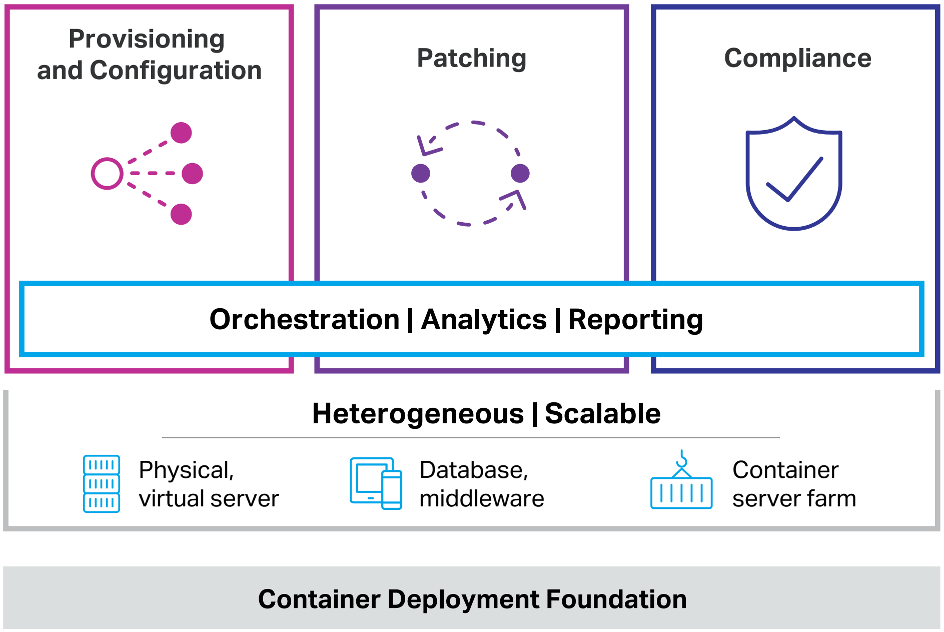


Figure 1. Micro Focus DCA framework

Drill into the dashboard for more detailed information including benchmark and resource identification. Customizable detailed and summary compliance reports are also available in PDF format.

Agent and agentless operation. Run compliance audit and remediation jobs on resources using agent or agentless based communication.

Provisioning and Configuration of Servers, Databases, and Middleware

Configure a build plan. Out-of-the-box customizable build plans for OS, database, and middleware including *but not limited to*: RHEL, Solaris, Windows, CentOS, Ubuntu, ESXi, MSSQL, ORACLE, Apache Web Server, Jboss, Websphere, and Tomcat Web Server. Build plans can be customized to include advanced configurations such as RAID and BIOS settings. Configure custom scripts to be run at time of build to further customize deployments. All provisioning can be scheduled or run ad hoc.

Provision bare metal. Bare metal servers can be provisioned using a PXE boot process. Servers are PXE booted and brought under management using an agent. The customizable build plan plan is then deployed which installs the desired OS.

Provision virtual servers. View an inventory of unmanaged VMware vCenter and Microsoft SCVMM VMs. OS build plans can be configured to create a VM from a template. When an OS build plan is deployed the selected servers are brought under management and the desired OS is installed.

Provision database (DB) and middleware (MW). Deploy DB and MW workflows to perform tasks such as: database/middleware provisioning (binaries, instances, and database configuration), DB upgrades, DB migration to a new server, DB utilities (Start/stop instance), and DB and MW code release. Automate tasks including deployment of MSSQL clusters or Tomcat Web Server.

Provision container server farms. Provision Docker-based Kubernetes clusters. Out-of-the-box customizable provisioning templates for Kubernetes/Docker clusters are used to deploy completely configured container infrastructure. Worker nodes can be provisioned and pointed to a selected master.

Process Orchestration

Orchestration workflows. Thousands of OOTB workflows are provided to perform orchestrated tasks across the datacenter for servers, database, and middleware.

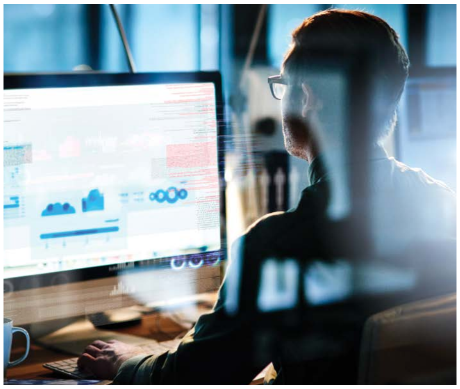
Orchestrate any provision, patch, or compliance process. Integrate with 3rd party tools and existing content by creating workflows that invoke vendor APIs (SOAP, REST, PowerShell, etc.) or open source scripts. Run orchestration workflows using the UI or the open APIs.

Create and debug workflows. Create or modify workflows using the drag and drop workflow studio. Workflows are created with variable placeholders for parameter inputs (credentials, IPs, etc.) to be highly reusable. Debug and test workflows in the studio before placing them into production.

