

EMC ControlCenter 6.1 Expands Cross-Domain Resource Management

July 2008



The enterprise storage environment is getting more and more challenging to control thanks to multiplying storage resources, ever-expanding data to protect and manage, and the sheer scope of the servers and applications that depend on networked storage. A critical toolset for managing this challenging environment is Resource Management and its subset Storage Resource Management (SRM), which enables administrators to visualize and control storage resources and their relationships and dependencies. However, the virtualized network is a large fly in the SRM ointment. When server virtualization is introduced into the stack, the server-to-storage dependency trail is broken and traditional SRM is crippled. The IT administrator can manage the virtual servers using VMware ESX tools, but cannot use the enterprise SRM to even discover where the virtualized server data is, let alone to visualize it along with the rest of the data center storage domains.

For a Storage Resource Management toolset to work reliably across the enterprise, it must integrate virtual and physical resource management while protecting the layers of security that IT has erected to safeguard the environment. Ideally it should also be a part of a comprehensive Resource Management tool that can cross storage, server and networking domains to provide fully integrated cross-domain intelligence.

EMC ControlCenter is the extensive SRM piece of EMC's initiative for Cross-Domain Resource Management for virtualized and physical environments. ControlCenter 6.1 expands its ability to provision fast-growing virtual networks with improved troubleshooting, monitoring and reporting tools. This Product Profile will review EMC's ControlCenter 6.1 upgrade and its role in Cross-Domain Resource Management.

The Challenge of Resource Management

When the data center is bursting at the seams with storage, server, applications, and networking resources of all types, managing these resources gets progressively harder. This is where cross-domain Resource Management shines by allowing IT to gain a unified perspective and control across multi-vendor SANs. For example, Resource

Management presents clear views of dependencies that allow IT to accurately forecast the effect changes would have to the entire infrastructure. It also visualizes and remediates bad-acting physical and virtual resources across multiple domains, while root cause analysis provides actionable intelligence to administrators.

However, the ability to successfully manage data center resources across types and

P R O D U C T P R O F I L E

domains has been hampered by four major challenges: the lack of common semantic models, limited root cause analysis, inadequate relationship mapping, and poor business visibility.

1. *Lack of common semantic models.* A common semantic model assigns consistent definitions across a set of elements. This allows much greater communication between previously unrelated component sets and enables the same management tools to run across different domains. Without a common model, management tools are restricted to silos and narrow stacks that cannot share valuable information. Individual domains and components stay fragmented and discrete. The cost of management remains high, comprehensive views are difficult to produce, and automation and scalability suffer.
2. *Limited analysis.* Manual or inadequate software-based analyses cannot yield an accurate picture of the data center. Detailed, automated analysis produces an accurate picture of the data center infrastructure, while root cause analysis solves looming threats with actionable intelligence.
3. *Inadequate application mapping.* Mapping application dependencies across storage, servers and networks produces centralized and real-time views of cross-domain dependencies. Manual mapping is difficult to impossible in complex environments, as dependencies rise from multiple applications and a spider-like

web of connections between applications, server and devices. Add logical and virtualization layers to dependencies and manual mapping becomes virtually impossible across a complex data center.

4. *Poor business visibility.* Visibility at the business level allows IT to serve business strategy. Lacking this visibility threatens compliance, SLAs, and IT-business alignment. Visibility is lacking more often than not because of the silo—centric nature of traditional infrastructure views, making it impossible to see a comprehensive and holistic view of information.

The Big Picture: EMC's Resource Management Strategy

EMC sees the data center's lack of Cross-domain Resource Management as a major pain point. As this vendor is doing with its backup and archiving product line, EMC is busily integrating individual Resource Management products into a cross-domain strategy for an integrated, service-centered approach.

EMC has integrated several software packages for Resource Management capability including EMC ControlCenter 6.1, Smarts Service Assurance Manager and IP Management Suites, Application Discovery Manager, and Storage Insight. Put together these tools are greater than the sum of their parts, and as a strategy will serve data center management and consolidation, ITIL and CMDB process automation, next-generation networks (NGN) service delivery and tiered storage management.

