



5<sup>o</sup>

# Coloquio de proyectos de Becarios en Seguridad Informática

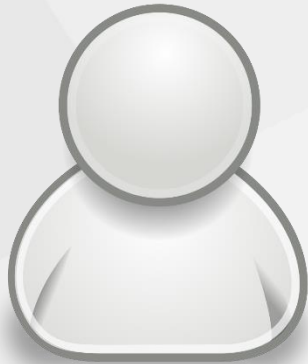
## Sistema centralizado para la administración de equipos y solución automatizada de errores

Luis Daniel Sánchez Vélez

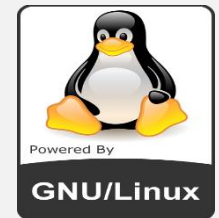
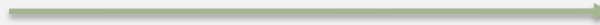
# Agenda

- Objetivo
- SC Virtual Machine Manager
- SC Operations Manager
- SC Configuration Manager
- SC Orchestrator
- Dificultades
- Conclusiones

# Objetivo



Administrador  
de Sistemas



# Objetivo

Crear un ambiente real para desplegar servicios en producción de forma eficiente y en menor tiempo.



Administrador  
de Sistemas



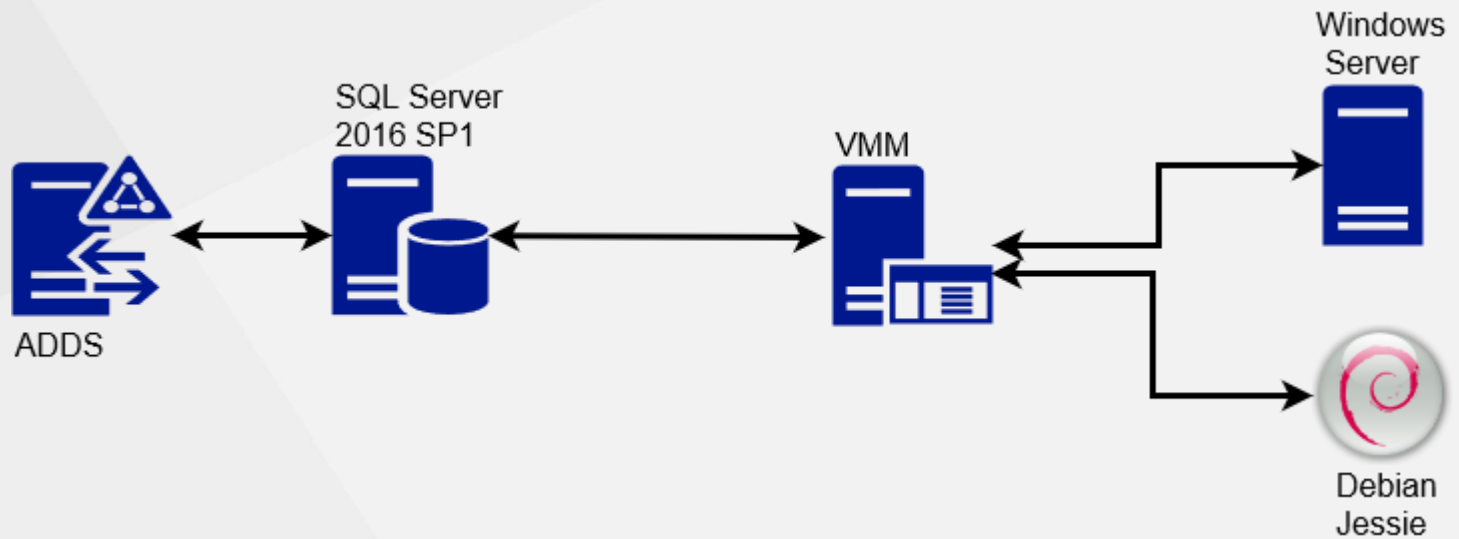
# SC Virtual Machine Manager

Es una solución de administración de centros de datos virtualizados.

Reduce el tiempo de implementación de sistemas operativos virtualizados.

Descentraliza la gestión individual, delegándola a usuarios específicos.

# Diagrama de red



# SC Operations Manager

Tecnología especializada en monitorear servicios, dispositivos y operaciones para múltiples equipos finales o servidores desde una consola.

The screenshot displays the SCOM - Operations Manager interface. The left-hand navigation pane shows a tree view under 'Monitoring' with various categories like Active Alerts, Discovered Inventory, and Distributed Applications. The main area is titled 'Monitoring Overview' and contains several informational sections:

- Required Configuration Tasks:** A list of tasks that must be completed for full functionality, including 'Configure computers and devices to manage', 'Import management packs', 'Enable Notification Channels', and 'Upgrade to full version'.
- Actions:** A list of available actions such as 'View all Active Alerts', 'View Computer State', and 'View Distributed Application State'.
- Key Concepts:** A list of conceptual links including 'The Monitoring Workspace', 'Standard Views', and 'Health Explorer'.
- Learn About:** A list of educational links like 'Finding Data and Objects in the Operations Console' and 'Using Views'.
- State and Alerts:** A summary table showing the status of various components.
 

