Architectural & Implementation Overview

Goverlan Central Server 1.3

SYNOPSIS

This document provides an architectural and implementation overview of the Goverlan Central Server v1.3.

Publication Information

This document was written by Pascal Bergeot, Chief Software Architect of PJ Technologies, Inc.

Published by
PJ Technologies, Inc.
www.pjtec.com

PJ Technologies, Inc.®
Software Solutions for IT Professionals

Contents

Purpose of the Goverlan Central Server

The purpose of the Goverlan Central Server is to centrally manage and globally control both settings distribution and auditing pertaining to the Goverlan Remote Administration, Goverlan Remote Control, WMIX and Goverlan Client Agents software products (collectively the "Goverlan Solution").

The Goverlan Central Server must be implemented within your infrastructure if stringent corporate security policies require a central control over the behavior of a solution as well as its auditing.

Default System Architecture without the Goverlan Central Server

This section describes the process flow of the Goverlan Solution settings distribution as well as auditing in its default context - where the Goverlan Central Server is not implemented.

Settings Distribution

The Goverlan Solution offers a large set of Universal Settings which are used to control the behavior of the solution across all machines. It also includes text customization settings which allows for the customization or translation of the user interface on the client machine.

In the default Goverlan Solution implementation, the Universal Settings are controlled either via direct registry modification or by configuring an Active Directory Group Policy Object ("GPO"). If no GPO or registry modifications are performed, the default settings value is used.

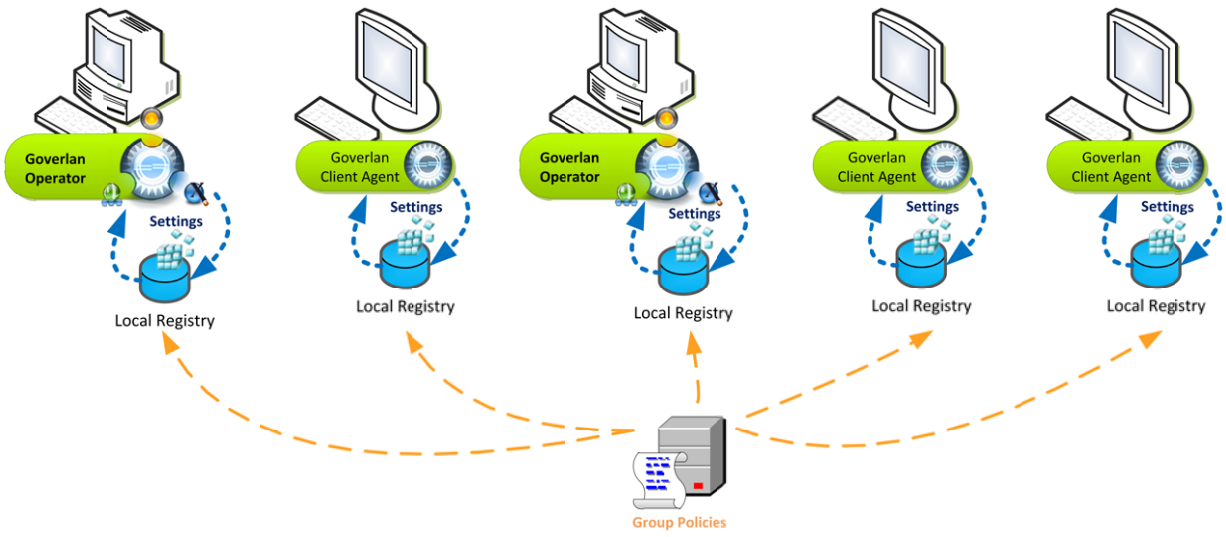


Figure 1 – Ad Hoc Settings Distribution

Auditing

In the ad hoc implementation, every remote control event registers an audit entry on the machine being accessed (additional notifications can be configured such as Email Notifications). The audit data is registered in both the local Event Application log as well as in a proprietary log in the registry. Even though the proprietary logs can be queried remotely, the audit data is still distributed across all client machines.