P R O D U C T P R O F I L E

- **Model-based.** EMC bases its resource management capabilities on behavioral and relational models rather than discrete components. Resource Management routines reference these models across the infrastructure, creating a unified management fabric for cross-domain, service-centered management. The modeling technology is largely built on EMC's recent acquisitions of Smarts for software management and nLayers for application discovery.
- **Automatic analysis and root cause.** Automating analysis is crucial in the complex data center. EMC's cross-domain analysis and root cause technology use common models to correlate events and to drive incident management and impact analysis, all in real time. If a model is threatened, analysis produces actionable threat intelligence for users.
- **Application dependency mapping.** EMC put the nLayers agentless appliance to good use. nLayers technology is based on Application Behavior Modeling (ABM) that continuously and passively discovers and monitors application components, resource dependencies, service levels and usage within data centers. In its EMC Smarts incarnation, the technology operates across multiple domains, which enables cross-domain automation to drive important initiatives and operations like ITIL and incident management.
- **Business level visibility.** Real-time visibility into business processes enables IT to visualize and track compliance, end-to-

end service quality, and dynamic IT-business alignment. EMC developed their business level views independently of individual silos. Cross-domain intelligence posts into a centralized interface and allows drill-down to deepening levels of business-focused detail.

ControlCenter 6.1

ControlCenter 6.1 occupies an important place in EMC's Resource Management strategy. Paired with EMC Storage Insight, ControlCenter provides SRM capabilities of discovery, monitoring, reporting and provisioning to VMware ESX environments as well as physical and mixed environments.

ControlCenter and Virtual Networks

Managing the flow of data on virtual networks can be extremely challenging. ControlCenter 6.1 makes real strides in provisioning and managing virtual storage by providing a new level of visibility from the physical disk up to virtual machine clusters. This enables IT to trace the flow of applications and data from physical to logical servers and storage, and to monitor the performance of the virtual devices.

As part of this significant release, EMC introduced Virtual Provisioning for Symmetrix DMX-3 and DMX-4. Virtual Provisioning is EMC's implementation of thin provisioning for virtual networks, and is a major new capability in ControlCenter 6.1. Virtual Provisioning enables simplified array management and improved utilization, leading to efficient storage tiering.

P R O D U C T P R O F I L E

Virtual Provisioning works by presenting an application with more capacity than is physically available on disk. Many applications prefer to have maximum capacity allocations, but this fills up large portions of disk with unusable sectors that the application may or may not use. Virtual Provisioning presents the application's preferred allocation while in fact only allocating a fraction of the storage tracks on physical disk. Capacity can be dynamically assigned as the application's actual space needs grow. This results in simple and fast provisioning, which in turn greatly eases data layout and growth. ControlCenter provides for comprehensive monitoring, reporting, and automated provisioning along with local and remote replication.

Virtual Provisioning's top layer is called a thin device and consists of the application's perceived allocated capacity. The physical capacity is only those storage tracks which the application has physically used and the additional allocation is virtual. Underlying the thin devices are "data devices" that form storage pools for allocation. These data devices are in fact virtualized storage that is automatically striped across multiple spindles to increase performance. They create thin storage pools that Virtual Provisioning dynamically assigns to thin devices. Like physical drives, each data device can be independently managed, is assigned RAID schemes, is visible to the host and has the same numbering scheme as standard storage devices. Thin pools can coexist with standard storage.

Virtual Provisioning preserves logical relationships to physical devices, enabling

EMC SAN Manager to display relationships between host devices, thin devices, storage pools, and data devices; and to link them to the standard physical environment as well. This results in a simplified virtual architecture that dynamically and predictably accommodates application growth. Performance Manager enables administrators to monitor the thin devices while StorageScope allows them to proactively monitor the capacity on the physical storage devices and pools.

The ControlCenter 6.1 interface also allows administrators to view properties, capacity, and usage information for an ESX Server and corresponding virtual machines (VMs). It can discover and report on individual VMware guest names, OS versions, and IP addresses and can report the capacity, utilization, and trending. Properties View displays a VM's properties and allows administrators to view selected objects' most common attributes, including configuration. Relationship View maps logical relationships of VMware guests and hosts to storage topology views, and *Free Space View* visualizes both free and allocated space on storage arrays that are related to a selected VMware server. Administrators can view details on HBAs, ports, devices and storage pools.

EMC ControlCenter Security

In addition to comprehensive virtual provisioning and management, ControlCenter 6.1 also integrates new security standards along with RSA key management.