Containerized Suite Deployment Option

Container Deployment Foundation (CDF) is the foundation required to install the new containerized version of DCA. CDF has a simple install process and once installed handles all provisioning, orchestration, and management of the underlying core Kubernetes/Docker cluster infrastructure. The CDF UI is a single portal used for DCA suite and CDF platform management tasks such as installs or upgrades.

DCA suite management. Monitor job queues and check the health and status of individual service pods from the analytics dashboard. Debug issues by viewing log files and configuration files from the UI. Create and manage suite namespaces and perform other suite configuration tasks including installs and upgrades.



High Availability (HA) PostgreSQL clustered databases. The DCA suite on CDF uses an embedded HA PostgreSQL cluster which provides resiliency and increased performance capacity. In the event any one pod per PostgreSQL cluster fails, DCA services will continue to run without disruption.

Scale horizontally. Easily scale DCA for greater resource capacity by adding new Kubernetes worker nodes and/or configuring multiple master nodes. Worker nodes can be added from the CDF UI. Once credentials are provided for the new worker node, CDF installs Kubernetes/Docker on the node. When CDF completes the provisioning of the new worker node it is added to the cluster and begins to accept workloads from the master.

Headless Operation. Because CDF is built on open APIs, any DCA on CDF feature is available using RESTful APIs. These APIs enable the full capacity of DCA to be leveraged from any technology capable of consuming an API.

ChatOps Collaboration

Collaborate with systems and teams. A Slack channel can be used to run DCA compliance commands or retrieve compliance information in the channel. Users are authenticated against the DCA IDM using HuBot Enterprise to ensure that the slack user has the required permissions to execute the command requested. Invite other team members to participate in diagnosis and remediation of compliance issues in a conversation-like manner. Obtain resource group compliance status and information, watch resources for a change in compliance status, and remediate non-compliance issues from the slack channel.

Virtualized Infrastructure Optimization

Performance statistics. View performance, utilization, and capacity of virtual environments. Quickly identify wastage and reduce sprawl caused by idle or oversized VMs.

Infrastructure planning. Best-fit placement suggestions for new workloads help determine where a new VM can be provisioned and how the environment should be sized based on historical usage trends and available capacity.

Forecast Reports. Forecast reports use historical consumption and performance data trends to determine the number of days until the resource will reach capacity.

New Features

- Containerized suite deployment option
- Service Level Objective (SLO) policy based dynamic patching and regulatory compliance
- Puppet Integration
- Dynamic patching with exception management
- CVE Risk Dashboard
- Compliance Dashboards
- Deployment of Docker-based Kubernetes clusters
- APIs for headless operations
- High Availability (HA) with PostgreSQL clustered databases
- ChatOps collaboration tool

System Requirements[1]

DCA on CDF Minimum Hardware Requirements

- (1 DCA Server) 8 CPU / 32 GB RAM / 200 GB HDD
- (1 NFS Server) 4 CPU / 8 GB RAM / 100 GB HDD

DCA on CDF Recommended Hardware Requirements

- (1 DCA Server) 4 CPU / 16 GB RAM / 100 GB HDD
- (2 Worker Nodes) 4 CPU / 16 GB RAM / 100 GB HDD
- (1 NFS Server) 4 CPU / 8 GB RAM / 100 GB HDD

Operating Systems

- RHEL x86_64 (ver 7.3)
- Oracle Enterprise Linux x86_64 (ver 7.3)
- CentOS x86_64 (ver 7.3)

Languages

- Localization is not supported in DCA

High Availability

- To provide high availability of components, Kubernetes is used in the DCA infrastructure layers.

Contact us at:
www.microfocus.com

	Express Provisioning and configuration	**Premium** Patching, compliance and remediation	**Ultimate** Infrastructure optimization
Provisioning			
Server Discovery, Config, OS Provisioning and SW Deployment[2]	X	X	X
Database and Middleware Discovery, Config and Deployment	X	X	X
Infrastructure[3] LCM with Runbook Automation and Reporting	X	X	X
Compliance			
Patching for Server OS and Applications		X	X
Server Compliance, Audit and Remediation (+subscription content)		X	X
Database and Middleware Patching and Code release		X	X
Database and Middleware Compliance, Audit and Remediation (+subscription content)		X	X
Database and Middleware Upgrades and Migrations		X	X
Optimization			
Server Infrastructure Analytics			X
Virtual Infrastructure Capacity and Optimization			X
Planning and Forecasting			X

Figure 2. Three editions to meet infrastructure management needs

[1] *Other DCA suite products, and classic install products have different requirements. For a full list of requirements including network and tuning please see product documentation.*

[2] *Capability for clustered DB/MW instances offered in DCA Premium.*

[3] *Infrastructure includes Servers (Physical or Virtual), Database & Middleware, no platform or scale restrictions.*