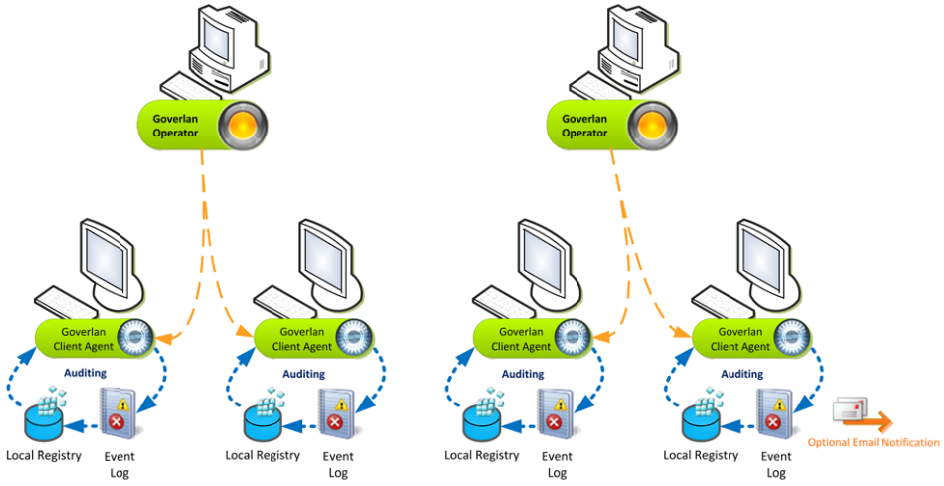


Figure 2 – Ad Hoc Auditing

System Architecture using the Goverlan Central Server

Settings Distribution

A Group Policy Object is a good way to centrally manage the settings of a solution; however, it is not a secure one. Anyone with local administrative privileges can manually change these settings and change the behavior of the Goverlan Solution against company policies.

In order to centrally manage and control the Goverlan Universal Settings securely, a Goverlan Central Server must be implemented. Once the Goverlan Central Server is configured and registered, the provisioning of all Universal Settings is processed via the Goverlan Central Server, bypassing locally configured policy settings. A local or domain administrator cannot tamper with these settings unless they have direct access to the Goverlan Central Server interface.

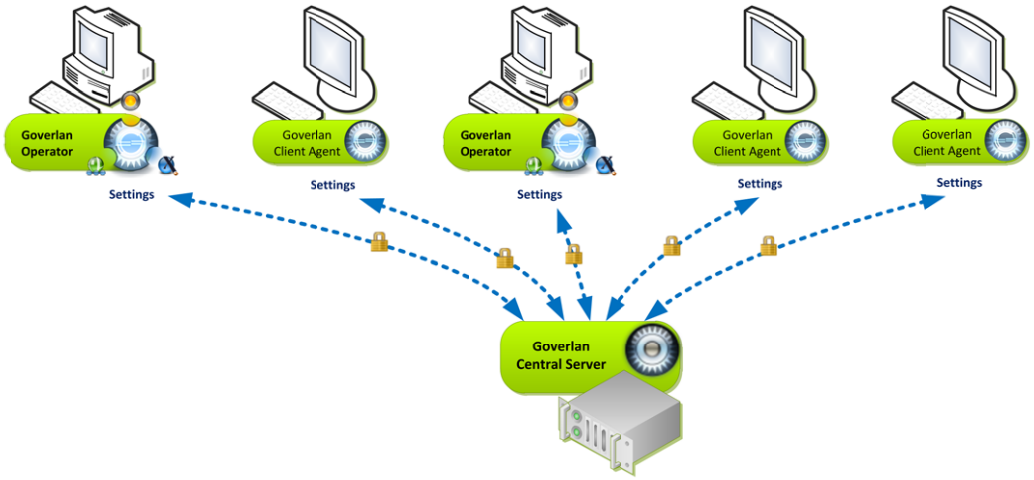


Figure 3 – Goverlan Central Server Settings Distribution

The Settings Distribution feature of the Goverlan Central Server allows you to configure some or all Universal Settings. The setting's value can be configured to a specific value for all machines, a conditional value based on machine scopes, or to the value as defined in the GPO accessible on the server.

