intigua

AUTOMATING SERVER TOOL MANAGEMENT

Improving Server Security by Minimizing Privileged Server Access

`

Improving Server Security by Minimizing Privileged Access

Table of Contents

Introduction

As your company's servers proliferate — and with the growth of cloud-based and virtual computing environments, that's practically a given — so does the risk to your business. Each server represents a potential for human error and an entry point to your network. Every additional person who has privileged access to that server raises the risk.

In an ideal world, enterprises would limit the scope of privileged server access. However, despite progress on this, there is one key IT workflow that still relies heavily on privileged server access: the care-and-feeding of numerous server management tools that provide services like back-up, security and monitoring, and that are placed onto servers.

Let's dive into why this is and what steps you can take to minimize privileged access, increase security, and, at the same time, improve service delivery to enterprise customers.

Scoping the Problem

Servers are provisioned to provide computing power for a variety of uses or roles, including applications, databases, middleware, and web-services – hence we speak of database servers, application servers, and so on.

However, every server also requires a variety of additional software tools to provide critical services including backup, security, compliance, monitoring, analytics and configuration management. Until these tools are applied, a server can't go into production and users can't consume it. And, after they're applied, this "stack" of server management tools needs to be maintained with patches, updates, and reconfigurations.

Many people needing server access

Maintaining these server management tools over a server's lifetime requires time and coordination among different IT teams. Enterprises typically support dozens of tools. Different teams and individuals are responsible for each tool's life cycle, from configuration, deployment and registration to monitoring, troubleshooting, updates, audit reporting and migration.

Accumulation of privileges

IT Ops and server tool subject matter experts (SMEs) request privileged server access to perform maintenance and troubleshooting tasks, even though they touch only a small portion of the server. Over time, companies often end up granting hundreds of people privileged server access for management tool oversight.

When too many people have this level of access, however, you can run into serious problems.

Server downtime

Accidental human error is the second-highest cause of downed servers. And the more people with privileged server access, the greater the opportunity for misconfiguration and human error to occur. Businesses that want to avoid the effects of server downtime, from lost revenue and lower productivity, to stains on your company brand, must make minimizing human touches a priority.

Running afoul of regulatory requirements

Mandates like PCI require businesses to limit server access by administrators. Non-adherence can be very costly to your organization.

How IT Ops Deals with Privileged Server Access

To date, enterprises have approached privileged access for server management tools teams in a variety of ways, all of which require tradeoffs.

Granting unlimited privileged access to management tools teams

As noted earlier, giving full access to everyone from NOC to level 1 and 2 support, to (SMEs, exposes your organization to the highest levels of risk. With this type of approach, errors and server downtime are bound to happen.

Limiting access to specific SMEs

Limiting server access to a smaller team clearly has upside in terms of lowering risk. However, it also creates bottlenecks that can slow down business since all tasks are handled by just a few people.

Creating workflows for granting temporary access

Temporary access rights limit scope of access, but also create a lot of administrative overhead. IT Ops can spend more time trying to gain privileged access than it needs to actually resolve problems. This is not agile.

Auditing access logs to diagnose human error

Reviewing logs after-the-fact doesn't stop problems from occurring. While it provides important data points that are useful for planning and forensics, auditing alone isn't enough. It needs to be complemented by a proactive approach that minimizes the chances of problems happening.

Deprioritizing management tool maintenance, upgrades and migrations due to risk of misconfiguration

Many IT organizations can't dedicate enough time or staff to keep up on care-and-feeding and ensure that tools perform correctly. As a result, problems happen because tools don't have the latest updates, security patches, and more.

A Better Way: Centralized, Fine-Grained Role-Based Access Control

The most effective approach to reduce privileged server access is to limit its necessity and availability. Access is generally requested to see information that typically only resides on the server. But what if information needed to perform various sever management tasks is securely available elsewhere? And what if access to that information could also be role- and task-based, to limit visibility to only what is required for the task at hand?

To enable this approach, you need a central solution from which key information about all servers can be accessed – ideally regardless of whether servers reside in:

- your own data centers – physical or virtual
- private clouds
- public clouds such as Microsoft Azure or Amazon Web Services
- hosted environments

You also need a high degree of granularity and the ability to differentiate among—and map directly to—company-specific organizational roles.

