

Controlling Change: The Missing Ingredient

Many IT organizations are using change management and datacenter automation solutions to automate the approval and implementation processes for change to the IT infrastructure. While this approach provides a solution for in-process change, emergency and ad hoc change are still problematic. Automated change control is the key 3rd ingredient in a complete solution. Change control complements Change Management and Datacenter automation, to maximize in-process change, capture and document all emergency change and eliminate ad hoc change.

Controlling Change

When a failure happens in the IT infrastructure, the first question which gets asked is, "What changed? It was working yesterday." Pro-actively controlling change is a key foundation for scaleable and reliable IT infrastructure. Change can be bucketed into three distinct categories: In-Process, Emergency and Ad hoc. Each one of these categories has very different organizational drivers and characteristics.

	Approved	Documented	Scheduled
In-Process	✓	✓	✓
Emergency	✓	×	×
Ad hoc	×	×	×

	Un-scheduled	Scheduled
Approved	Emergency	In-Process
Un-approved	Adhoc	
	Un-scheduled	Scheduled

Best practice in every organization is to

- Increase the percentage of In-process Change
- Document Emergency Change (who, how, what, when) after the fact
- Eliminate Ad hoc Change

Unless an organization is starting from scratch, controlling change has two distinct challenges: First having a technology platform capable of achieving the above objectives; second a good strategy to align organizational behavior to follow the prescribed process and technology.

Organizations are adopting a three-legged technology platform that includes: A ticketing system; a data center automation system and a change control solution that provide change visibility & policy enforcement solution. Ticketing & data center automation deliver the capability for in-process changes. Change visibility and policy enforcement deliver control for emergency and ad hoc changes.

Aligning organizational behavior is something people are just beginning to grapple with. Organizations have traditionally implemented ticketing systems and change process, followed by an automation or provisioning system and then a change visibility and policy enforcement solution. This approach can generate friction between how things are done today versus the “new” way. Many organizations now find that a better approach is to first gain visibility into change, then implement process and finally apply enforcement of policy. The details behind this approach are the subject of a follow-on brief.

Technology Platform to Control Change

In-process change as the name suggests follows the process defined in the organization to deploy change. Figure 1 below shows the outline of a generic change process. A change is requested by initiating a change ticket (a.k.a request for change /RFC). The change is then approved by a Change Control Board. An approved change is deployed, verified and the ticket is closed.

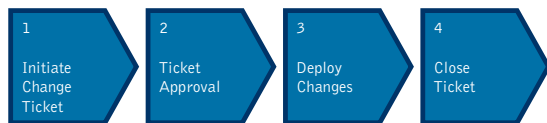


Figure 1: Change Process

Best practice for a change request is to document the content and success criteria of the change in production. The documentation should be generated based on the understanding from the change in the staging or pre-production environment. In addition, the provisioning system used to deploy changes should have a record of what the image will look like after the change is made so it can verify that the change was applied correctly.

Ticketing systems enable organizations to specify their approval processes (step 1 and 2 above), which are often multi-tier and complex. Data Center Automation solutions like help with steps 3 and 4. They help automate the provisioning process and keep a record of deployed changes and current configurations. They also reconcile the changes with the ticketing system.

In large complex environments changes may be made outside Data Center Automation solutions. As shown in Figure 2 there are multiple groups within a company who can update a system: central IT, security, business applications, business logic developers; and often outsourced entities which manage portions of the infrastructure. The tools used to make changes by these organizations are frequently different. Also, multiple agents can update the image or configuration on the machine.

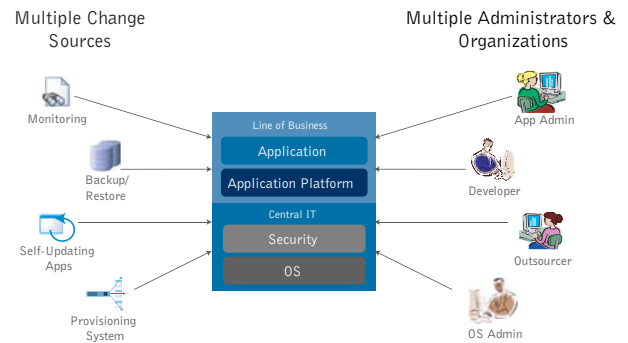


Figure 2: Complex Change Environment

Datacenter Automation solutions can often detect this change. However complete information (who, what, when, how) is not available for these changes.

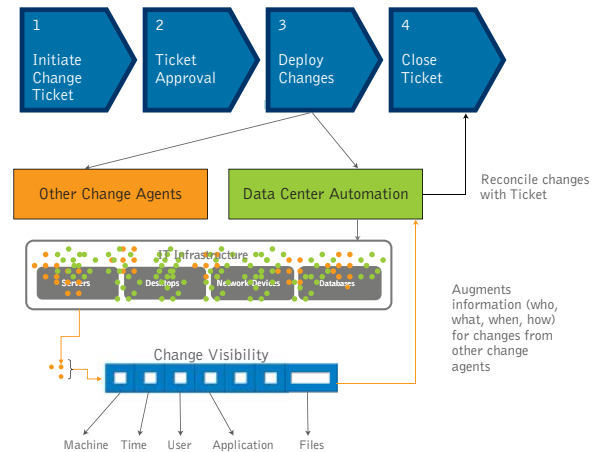


Figure 3: Multiple sources of change in large organizations

Change visibility complements datacenter automation systems to completely track information about changes made outside their control to enable complete and accurate reconciliation. In this manner, ticketing systems, data center automation and change visibility provide a complete solution for in-process changes.