PRODUCT PROFILE

ControlCenter uses secure protocols and RSA technology to safeguard communications. This protects physical and virtual networks against insidious attacks like “man in the middle” message interception, network eavesdropping, malicious code and command injection, and other threat types. Major security elements include:

- **Access control.** ControlCenter security authenticates attempted access against LDAP and Microsoft Active Directories. Discrete controls allow IT to define access by different parameters including managed objects and object groups, active commands, and users and user groups.
- **Data confidentiality and integrity.** RSA technology encrypts all stored and communicated passwords, and also applies digital certificates using BSAFE cryptographic algorithms to all communications between ControlCenter infrastructure components. These components, along with user interfaces and managed objects, communicate over standard and secure communications protocols by default. Protocols include Secure Sockets Layer (SSL), Secure Shell (SSH), and SNMPv3.
- **Logging and Auditing.** Security operations log all command history to the ControlCenter database, and all security-relevant events to the Windows Event log. ControlCenter Trust Manager helps identify and manage trust status between ControlCenter components.

ControlCenter security also provides for ongoing vulnerability identification and

management. EMC continually monitors public disclosers of software vulnerabilities that might impact ControlCenter users, and provides current notification and consistent security updates.

More Reporting with StorageScope

EMC merged StorageScope and StorageScope File Level Reporter for ControlCenter 6.1. The single reporting infrastructure now creates merged reports on files and directories with StorageScope information on servers, storage devices, and arrays. The integrated entity shares a single host and file agent set and uses a single interface to jointly report expanded details of the data center infrastructure. The two also share a single reporting server and a data repository.

StorageScope File Level Reporter generates detailed reports on file sizes and owners, along with most recent modified date and access dates. Armed with this information, administrators are better able to identify duplicate files, reclaim storage capacity, stage data to less expensive disk and compress data files.

StorageScope can also improve operational efficiencies. It can find orphaned storage, identify masked storage as opposed to mapped, and provide a high-level summary of managed resources and objects. StorageScope can also show end-to-end mapping for a VMware ESX server.

- **User interface views.** Web-based views provide high-level information for initial analysis. The StorageScope Dashboard summarizes the entire infrastructure and

PRODUCT PROFILE

allows for customized views. The interface allows for views of the data center and historical trends, and allows for drill-down and filtered views.

- **Built-in reports.** There are twelve built-in reports based on primary use cases and most commonly requested reports. For example, a Hosts report details capacity and usage for all enterprise hosts.
- **Query Builder.** Administrators can build queries with StorageScope, which comes with a wizard-based interface for generating ad-hoc reports. Common queries come with StorageScope, and queries can be modified, copied, and saved for customization. StorageScope can output into multiple settings including XML, PDF, e-mail and others, and administrators can view and expert SQL created by Query Builder.
- **Custom reports.** Users can create and generate customized reports. Users can adjust filtering and report format settings and can schedule both built-in and custom reports based on business requirements,

and the reporting function can accept Crystal Report imports.

- **Repository access.** StorageScope and StorageScope File Level Reporter maintain open access to a centralized reporting repository. This data can be imported into other data stores for advanced reporting.

Taneja Group Opinion

EMC's enterprise storage expertise and their ownership of VMware have given them a head start in resource-managing the complex data center. Expanding ControlCenter 6.1's SRM abilities allows EMC to discover, visualize and manage virtualized server storage as well as physical deployments. And the ability to report on both block and file level storage in a single integrated interface unifies data visualization and management throughout the data center.

Taneja Group applauds EMC for expanding its ability to intelligently and securely manage virtual and physical networks. ControlCenter 6.1 occupies an important place in EMC's highly integrated Cross-domain Resource Management strategy.

NOTICE: The information and product recommendations made by the TANEJA GROUP are based upon public information and sources and may also include personal opinions both of the TANEJA GROUP and others, all of which we believe to be accurate and reliable. However, as market conditions change and not within our control, the information and recommendations are made without warranty of any kind. All product names used and mentioned herein are the trademarks of their respective owners. The TANEJA GROUP, Inc. assumes no responsibility or liability for any damages whatsoever (including incidental, consequential or otherwise), caused by your use of, or reliance upon, the information and recommendations presented herein, nor for any inadvertent errors which may appear in this document.