Component	Critical	Warning	Healthy	Maintenance Mode	Unknown Status
Computer Health:	0	0	1	0	0
Distributed Applications:	0	0	1	0	0

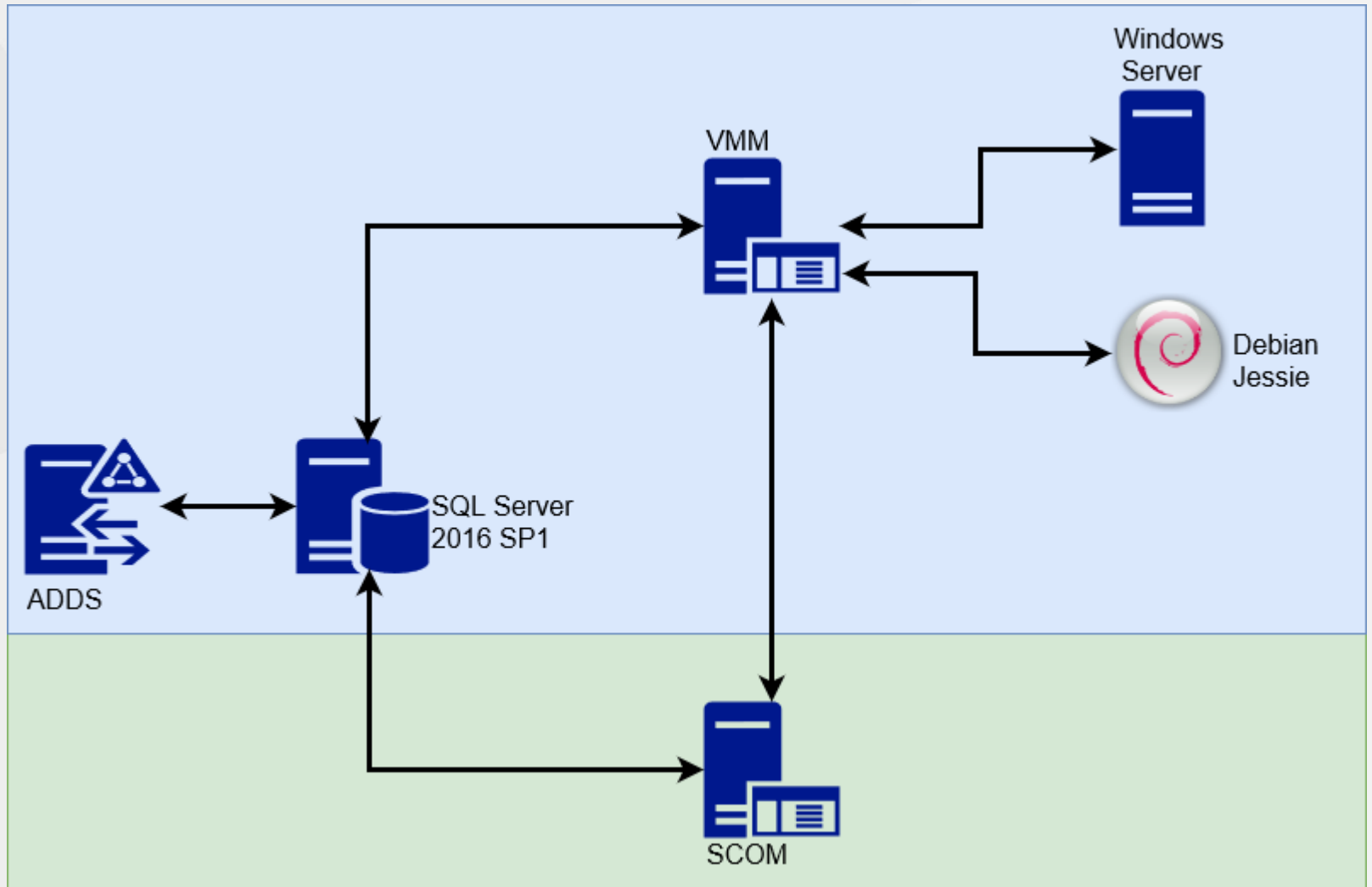
The status bar at the bottom left indicates 'Ready'.

# Características SCOM

- Servidor de administración
- Base de datos de operaciones
- Data Warehouse
- Consola web
- Servidor de reportes



# Diagrama de red



# SC Configuration Manager

Consola de administración unificada con un conjunto de herramientas administrativas automatizadas para:

- Distribuir software
- Proteger datos
- Monitorizar equipos de la organización

Cuenta con un repositorio de información con las características de los equipos en la organización.

