

Domino Server Configurations: Compliance with the Sarbanes-Oxley legislation and ITIL Framework



Published May 2009 - Version 1.1

This document is provided for reference purposes only. It is provided "AS IS" without warranty of any kind. The user assumes the entire risk as to the accuracy and the use of this document.

Contents

Table of Contents

- 2. Abstract.....3
- 3. The Problem.....3
- 4. The Solution.....4
 - 4.1 Sarbanes-Oxley (SOX).....4
 - 4.1.1 Risk Assessment.4
 - 4.1.2 Control Activities.4
 - 4.1.3 Monitoring/Auditing.4
 - 4.1.4 Information and Communication.4
 - 4.1.5 Material Events.4
 - 4.2 The ITIL (Information Technology Infrastructure Library) Framework.....5
 - 4.2.1 Change Management.5
 - 4.2.2 Configuration Management.5
 - 4.2.3 Problem and Incident Management.5
 - 4.2.4 Security Management.5
 - 4.2.5 Service Delivery.....5
- 5. Conclusion.....6

1. Introduction

If you're in the U.S., you'll be aware that the Sarbanes-Oxley legislation requires (amongst many other things), that Management accept responsibility for the effectiveness of the company's internal controls, and also report an assessment of these controls at the close of each fiscal year.

You might also be aware that Section 490 calls for real-time reporting of material events that could affect the company finances or business operations. A 'material event' might for example be a security breach, say where the user level 'anonymous' is given Manager access to all databases on the company website.

In addition to the U.S. Sarbanes-Oxley legislation, many international companies are now turning to the ITIL Framework (<http://www.itil-officialsite.com>), to provide a consistent and professional Service Delivery across their IT operations.

These requirements need to be equally applicable to the IBM Lotus™ Domino™ Server environment.

2. Abstract

The Domino Server environment is a largely self-administered entity, without a wide range of native controls. There is some monitoring, but only for a subset of the elements used in the configuration of servers.

Within the Domino environment, Administrators lack tools to control the maintenance of the (mission-critical) Server configurations, while Managers and Auditors lack an audit trail of changes. This could easily prove costly for an organisation required to report on the history of changes affecting their data security (for example, modifications to an 'All Managers' group).

What is required in any I.T. Department is a process to monitor and control the Server configurations within the environment. If this process can be further extended to provide useful features that complement the administration of that environment, then so much the better.

3. The Problem

Each Domino server can be configured in various different places – the Operating System, the Server Console, the Domino Directory, etc.

For instance, the NOTES.INI file is an OS file on each server that contains important configuration information. If this file is accidentally or deliberately damaged, the server operation can change.

In other cases, any Administrator without the 'big picture' can cause major problems by such innocuous actions as changing the contents of a Group, deleting a Connection Document, or modifying User Policies.

So the problem is, how can you control, monitor and audit your Domino Server environment to provide Sarbanes-Oxley and ITIL compliance? i.e. how can you provide a stable and controlled environment for your servers, and therefore your data and applications?

4. The Solution

The ability to control the configuration of your Server environment, understand how it's components interact, and provide an audit trail of changes are a key requirement for every I.T. Department, as well as integral to the Sarbanes-Oxley legislation and the ITIL (Information Technology Infrastructure Library) Framework.

The IONET Change Manager is the only tool that can provide these functions for the Domino Server environment, and it does so in a number of ways;

4.1 Sarbanes-Oxley (SOX)

4.1.1 Risk Assessment.

IT management need to understand how the company's Domino system is being used, including the level and accuracy of existing documentation. The Change Manager automatically provides this by recording all aspects of your Server Configurations in one place, including such diverse elements as Server configurations, NOTES.INI files, Administrator Groups, User Policies, and Web configurations. This results in a real-time and historical record of all configuration elements, including all changes (i.e. what changed, who made the change, when, and why).

4.1.2 Control Activities.

The Change Manager provides automatic Control activities to ensure that the necessary actions are taken to address risks when performing changes to your environment. The out-of-the-box functions of the Change Manager include Approvals/Authorisations, verification, reconciliation, security of assets and the segregation of duties. For example, you can assign a local expert responsibility for verifying and approving changes to the Web environment for a single server (or a group of servers), and another expert responsibility for the Mail & Network environment.

4.1.3 Monitoring/Auditing.

The Change Manager automatically monitors the configuration of your Domino servers, Database Security AND User Certifications & Sessions, alerting specified people to both authorised and unauthorised changes. This automatic auditing can be performed as often as every 15 minutes. Historical configurations and changes are retained and available.

4.1.4 Information and Communication.

Automatic notification of changes to your Domino Server environment allows Administrators an accurate, easy way to pro-actively identify and address areas of risk, as well as providing a 'heads-up' for interested parties. This ensures there are no surprises, and appropriate staff can react to issues as they occur. This also demonstrates to management Domino compliance with your Sarbanes-Oxley requirements.

4.1.5 Material Events.

Customisable, automatic notifications of configuration changes assists Administrators to monitor Material Events that may have a negative impact on the Server environment, and/or otherwise go unnoticed.

4.2 The ITIL (Information Technology Infrastructure Library) Framework

4.2.1 Change Management.

By using the automated Change Manager Approval Process, you can easily apply standardised methods, approvers and procedures to control potentially high-risk changes to your environment. For instance, Administrator A might approve all Server Changes for the 'Application Servers' group, whereas Administrator B approves all Web changes for the ACMEWEB Domain. This Change Approval process is highly customisable, for example to include multiple Approvers for certain requests, or include Courtesy emails.

4.2.2 Configuration Management.

The Change Manager acts as a CMDB for Domino Servers configurations, by recording all current and historic Configuration Items, the relationship between them, and any changes to them (including who changed them, when and why). This means you can also examine different server configurations (for example NOTES.INI files line-by-line), to see how your environment matches up.

4.2.3 Problem and Incident Management.

The in-built Approval Process will eliminate most Incidents and Problems related to configuration changes, before they occur. However even if you choose not to use it, you can still get advance warning of potential Incidents by being alerted to configuration changes made by others, and quickly resolve known Incidents by checking for related configuration changes.

4.2.4 Security Management.

The same Notification and Approval processes mentioned above also relate to security. For instance the Approval Process would normally prevent Administrator A from adding * to the 'Full Access Administrators' field, but even if you choose not to use it, you can quickly advise the right person automatically of any otherwise unrecorded security breach.

4.2.5 Service Delivery.

Ensure efficient Service Delivery by using the Change Managers Capacity Management tools: These include Benchmarking, Server Comparisons, NOTES.INI Comparisons, and Directory Validation to measure the differences in your environment, identify possible bottlenecks, and ensure Servers conform to a known standard.

5. Conclusion

All I.T. Departments require the ability to manage the configuration of their environments in a controlled, secure, easy and yet flexible manner. Lotus Domino is no exception. Recent legislative requirements in the U.S. and the trend toward basing I.T. services on a framework such as ITIL simply reinforce this requirement.

In order to structure the workload of multiple Administrator sites, enhance the accountability and management of Domino servers, and fulfill your obligations for management initiatives and compliance regulations, you need the ability to control the most important part of your Domino environment – the servers themselves.

The IONET Change Manager allows you to actively lock down, distribute and manage the administration of all of your Domino servers, and additionally provides many features that will enhance the responsiveness of your I.T. Department.

For more information or an evaluation copy, please visit <http://www.ionetsoftware.com/change>.