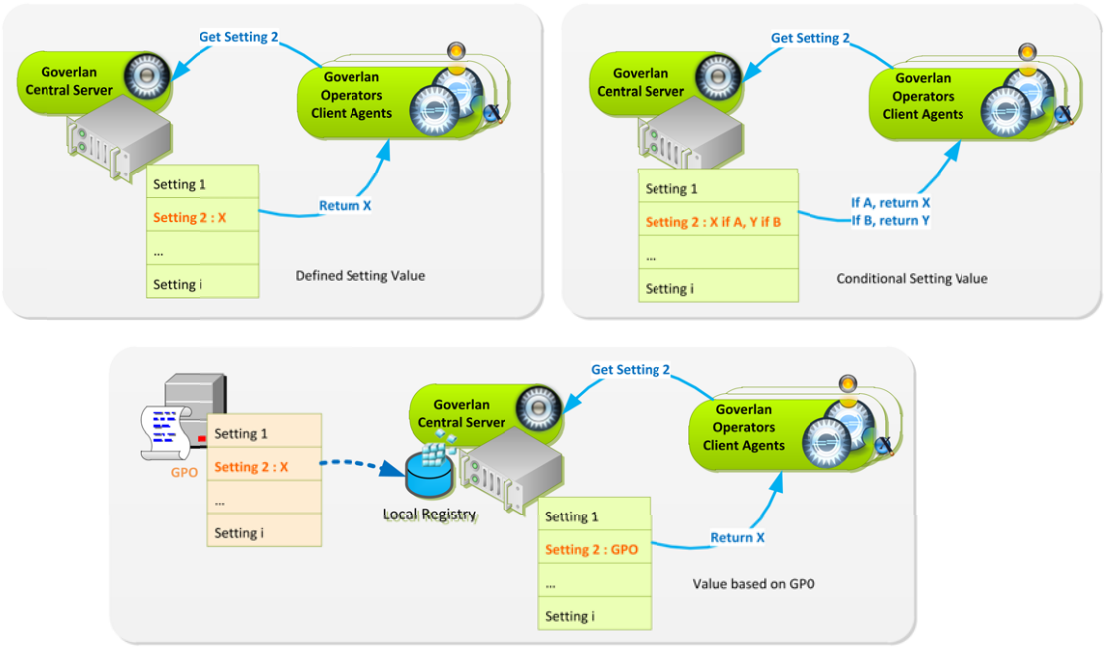


Figure 7 – Settings Distribution

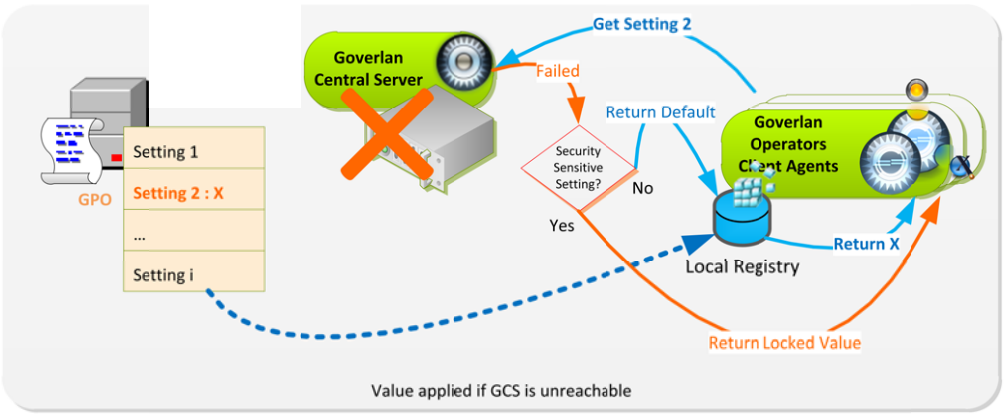
Conditional values are useful in order to configure different behaviors based on the machine's type (e.g.: server versus workstation, based on an IP range or domain group).