# Información de equipos

Icon	Name
	PROYECTO10G\adddomain (adddomain)
	PROYECTO10G\luis.sanchez (Luis Daniel S)
	PROYECTO10G\orchestrator (orchestrator)
	PROYECTO10G\sccm (sccm)
	PROYECTO10G\sccm_clientes (sccm client)
	PROYECTO10G\scom (scom)
	PROYECTO10G\sqlserver (sqlserver)
	PROYECTO10G\vmm (vmm)

Search

Icon	Name	Client	Sit
	CLIENTEW10	Yes	PI
	ORCHESTRATOR	No	
	SCCM	Yes	PI
	SCOM	No	
	SQLSERVER	Yes	PI
	x64 Unknown Computer...	No	PI
	x86 Unknown Computer...	No	PI

System Center Configuration Manager - Resource Explorer

CLIENTEW10

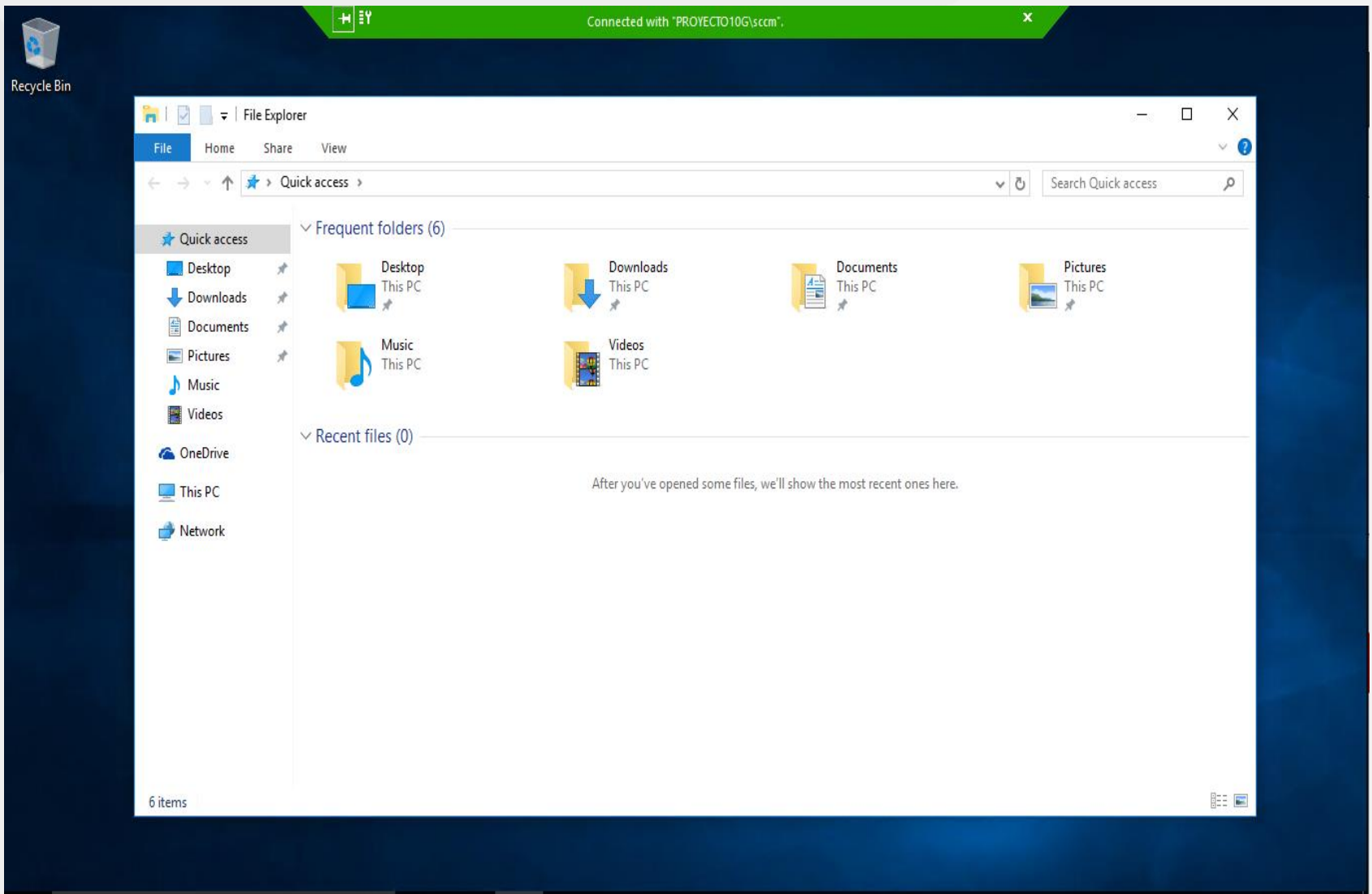
- Hardware
  - CDROM Drive
  - Client Events
  - Computer System
  - Configuration Manager Client SSL Config
  - Configuration Manager Client State
  - Desktop Monitor
  - Disk Drives
  - Disk Partitions
  - Folder Redirection Health
  - Installed Applications
  - Installed Applications (64)
  - Logical Disk
  - Memory
  - Motherboard
  - Network Adapter
  - Network Adapter Configuration
  - Network Client
  - OFFICE365PROPLUSCONFIGURATION
  - Operating System
  - PC BIOS
  - Physical Memory
  - PNP Device Driver
  - Power Capabilities
  - Power Management Exclusion Settings
  - Power Settings
  - Processor
  - Recently Used Applications
  - SCSI Controller
  - Services
  - System
  - System Console Usage
  - System Console User
  - System Devices
  - System Enclosure
  - User Profile Health