To minimize training and ongoing management costs and to ensure the solution is easily adoptable, tasks should be automated when possible. All capabilities should be wrapped in an intuitive UI that enables remote tool management. This will allow generalists to perform tasks previously restricted to SMEs. And, of course, you need to ensure detailed activity logs are maintained.

Intigua – Faster IT Ops without Privileged Server Access

Intigua Agent Controller enables a virtualized IT Operations command center for server management tools that makes it easy to increase server security by minimizing privileged access, while simultaneously ensuring faster and more consistent services delivery. Intigua accomplishes this by giving you three powerful capabilities:

1. Complete visibility, control and troubleshooting of management tools, without direct privileged server access
2. Customer-definable roles, i.e., by job, location, server-role and management tool
3. Automation of common activities that normally require direct server access

Let's look at each of these more deeply.

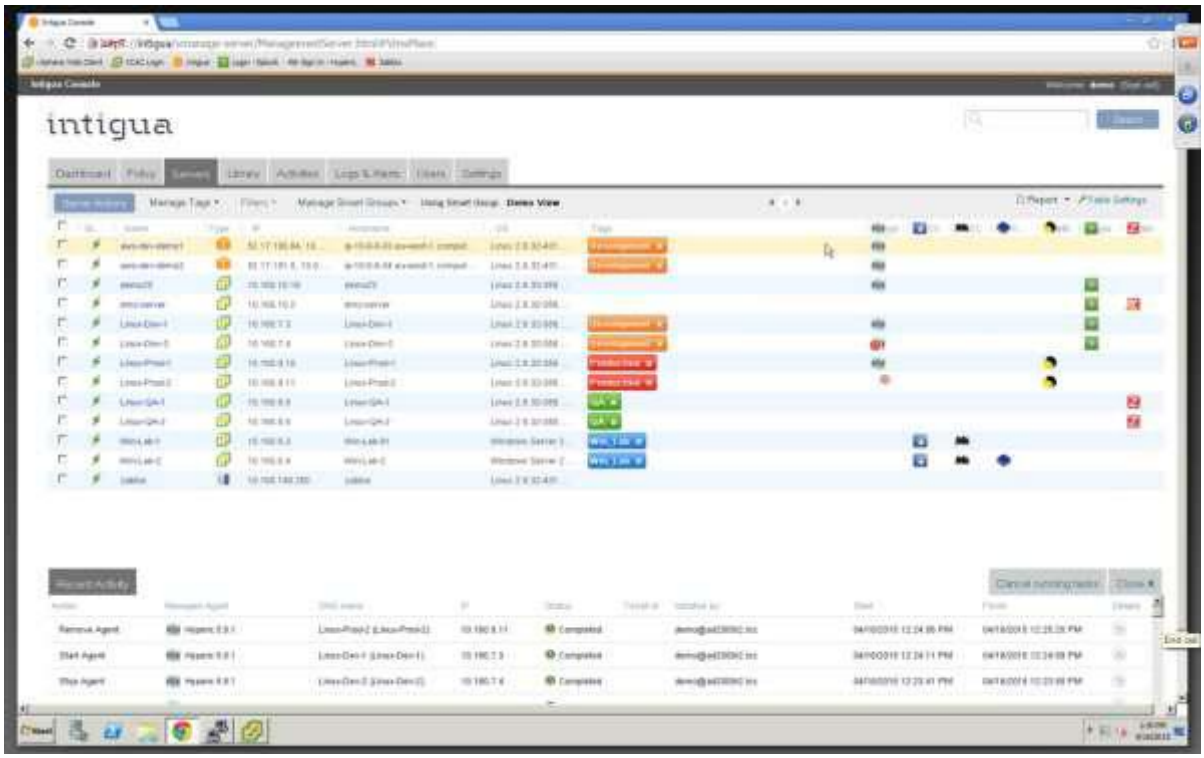
Complete visibility, control and troubleshooting of management tools, without direct privileged server access

Intigua gives IT Ops, Tool SMEs, DevOps and other IT teams role-based and task-based views and information across server management tools, server roles, operating systems and mixed infrastructure from a central portal to perform their tasks, rather than into individual servers themselves. For example, information needed to diagnose problems agents running on servers is available from Intigua, and without requiring direct access to servers. This workflow greatly reduces the need for privileged server access, and it eliminates all the time consuming steps associated with granting and revoking temporary privileges.

