Building a Solid ITOM Mid-Server Architecture in ServiceNow: A Step-by-

'ike (knowledge) level: Novice

Rev. February 9, 2025

When it comes to building a robust **IT Operations Management (ITOM)** architecture in ServiceNow, one of the key building blocks is the **Mid-Server**. This often-overlooked component plays a crucial role in making sure your ITOM discovery, orchestration, and automation tasks run smoothly. Think of the Mid-Server as a bridge between ServiceNow and your on-premise or cloud systems, ensuring secure and efficient data flow.

So, how do you build a successful **Mid-Server architecture**? In this guide, we'll walk through everything you need to know to get started—what to consider, what activities to focus on, and the top mistakes organizations make. Let's dive in!

Key Considerations When Building a Mid-Server Architecture

Before jumping into the technical setup, it's important to lay out some basic guidelines and things to think about. You'll want to answer these questions early on:

1. **Network Connectivity:**
    - Is your Mid-Server in a location where it can securely access both ServiceNow and your target systems?
    - Does your organization have a secure, stable network that can handle data traffic between your on-premise infrastructure and ServiceNow?
2. **Scalability:**
    - Do you anticipate growing your ITOM footprint? If yes, consider how the architecture can scale as you add more regions, systems, or discovery probes.
    - Will you need to deploy multiple Mid-Servers for redundancy or performance reasons?
3. **Security:**
    - How will you ensure secure communication between the Mid-Server and your systems? You'll need to configure things like firewalls and secure authentication mechanisms.
    - Does your Mid-Server have the right access control policies and permissions to handle sensitive data?
4. **Fault Tolerance & High Availability:**
    - What happens if your Mid-Server goes down? Consider deploying multiple Mid-Servers for failover or load balancing to ensure continuity.
    - How will you monitor the health of your Mid-Servers? It's crucial to ensure that they're up and running all the time.
5. **Performance:**

- How much load will your Mid-Server need to handle? You'll want to plan for the resources it needs (CPU, memory, etc.) to handle discovery and orchestration tasks efficiently.
- How many concurrent tasks should it support at once? This could affect both server and network performance.

Activities to Complete During Mid-Server Architecture Setup

Once you've considered these factors, it's time to roll up your sleeves and get to work! Here are the key activities to focus on during the build phase:

1. **Install the Mid-Server:**
   - First things first, install the **ServiceNow Mid-Server**. You'll need to download and deploy it on a server that's capable of communicating with both your target systems and the ServiceNow instance.
   - Don't forget about firewalls and proxies that may need adjusting to allow secure communication.
2. **Configure the Mid-Server:**
   - Once installed, go into **ServiceNow** and configure the Mid-Server properties. This includes things like credentials, proxy settings, and connection types (e.g., HTTP or HTTPS).
   - If your organization has specific security requirements (e.g., VPN, SSH), make sure the Mid-Server is set up to comply.
3. **Set Up Security Credentials:**
   - For the Mid-Server to communicate with your systems (e.g., for Discovery, Orchestration, etc.), you need to configure proper credentials in ServiceNow.
   - This is also where you'll configure things like **SSH keys** or **API tokens** for secure communication with target systems.
4. **Configure Discovery and Orchestration Probes:**
   - Define the discovery probes and orchestration workflows that the Mid-Server will support. This could include network scanning, database discovery, cloud instances, or application monitoring.
   - Make sure you test the probes and workflows to confirm everything is working as expected.
5. **Monitoring & Alerting:**

- Set up a system to monitor the health of your Mid-Server. ServiceNow provides a **Mid-Server Health Dashboard** where you can monitor status, performance, and logs.
- Create **alerting rules** so you can be notified if there are any issues with connectivity, performance, or downtime.

6. **Establish High Availability (if needed):**
   - If you need redundancy or failover, set up additional Mid-Servers in different locations and configure them in a **high availability (HA) setup**.
   - You can configure load balancing or round-robin DNS to ensure that traffic is distributed evenly across all your Mid-Servers.

Preparation Checklist for Mid-Server Architecture

Here's a simple checklist to keep track of the key tasks as you prepare your Mid-Server architecture:

- **Network and Connectivity:**
  - Ensure the Mid-Server can connect to your target systems and ServiceNow instance.
  - Verify firewall and proxy settings.
- **Server Requirements:**
  - Ensure the server has sufficient **CPU**, **memory**, and **disk space** to handle your needs.
  - Consider scalability for future growth.
- **Mid-Server Installation:**
  - Download and install the **Mid-Server** from ServiceNow.
  - Validate system requirements (e.g., Java version, OS compatibility).
- **Security Setup:**
  - Configure **SSL/TLS** and other encryption protocols for secure communication.
  - Set up user roles and **access control** for Mid-Server operations.
- **Discovery & Orchestration Configuration:**
  - Define your discovery probes, **pattern configurations**, and orchestration workflows.
  - Test discovery probes to ensure they are functioning properly.
- **Redundancy and High Availability:**
  - Decide if you need multiple Mid-Servers for failover or load balancing.
  - Set up failover rules and **load balancing** as necessary.