Filter...

Display Name

- Configuration Manager Client
- Microsoft Visual C++ 2013 x64 Additional Runtime - 12.0
- Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0
- Microsoft Policy Platform
- Microsoft Visual C++ 2005 Redistributable (x64)

# Remote tools



# Remote tools

System Center Configuration Manager (Connected to PRU - SitioSCCM) (evaluation, 130 days left)

Home

Import User Device Affinity | Import Cor Informa

Change Category | Change Ownership | Clear Required PXE Deployments | Delete

CLIENTEW10 - Configuration Manager Remote Control

File View Action Help

Connected with "PROYECTO10G.sccm"

Recycle Bin

File Explorer

File Home Share View

Quick access

Search Quick access

Quick access

- Desktop This PC
- Downloads This PC
- Documents This PC
- Pictures This PC
- Music This PC
- Videos This PC

Frequent folders (6)

Recent files (0)

After you've opened some files, we'll show the most recent ones here.

6 items

CLIENTEW10 | Authenticated

Active Directory Site:	Default-First-Site-Name	Management Point:	SCCM:projecto10g.local
Last Logon:	2/14/2017 11:29:27 AM	Status Message:	2/15/2017 8:22 AM
		Days Since Last Communication:	0

Summary | Client Check Detail | Malware Detail | Antimalware Policies | Client Settings

Ready

Activate Windows  
Go to Settings to activate Windows.

# Reportes de equipos

Collection  [View Report](#)