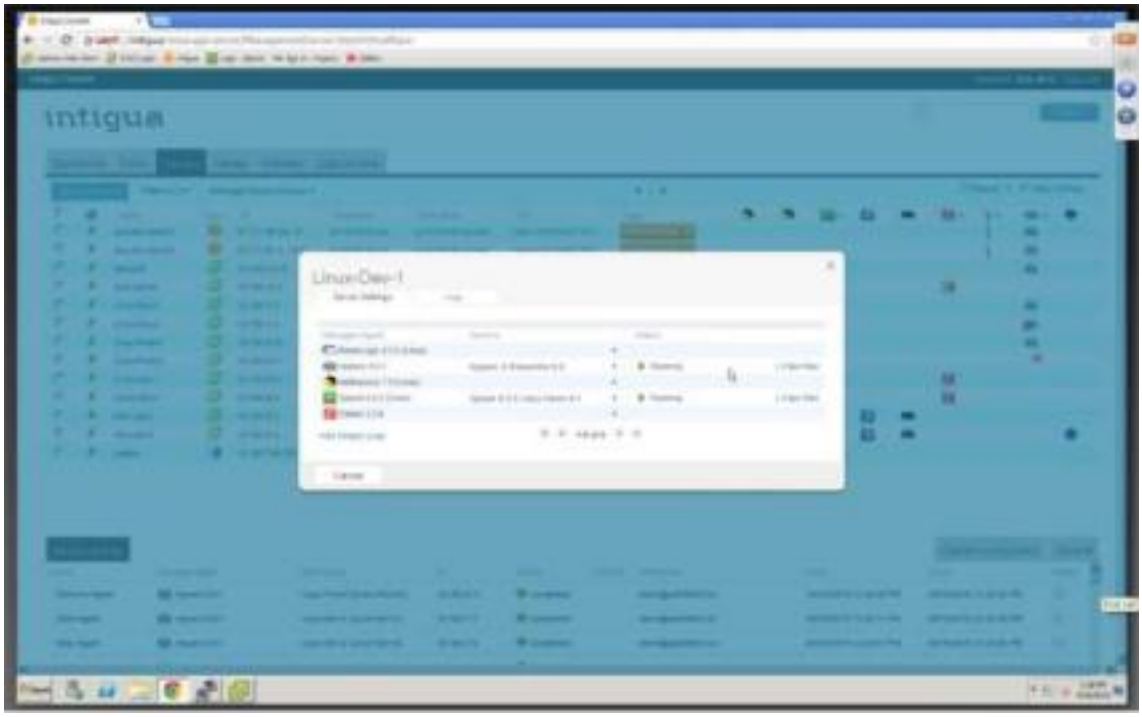
Customer-definable roles, i.e., by job, location, server-role and management tool.

Intigua provides fine-grained role definitions so you can map different levels of server access, information visibility and activity permissions to specific tasks and roles. For instance, you might grant NOC and Level 1 users read-only access to the server management landscape, while providing Level 2 users read/write access to specific tools on specific parts of the data center, and giving IT engineering and management tool SMEs read/write and diagnostic access to specific tools.

