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

Automated Policy-Based Operating System, Database, and Middleware Patching

Patch Policies. Perform automated patch vulnerability scan and remediation using patch policies. Policies contain measurement and remediation Service Level Objectives and patch bundles. Service Level Objectives define the frequency for automated scan and remediation actions while resource group maintenance schedules define the windows when the jobs can be run. Resource groups are subscribed to policies, with the ability to create patch exceptions for individual resources in a group. Resource patch bundles contain information about types of patches, i.e. vendor recommended or an explicit list of patches. When a resource is scanned ad hoc or based on policy requirements, needed patches are displayed on resource dashboards along with any corresponding CVSS score. Remediation SLO will ensure resources remain compliant with patch policies.

Static Patching. Individual patches can be downloaded directly from the vendor or imported in multiple formats e.g. exe, tar, zip, and more. Patches can also be applied using vendor specific patching infrastructure and local repositories. Create custom patch policies of various types e.g. recommended, critical, etc. for various operating systems, database, and middleware such as Windows, RHEL, SOLARIS, Oracle, JBoss, Apache, and more. When adding patches to a patch policy, patch filters allow sorting of patches based on patch release date, CVSS, and more.

Dynamic Patching. Unlike static patching, dynamic patching only installs required patches. DCA queries the vendor specific update utilities on the target resource to determine which patches should be applied based on vendor recommendations.

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

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

Needed Patches

<table>
<thead>
<tr>
<th>Severity</th>
<th>Critical</th>
<th>High</th>
<th>Low</th>
<th>Medium</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>10</td>
<td>9</td>
<td>3</td>
<td>15</td>
<td>198</td>
</tr>
</tbody>
</table>

Figure 1. The vulnerability risk dashboard shows patch and CVE vulnerabilities across the datacenter

Figure 2. Resource dashboard showing needed patches with corresponding CVSS severity
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.

**Automated Policy Based Regulatory Compliance Scan 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 scan 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 using DCA deployment templates. Resources are provisioned with OS or Database templates designed to be compliant at time of deployment.

**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. 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.

**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
DCA uses out-of-the-box orchestration workflows to perform DCA operations on managed multi-vendor OS, DB, and MW. Orchestration flows can be customized or created to automate any processes in relation to the provision, patch, and compliance lifecycle of a resource. Integrate with 3rd party tools and existing content using hooks in the compliance workflows that invoke vendor APIs (SOAP, REST, PowerShell, etc.) or open source scripts, e.g. create a workflow that updates a service management ticket when a compliance or provisioning operation is performed on a particular resource or resource type.

DCA Containerized 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.

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.

Mixed mode operation. Containerized DCA manages mixed mode deployments on agentless and agent based resources in the datacenter. Agent based operations are performed using existing agent based infrastructure such as Server Automation or Puppet. Agentless resources can also be imported directly into DCA using orchestration workflows.

Puppet and Server Automation integration. After a Puppet Integration is configured, DCA discovers Puppet managed nodes by communicating with a Puppet Master. DCA can also be integrated with Server Automation to discover resources and resource groups under SA management. Once resources are discovered, DCA discovers OS, DB, and MW deployed on the discovered resources. DCA operations can be performed on these resources, leveraging the full capability of DCA. Quickly identify Puppet and SA managed resources on DCA dashboards and resource lists.

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

New Features

- Containerized DCA deployment option
- Perform compliance and patching on Puppet managed infrastructure with Puppet integration
- Dynamic and Static policy based patching with Service Level Objectives and exception management
- Patch vulnerability risk dashboard with CVE information
- Regulatory compliance dashboards
- Deployment of Docker-based Kubernetes clusters
- APIs to perform all DCA functions
- High Availability (HA) with PostgreSQL clustered databases
- ChatOps collaboration tool
- Orchestrate additional processes into patch, compliance, and provisioning processes using orchestration workflow hooks
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.

---

<table>
<thead>
<tr>
<th>Provisioning</th>
<th>Express Provisioning and configuration</th>
<th>Premium Patching, compliance and remediation</th>
<th>Ultimate Infrastructure optimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Discovery, Config, OS Provisioning and SW Deployment</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Database and Middleware Discovery, Config and Deployment</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Infrastructure LCM with Runbook Automation and Reporting</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compliance</th>
<th>Patching for Server OS and Applications</th>
<th>+subscription content</th>
<th>X</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Compliance, Audit and Remediation</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database and Middleware Patching and Code release</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database and Middleware Compliance, Audit and Remediation</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database and Middleware Upgrades and Migrations</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Optimization | | |
|-------------|-------------------|
| Server Infrastructure Analytics | X |
| Virtual Infrastructure Capacity and Optimization | X |
| Planning and Forecasting | X |

**Figure 5.** Three editions to meet infrastructure management needs

**Configuration Sizing**

<table>
<thead>
<tr>
<th>DCA Master Nodes</th>
<th>DCA Worker Nodes (worker/master)</th>
<th>NFS Server Specs</th>
<th>No. Managed Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic configuration</td>
<td>8 CPU / 48 GB RAM / 200 GB HDD</td>
<td>4 CPU / 8 GB RAM / 100 GB HDD</td>
<td>50</td>
</tr>
<tr>
<td>Number of servers: 1</td>
<td>Number of servers: 1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Recommended configuration | 8 CPU / 24 GB RAM / 100 GB HDD | 4 CPU / 8 GB RAM / 100 GB HDD | 200 |
| Number of servers: 1 | Number of servers: 1 |

| Large scale, HA configuration | 4 CPU / 16 GB RAM / 100 GB HDD | 4 CPU / 8 GB RAM / 200 GB HDD | 15,000 |
| Number of servers: 3 | Number of servers: 1 |

Recommended to use RAID 10 for HDD. DCA hosts and NFS server should be connected through a 1 GBPS network backbone and should have a minimum of 100 MBPS network throughput between the servers.

To provide high availability to its components, DCA uses Kubernetes in its infrastructure layers.

---

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.

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

Learn More At microfocus.com/DCA