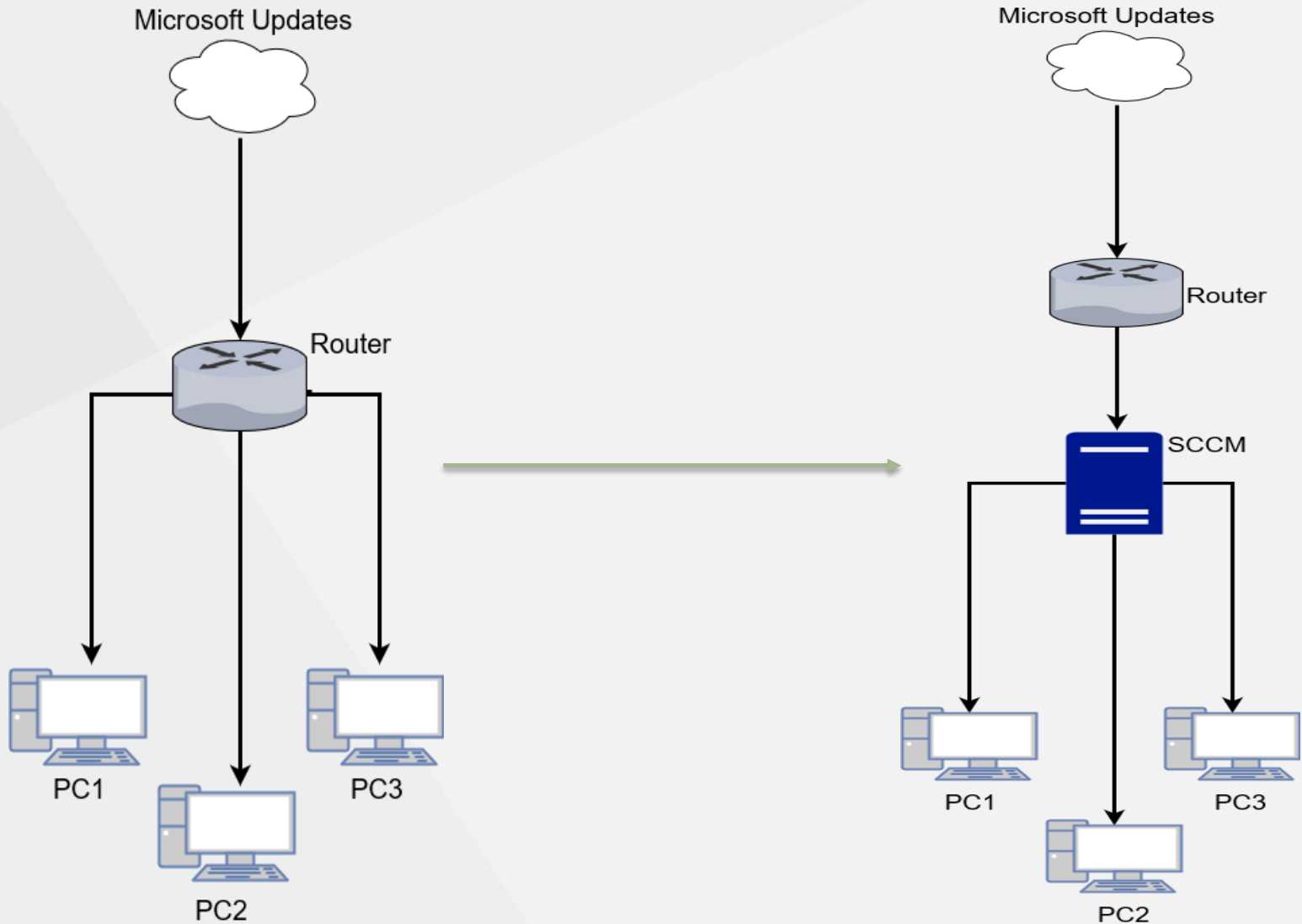
⏪ <  of 1 > ⏩ 🔄  ⏴ 🖨️  Find | Next

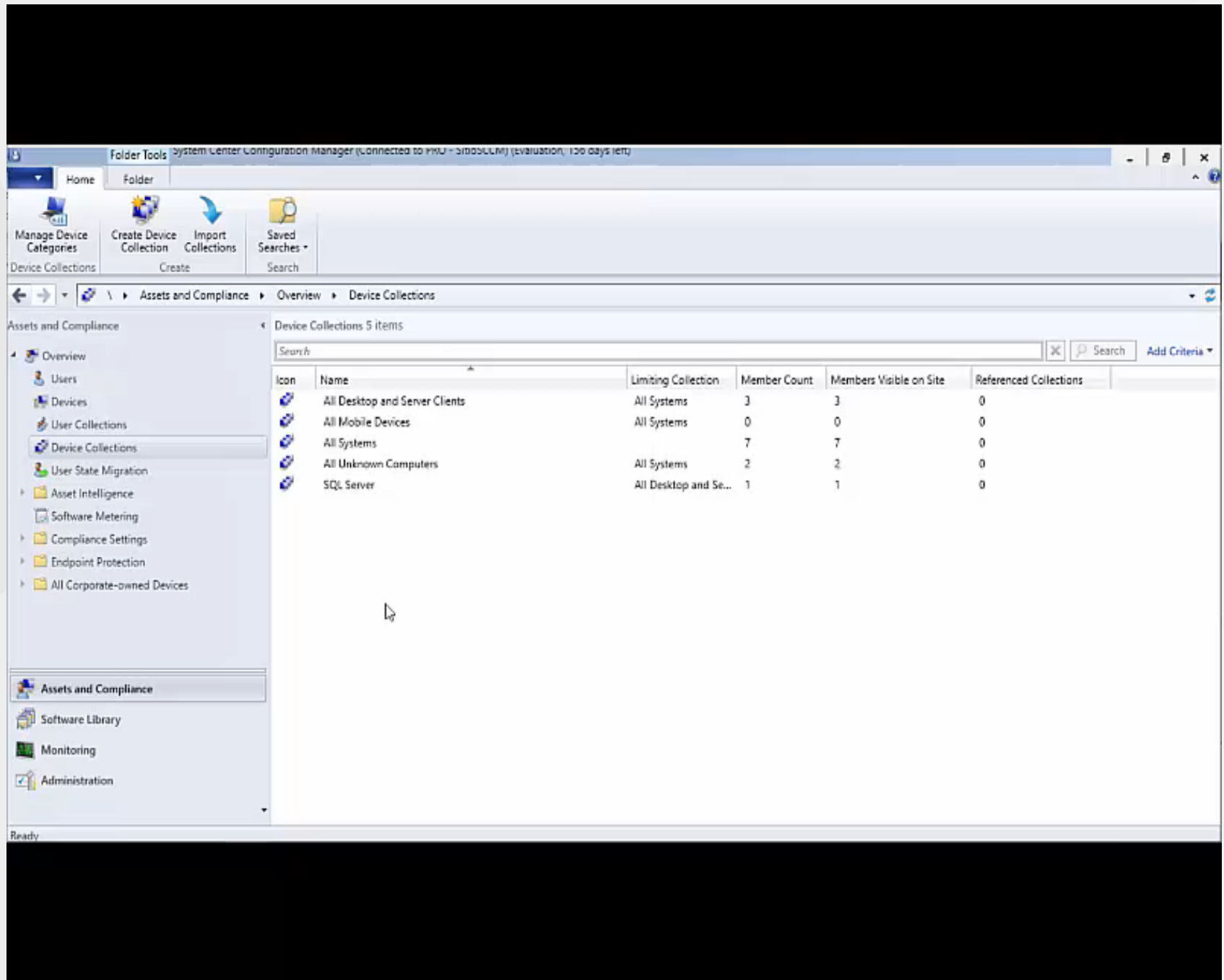
## Hardware 01A - Summary of computers in a specific collection