- **Monitoring & Alerts:**
  - Set up the **Mid-Server Health Dashboard** for continuous monitoring.
  - Define alert rules to catch any failures or performance issues early.

Top Mistakes to Avoid When Building a Mid-Server Architecture

As with any IT project, there are a few common mistakes that can trip you up. Here are the **top mistakes** you should watch out for:

1. **Ignoring Network Configuration:**
   Network access is crucial! Don't forget to check firewall rules, proxy settings, and ensure your Mid-Server can talk to both **ServiceNow** and your target systems.
2. **Underestimating Resource Needs:**
   Make sure the Mid-Server is running on hardware that can handle your workload. Don't set up on a machine that's already running multiple other services—give it the resources it needs!
3. **Lack of High Availability:**
   If you're running critical discovery or orchestration jobs, not having a backup Mid-Server in place can cause major headaches when things go wrong. Always plan for redundancy.
4. **Skipping Test Configurations:**
   It's tempting to move on after installing the Mid-Server, but skipping tests on your discovery probes and orchestration workflows is a big mistake. Make sure everything works as expected before going live!
5. **Not Monitoring the Mid-Server:**
   The Mid-Server needs attention too! Don't just set it and forget it. Make sure you're actively monitoring its performance and health to catch issues before they turn into problems.
6. **Overcomplicating Permissions and Security:**
   It's easy to go overboard with permissions, but try to avoid excessive complexity. Keep it simple and only grant necessary permissions to minimize risk.

Summary

Building a successful ITOM Mid-Server architecture in ServiceNow is all about planning ahead and getting the little details right. By carefully considering network setup, security, and scalability, you can ensure your Mid-Server is performing at its best. Don't forget to monitor its health and scale as needed, and always leave room for growth in your architecture.

With the right preparation, you'll have a reliable, high-performance ITOM Mid-Server setup that enables your ServiceNow instance to communicate seamlessly with your systems—ultimately streamlining your operations and setting the stage for success!

Mid-Server Test Plan for ServiceNow ITOM Setup

When you're setting up **ServiceNow Mid-Servers**, it's crucial to test everything to ensure it's working smoothly. This test plan is designed to cover a variety of scenarios that confirm your Mid-Servers are properly set up, including connectivity, performance, security, and redundancy. Testing these areas will help you avoid any nasty surprises down the road.

Objective

Ensure that the **ServiceNow Mid-Servers** are configured and functioning properly, verifying network connectivity, performance, security, and redundancy. The test plan will validate both the **core installation** and **specific use cases** like discovery and orchestration.

Test Plan Overview

- **Test Categories:**
    1. **Installation & Basic Configuration**
    2. **Network Connectivity**
    3. **Security & Permissions**
    4. **Performance & Load**
    5. **Discovery & Orchestration Functionality**
    6. **High Availability & Failover**

Test Cases

1. Installation & Basic Configuration

Objective: Ensure the Mid-Server is installed properly and the basic configuration is correct.

- **Test Case 1.1: Verify Mid-Server Installation**
    - **Description:** Confirm that the Mid-Server is installed successfully on the specified server.
    - **Steps:**
        - Check the Mid-Server log for any installation errors.
        - Ensure the Mid-Server is listed as **"Active"** in the **Mid-Server Dashboard**.
    - **Expected Results:** No installation errors, Mid-Server is online.
- **Test Case 1.2: Verify Configuration in ServiceNow**

- **Description:** Ensure that the Mid-Server is correctly configured in ServiceNow.
- **Steps:**
  - Go to **Mid-Server Setup** in the ServiceNow platform.
  - Verify that the **MID Server Name**, **IP Address**, and **Version** are correct.
  - Ensure that the **Status** is "Active".
- **Expected Results:** Mid-Server is correctly listed and showing the correct configuration details.

---

2. Network Connectivity

Objective: Validate that the Mid-Server can communicate with both the ServiceNow instance and target systems.