Settings Locked Mode

In the event that the Goverlan Central Server is advertised in DNS but is unreachable, the Goverlan Solution enters the *Locked Mode*.

Under Locked Mode, universal settings which have a security risk associated with them are automatically set to their most secure value.

If a setting doesn't represent a security threat, it doesn't have a Locked Mode defined value. Such settings are treated as if they were not enforced by the server.



Auditing

In addition to centrally and securely managing settings distribution, the Goverlan Central Server can be used to centrally and securely audit all Goverlan remote control session events as well as Windows logon events. This feature doesn't replace the existing distributed audit system but runs in parallel.

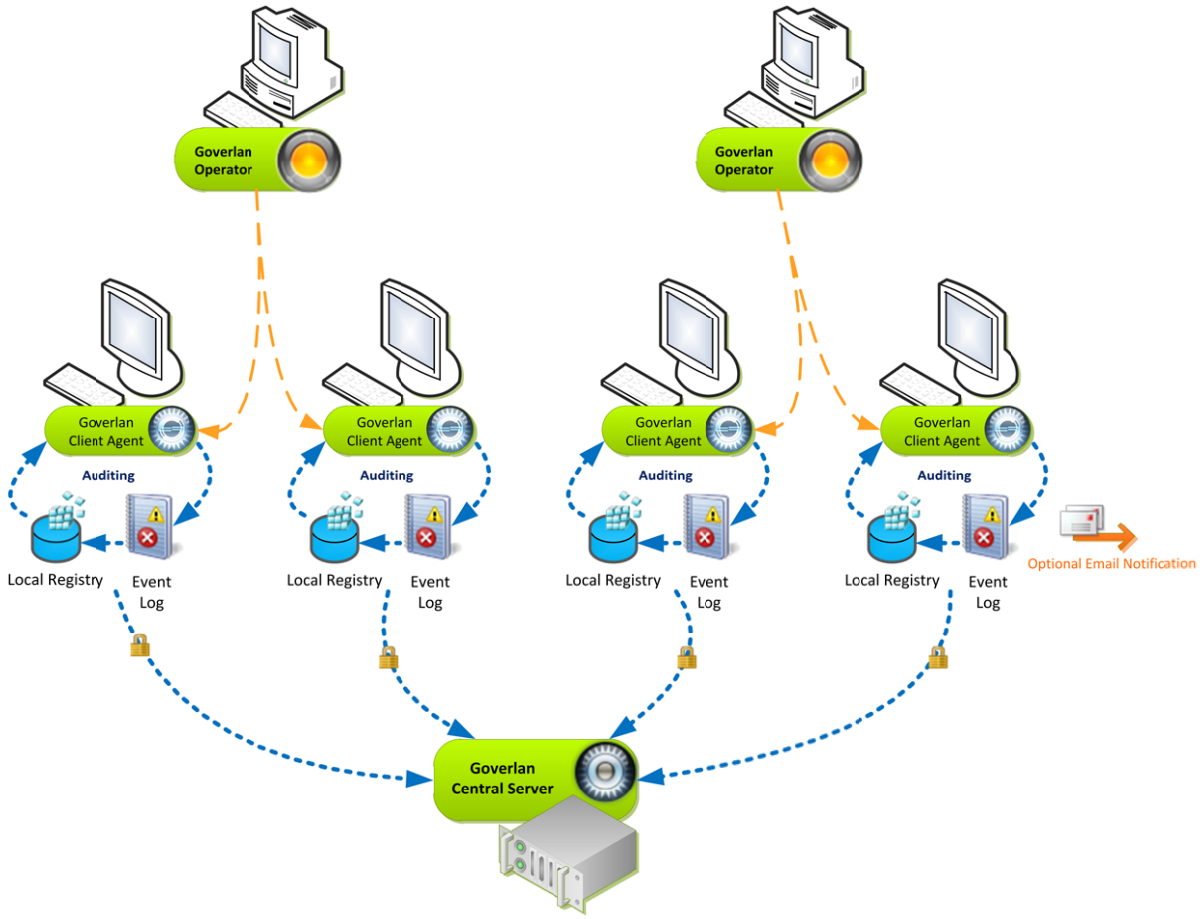


Figure 4 – Goverlan Central Server Auditing

Implementation & Process Flow of the Goverlan Central Server

Implementation & Registration