Description

Computer Name	Domain/Workgroup	ConfigMgr Site Name	Top Console User	Operating System	Service Pack Level	Serial Number	Asset Tag	Manufac
<u>CLIENTEW10</u>	PROYECTO10G	SitioSCCM	proyecto10g\luis.sanchez	Microsoft Windows 10 Pro N		0995-5860-5870-7362-6387-8846-85	0995-5860-5870-7362-6387-8846-85	Microsol Corpora
<u>SCCM</u>	PROYECTO10G	SitioSCCM	proyecto10g\sccm	Microsoft Windows Server 2016 Datacenter Evaluation		1363-9311-5332-0280-2100-4354-96	1363-9311-5332-0280-2100-4354-96	Microsol Corpora
<u>SQLSERVER</u>	PROYECTO10G	SitioSCCM	proyecto10g\sqlserver	Microsoft Windows Server 2016 Datacenter Evaluation		1363-9311-5332-0280-2100-4354-96	1363-9311-5332-0280-2100-4354-96	Microsol Corpora

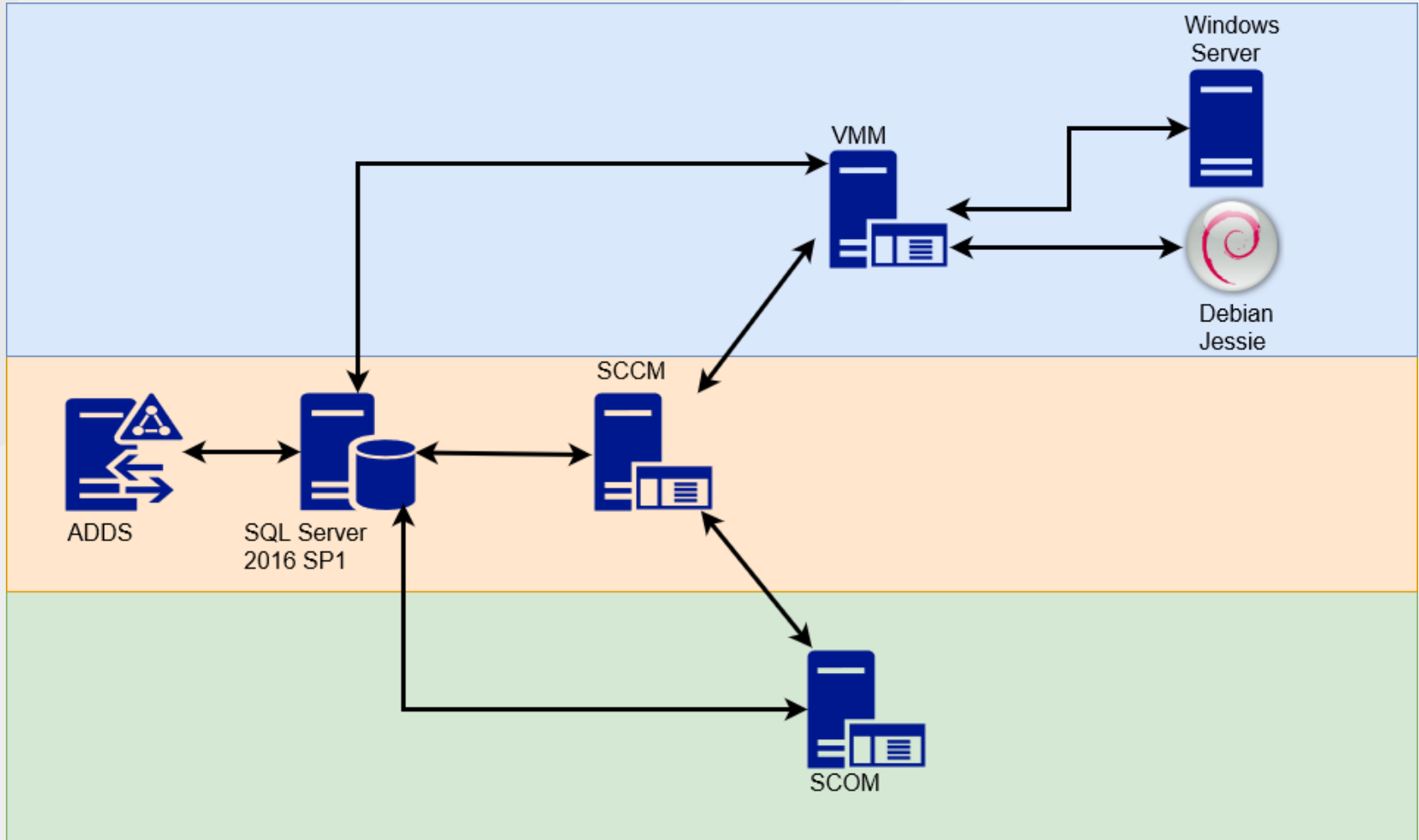
# Software update point







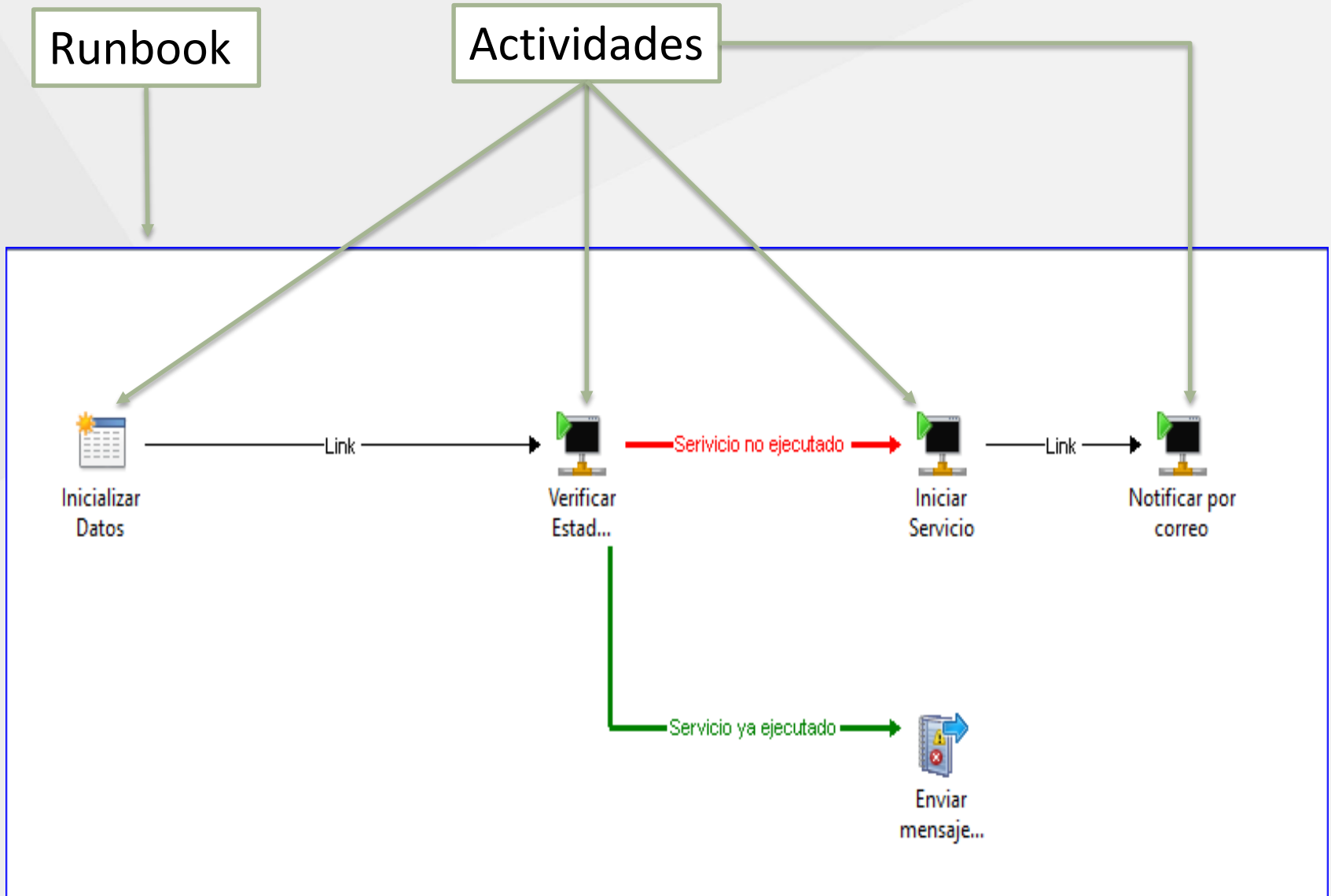
# Diagrama de red



# SC Orchestrator


- Administra soluciones de flujo de trabajo
- Automatiza recursos y procesos en el ambiente que se tiene en la organización
- Sin importar el hardware o plataforma