Emergency change happens when a problem occurs in the production infrastructure, when a service is down or a server has crashed. During these events, the highest priority of the IT staff is to restore the service or bring the infrastructure back online. There are several things which need to happen during this time period: First, the problem needs to be identified, typically without access to the server/infrastructure which went down. Second, multiple IT groups each using different management systems may get involved. Once the problem cause is found, actions need to be taken to fix the problem and restore service. In a large majority of the cases the fixes are done by administrators directly logged onto the machine and there is no documentation of what happened to restore the service. Many times, the opportunity of this emergency change process is used to insert changes not related to the problem.

Ticketing systems are not necessarily used during emergency changes, although best practices say that emergency change should be documented. (This documentation is often required by compliance initiatives). Automation solutions like provide partial help as they are able to conduct a scan of the environment later and detect what changed to aid with the documentation of an emergency change.

Change visibility provided in real time greatly augments the capability of the automation solutions in detecting what went wrong.

Figure 4 shows that when a failure happens, the information in the automation solution may not be current. In addition, it may not be possible or timely to resurrect the machine to do a scan once it is down as it may be unavailable or may lack system resources to conduct the scan. Also, in complex environments, change on a DB server may bring down the application server layer, thus it is not clear immediately what needs to be scanned. During emergencies, the time it takes to restore service is critical.

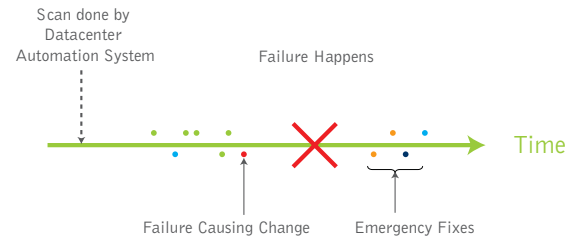


Figure 4 Production Failure

Real time change visibility captures the changes between scans in real time and supplements known configuration information. This eliminates the need to conduct frequent audits and enhances IT's ability to recover rapidly from failures in complex environments.

In addition, when emergency changes are made, real time change visibility captures who is



making the changes so they can be analyzed in a meaningful manner once service has been restored.

Ad hoc change is the Achilles heel of IT organizations. In most IT organizations there are many individuals (central IT, security, line of business IT, developers) who have administrative access to systems. These administrators can inadvertently make changes or "slip in changes" under the radar of the change management process which can cause significant problems down the road.

Change visibility and change policy enforcement can help organizations eliminate ad hoc change. This is done in two steps:

Step 1: Visibility enables everyone to see WHO is making WHAT changes

Visibility enables organizations to attribute responsibility for any change to individuals in the organization. Once administrators know that this visibility is available (i.e. everything is being tracked) there is almost always a dramatic reduction in the number and frequency of ad hoc changes.

Step 2: Ensure change can only happen in accordance with Change Policy

Solidcore can enforce that changes on a system can, for example, only be affected through an authorized datacenter automation system, or can only be made during approved change windows and only if there is a valid and approved change ticket present.

Having the capability to enforce change policy in this manner can completely eliminate ad hoc change. This is vitally important for systems that are “critical change control failure points,” where an inappropriate change presents exceptional business risk to the organization.

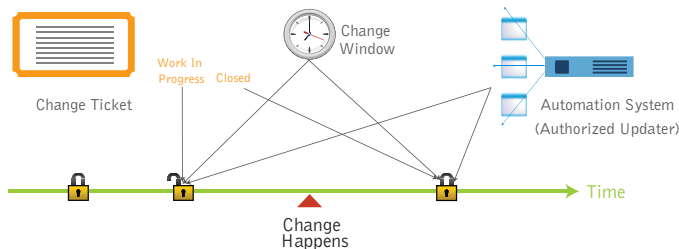
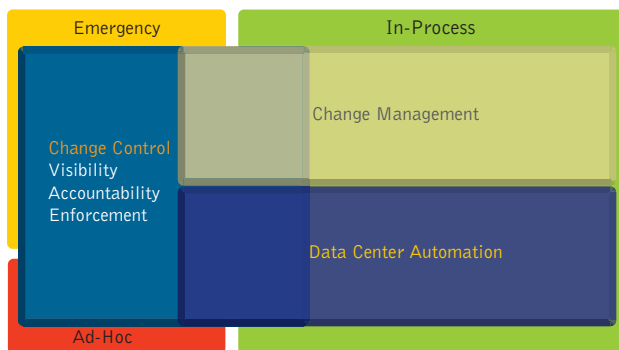


Figure 3 Enforcement enables elimination of Ad hoc Change

Conclusion

Ticketing, Data Center Automation, and Change Visibility and Policy Enforcement provide a complete solution to controlling change in the enterprise. This powerful combination forms the foundation of reliability and scalability and is being adopted by companies all over the world today.



About Solidcore Systems

Solidcore is a leading provider of change control for critical systems. Solidcore’s S3 Control software is the industry’s first and only solution to automate the enforcement of change management policies. Solidcore automatically reconciles infrastructure changes against change tickets, and provides real-time change auditing so enterprises can measure the effectiveness of change management processes and policies. Customers trust Solidcore to improve service availability, implement ITIL initiatives, and lower costs related to Sarbanes-Oxley compliance.

Solidcore also provides change control for embedded systems and is used by major device manufacturers to securely leverage open systems to meet their business requirements.

Solidcore is headquartered in Cupertino, California. For more information, visit www.solidcore.com



Solidcore Systems, Inc.
20863 Stevens Creek Blvd, Suite 300
Cupertino, CA 95014

Email: sales@solidcore.com
Web: <http://www.solidcore.com>
Tel: 888.210.6530