The Goverlan Central Server must be installed on a Windows 2003 or later server (Note: For a pilot run, the server can also be installed on a standard Windows XP or later operating system). Once installed, you can access the server control interface to configure its features, start or stop the server, and monitor server activity.

Once the server is installed, configured and started, it must be discovered across all machines. This is done using a DNS Service Location Record (SRV).

In an Active Directory environment, multiple Goverlan DNS SRV records can be created at the root of the AD Zone and within AD Site Zones, allowing for multiple Goverlan Central Servers to be used.

Goverlan Central Server Implementation – Single Zone

In the simplest configuration, a single DNS SRV record is created in the primary DNS zone. This SRV record can point to a single Goverlan Central Server or multiple Goverlan Central Servers for load balancing.

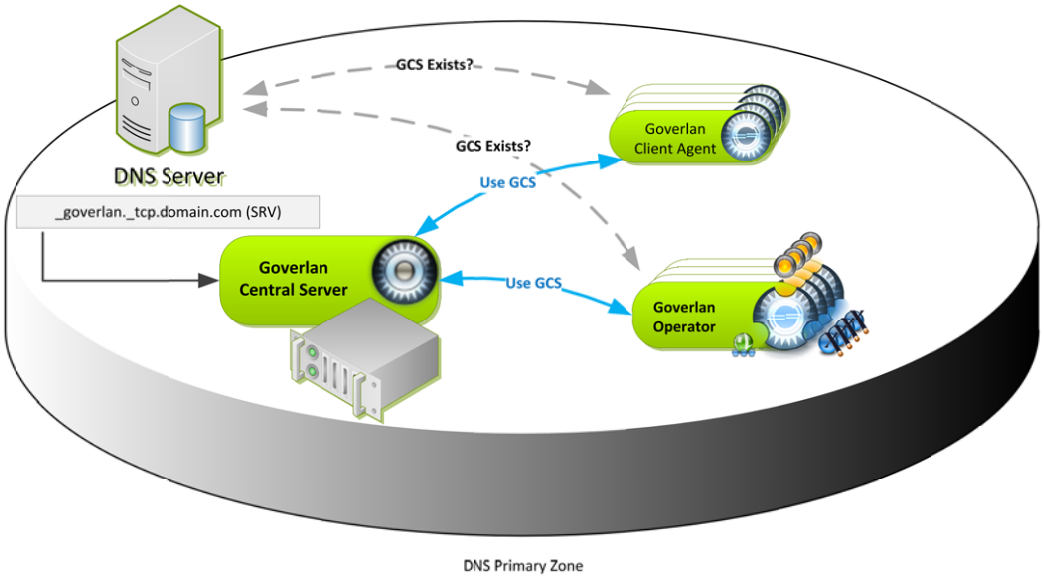


Figure 5 – DNS Registration Single Zone

Goverlan Central Server Implementation – Multiple AD Sites

In larger environments, a DNS SRV record can be created within each AD Site DNS Zones, each pointing to a different Goverlan Central Server.