# Características



http://10.0.1.6/ Apache2 Debian Default Pa... x

# Apache2 Debian Default Page



## It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

### Configuration Overview

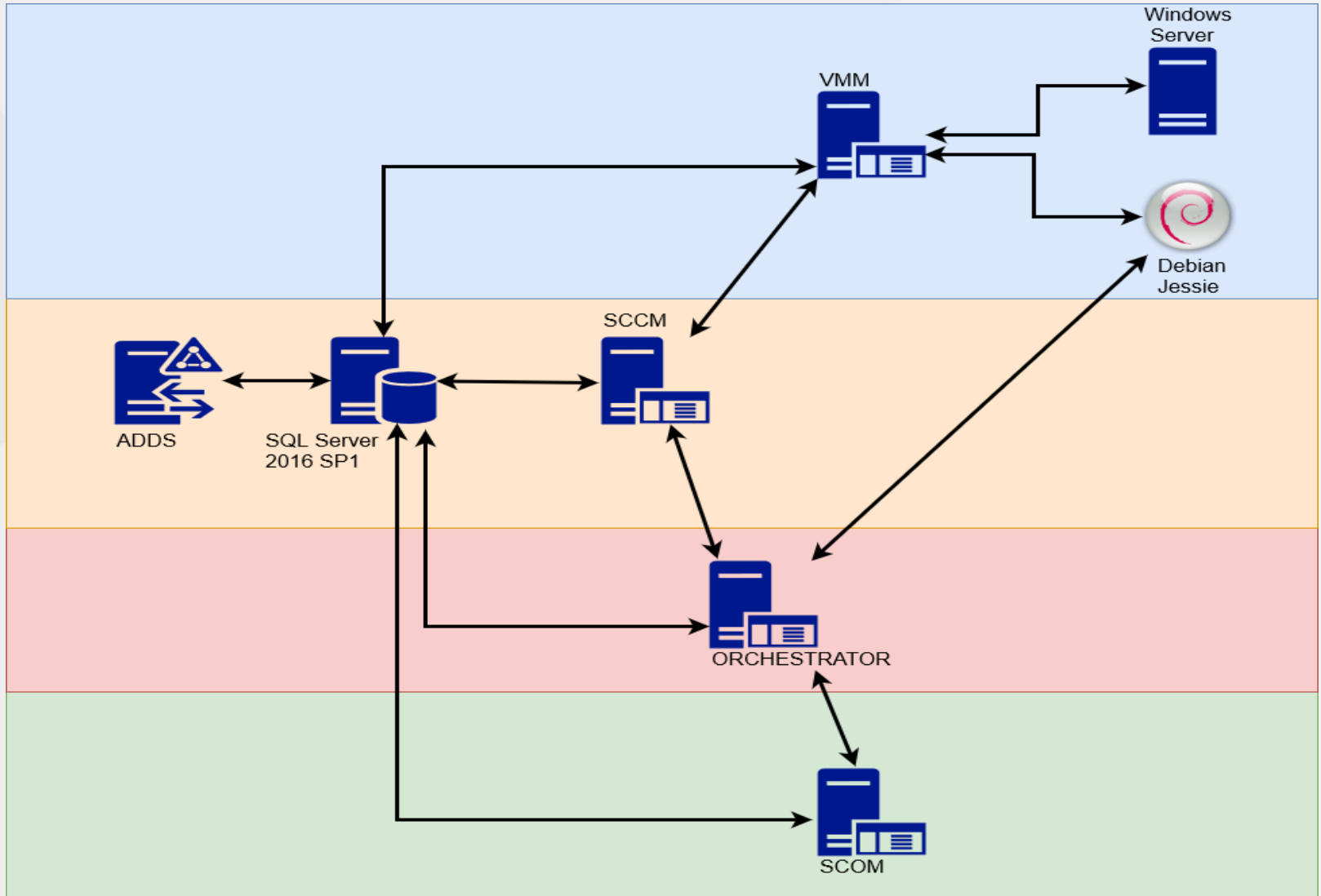
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
|   |-- ports.conf  
|-- mods-enabled  
|   |-- *.load  
|   |-- *.conf  
|-- conf-enabled  
|   |-- *.conf  
|-- sites-enabled  
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining

# Diagrama de red



# Dificultades

- Crear el ambiente con versiones de CTP de System Center
- Verificar los permisos necesarios
- Asegurar los requerimientos para cada tecnología de System Center
- Integrar WSUS con SUP
- Asociar Orchestrator con SCOM o SCCM mediante Integration Pack

# Conclusiones

- Se tiene un control de los equipos virtuales
- Se monitorean activos tecnológicos en la organización
- Se tiene equipos de cómputo actualizados y se conocen sus características
- Se cuenta con un ambiente inteligente que responde ante errores de forma automática

# GRACIAS

Luis Daniel Sánchez Vélez

UNAM-CERT

[luis.sanchez@cert.unam.mx](mailto:luis.sanchez@cert.unam.mx)