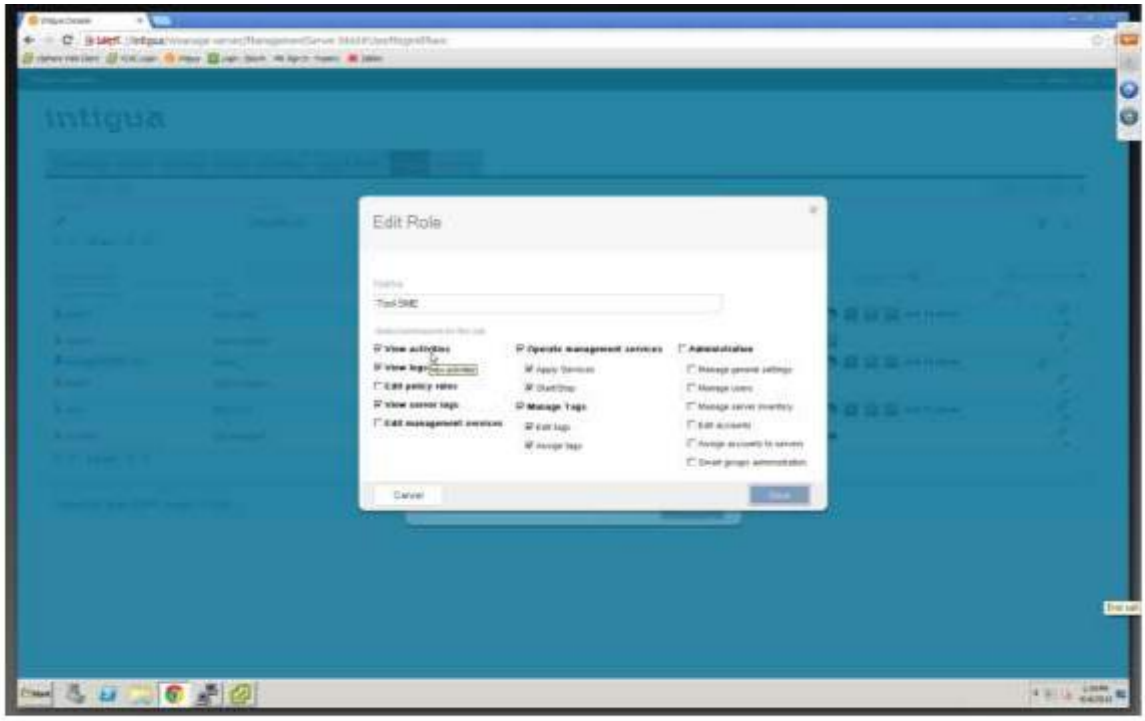
The screen below shows read-only access to all servers across operating systems and server roles, such as dev/test/prod, web/DB/app:



In the following example, a Level 1 NOC user is granted read-only access and cannot make changes. Note that the apply button isn't present.



Here, the tool SME role has permission to view activities and server logs, apply management services and manage tags, but not perform administration tasks.