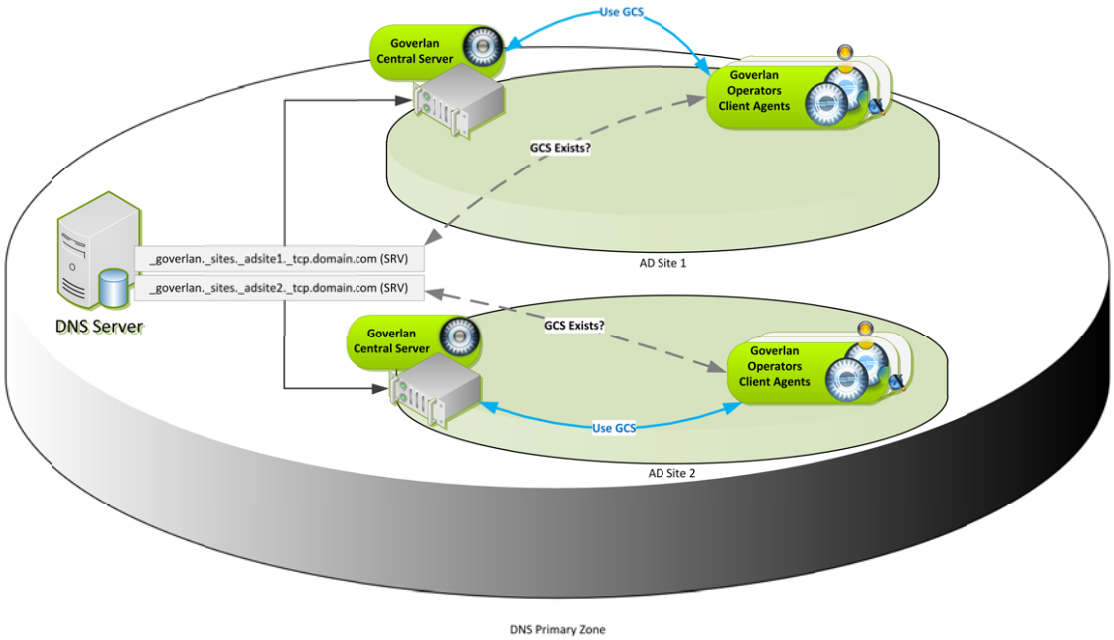


Figure 6– DNS Registration by AD Site

Note: The Goverlan Central Server doesn't provide replication services so each server must be configured individually.

Best Implementation Practice

If the Goverlan Central Server is not implemented, no Goverlan DNS SRV record should exist

The primary purpose of the Goverlan Central Server is to secure settings distribution and auditing. As soon as a DNS Service Location Record advertises that a Goverlan Central Server is present, it will affect the behavior of the Goverlan solution.

One such behavioral change occurs if the SRV exists and the Goverlan Central Server is not implemented or turned off. The Goverlan Solution knows that a server is present but cannot reach it to retrieve security directives. As a consequence, the Goverlan Solution enters the *Locked Mode*. If Goverlan is in Locked Mode, it will simply apply the most secure value for its settings. For instance, a client machine automatically locks the desktop session before and after a remote control session.

Note: If a setting doesn't represent a security threat, it doesn't have a Locked Mode defined value. In Locked Mode, such settings are treated as if they were not enforced by the server.

Therefore, if the Goverlan Central Server is removed from the infrastructure, **the DNS SRV records must be removed as well.**

Use a Group Policy Object as a Fail-Over

In the event the Goverlan Central Server becomes unreachable, implementing a GPO which has a set of default settings can be used as a fail-over system.

Use the Client Settings Tester Utility

The Goverlan Central Server comes with a Client Settings Tester Utility which can be used for advanced monitoring and troubleshooting of a client's connection to the central server. This utility shows you detailed information about the Goverlan Central Servers detected through DNS and the status of each connection to the primary server. It also shows the resulting Universal Settings value and the state resulting from the current environment.

References

- Web: **Goverlan Central Server Overview & Download**
  http://www.pjtec.com/Products/Goverlan_CS/index.html

- Web: **Goverlan Central User Guide**
  http://www.pjtec.com/Support/data/resources/UserManuals/GCS/index.html
  Note: The user guide is also accessible from the Goverlan Central Server by pressing the F1 key.