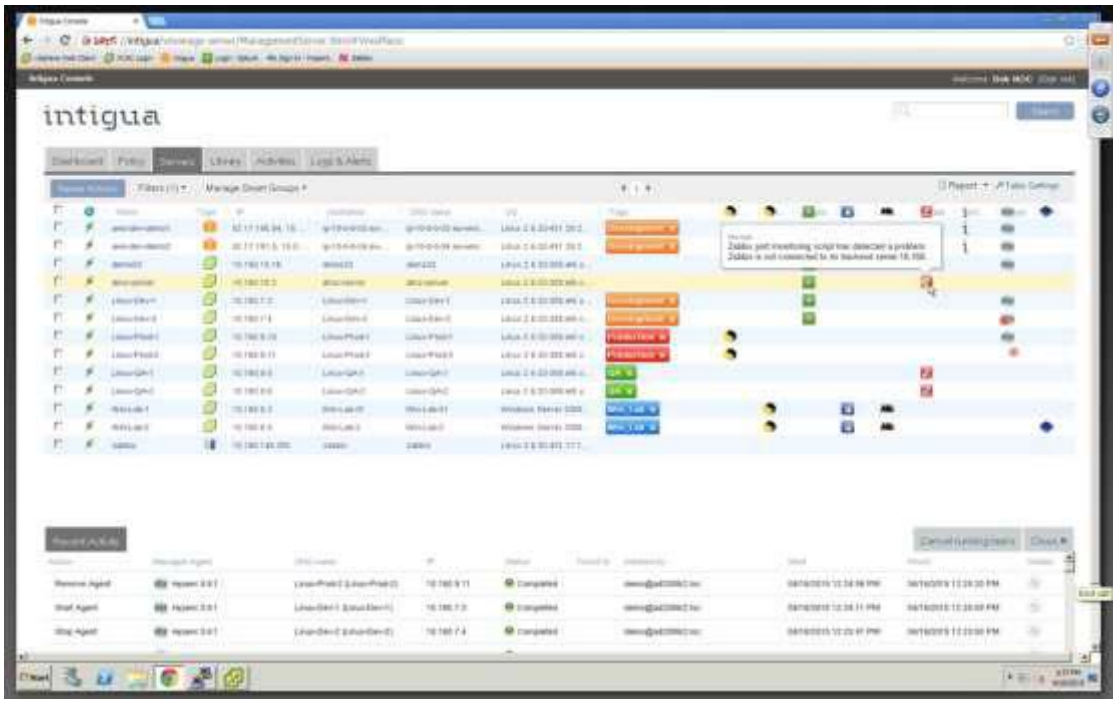


Automation of common activities that normally require direct server access.

With Intigua, tasks such as agent restarts, diagnostics, and reconfigurations can be automated, which makes these activities scalable across thousands of servers and mixed infrastructure.

Automation helps remove human error and ensures configuration consistency. Perhaps the biggest benefit for IT staff is that with automation handling many situations, Intigua gives time back to IT operations and tool SMEs so they can focus on more interesting and more demanding issues.

Automation also enables generalists to handle more of the tools management process. For example, as shown below in the screen's call-out box, Intigua empowers Level 1 users with automated diagnostics to help them resolve issues without escalating them. By removing bottlenecks, you'll accelerate IT Ops' ability to get the job done.



Summary

Widespread privileged access compromises server security, and until now, direct access to servers has been needed to maintain essential server managamant tools. IT organizations have tried everything from granting temporary privileges, to limiting permanent privileges to just a few staff members, to letting tool maintainence slide. None of these approaches are adequate. They lead to too much administrative overhead and cause process bottlenecks that limit IT's ability to get their job done, and put servers at risk of security breaches and downtime.

If, like most enterprises, privileged access-related security issues plague your organization, you may want to consider Intigua. By providing a centralized solution with role-based access control and automated operations, Intigua enables you to:

- Limit privileged access to the configuration items and tasks required for the job at hand
- Enable generalists to perform tasks previously restricted to SMEs
- Limit privileged access to servers and improve server security
- Increase IT Ops' aglity and provide faster, more consistent services delivery

About Intigua Agent Manager

Intigua Agent Manager is a configuration management solution for server tool agents. It saves IT and DevOps professionals countless hours of tedious work by streamlining, automating and accelerating agent deployment, maintenance and troubleshooting. Tasks that took weeks or months now take minutes, server policies are easily enforced at massive scale, and staff are free to focus on strategic projects instead of babysitting servers.

Discovery of agent and server inventory

Intigua talks to cloud, virtualization and tool servers, building a complete, central view of which agents are deployed, where they are running, and under what configuration.

User-defined central agent management policies

New servers get the right agents automatically. Servers migrating between data centers, or going through a dev-stage-run sequence, have their set of agents automatically adjusted for each situation.

Library of pre-integrated tool agents

Intigua includes a large set of pre-packaged, popular tool agents plus a self-service packaging wizard for adding new agents.

Agent auto-fix and reconfigure

Broken agents or agents in unhealthy state are automatically identified and restarted, reconfigured or reinstalled, as appropriate.

In the cloud and on-premise

Intigua works with all environments, including AWS, Azure and OpenStack clouds, and can accelerate the process of shifting workloads from one environment to another.

Deep visibility and diagnostics

Users can explore the status of any agent, collect and read its log files, without having to request privileged access to remote servers. Granular access controls ensure tool owners can remotely access only their own tools.

Orchestrate agents and their servers

Intigua automatically registers new agents with management servers, removes registered agents when no longer in use, and assigns configuration to each agent.

See how Intigua can simplify, accelerate and modernize the management of your enterprise IT tools and services.

http://www.intigua.com
info@intigua.com

Gartner

"Highly impressed ... real innovation in the cloud management market."
Chris Wolf, Research VP, Gartner (via Twitter)

FORRESTER

"Intigua's product is simple, laser-focused, easy to understand ... and designed to make real-world, everyday management of virtual environments simpler, faster, and less of a mess. Period."
Dave Bartoletti, Senior Analyst, Forrester

BEST OF VMWORLD

"I've never seen anything like this," said one of the judges, after selecting Intigua based on its "innovation and ability to fill a key market gap."