- **Test Case 2.1: Verify Connectivity to ServiceNow Instance**
  - **Description:** Ensure that the Mid-Server can reach the ServiceNow instance over the network.
  - **Steps:**
    - Attempt to establish a connection between the Mid-Server and ServiceNow.
    - Check if the Mid-Server appears as "Active" in the **Mid-Server Dashboard** in ServiceNow.
  - **Expected Results:** Successful communication; Mid-Server shows as **"Active"** in the dashboard.
- **Test Case 2.2: Test Connectivity to Target Systems (e.g., servers, databases)**
  - **Description:** Ensure the Mid-Server can access target systems (servers, databases, network devices) for discovery or orchestration tasks.
  - **Steps:**
    - Run a test discovery probe (e.g., for a server, network device, or database).
    - Check for successful connection and data retrieval.
  - **Expected Results:** The Mid-Server successfully discovers and retrieves data from target systems.
- **Test Case 2.3: Verify Proxy/Firewall Configurations**
  - **Description:** Ensure that firewalls and proxies are correctly configured to allow traffic to/from the Mid-Server.

- **Steps:**
  - Confirm the correct ports are open (e.g., HTTP, HTTPS, SNMP, SSH).
  - Perform a test to ensure traffic can flow through any firewall or proxy in place.
- **Expected Results:** Mid-Server can establish communication despite proxy/firewall configurations.

---

3. Security & Permissions

Objective: Test the security configurations to ensure proper access control and encryption.

- **Test Case 3.1: Verify SSL/TLS Encryption**
  - **Description:** Ensure that all communication between the Mid-Server and ServiceNow is encrypted.
  - **Steps:**
    - Check the **SSL certificate** used by the Mid-Server.
    - Verify that **SSL/TLS encryption** is enabled for communication between the Mid-Server and ServiceNow.
  - **Expected Results:** Communication is secured via SSL/TLS encryption.
- **Test Case 3.2: Verify Access Control and User Permissions**
  - **Description:** Verify that the right permissions are granted to the Mid-Server for accessing target systems and the ServiceNow platform.
  - **Steps:**
    - Check user roles and permissions assigned to the Mid-Server.
    - Validate that the Mid-Server has **read/write** access to required resources in ServiceNow.
  - **Expected Results:** Mid-Server has the correct permissions for discovery, orchestration, and communication.

---

4. Performance & Load

Objective: Ensure that the Mid-Server can handle the required workload without performance degradation.

- **Test Case 4.1: Test Performance Under Normal Load**

- **Description:** Test how the Mid-Server performs under typical load (e.g., normal number of discovery jobs or orchestration tasks).
- **Steps:**
  - Run several discovery probes or orchestration tasks.
  - Monitor the **CPU**, **memory usage**, and **network latency** of the Mid-Server during operations.
- **Expected Results:** Mid-Server performs without resource overuse or slowdowns.

- **Test Case 4.2: Test Performance Under High Load**
  - **Description:** Test how the Mid-Server performs under heavy load (e.g., multiple discovery jobs running simultaneously).
  - **Steps:**
    - Trigger simultaneous discovery and orchestration tasks.
    - Monitor for any performance issues (e.g., lag, failed tasks).
  - **Expected Results:** The Mid-Server handles the load without significant performance degradation.

---

5. Discovery & Orchestration Functionality

Objective: Ensure that the Mid-Server is fully functional for discovery and orchestration tasks.

- **Test Case 5.1: Verify Discovery of Servers and Network Devices**
  - **Description:** Ensure the Mid-Server can discover servers, network devices, and other systems.
  - **Steps:**
    - Run discovery probes for servers, network devices, and databases.
    - Check if discovered items appear in the **Configuration Management Database (CMDB)**.
  - **Expected Results:** Devices and servers are discovered and correctly mapped in the CMDB.

- **Test Case 5.2: Verify Orchestration Workflow Execution**
  - **Description:** Test the Mid-Server's ability to run orchestration tasks.
  - **Steps:**

- Run an orchestration workflow (e.g., start/stop services, automate incident response).
- Check if the task completes successfully and actions are performed on the target system.

- **Expected Results:** Orchestration tasks are executed successfully.

---

6. High Availability & Failover

Objective: Ensure the Mid-Server setup includes redundancy and failover capabilities to maintain uptime.

- **Test Case 6.1: Test Mid-Server Failover**
  - **Description:** Test the failover capabilities by simulating a Mid-Server failure.
  - **Steps:**
    - Take one Mid-Server down (either manually or by disabling it).
    - Verify that traffic is routed to a backup Mid-Server and operations continue without interruption.
  - **Expected Results:** Failover occurs seamlessly, and operations are not impacted.
- **Test Case 6.2: Test Load Balancing Between Mid-Servers**
  - **Description:** Ensure that multiple Mid-Servers are load-balanced correctly.
  - **Steps:**
    - Run simultaneous discovery or orchestration tasks across multiple Mid-Servers.
    - Monitor the load distribution.
  - **Expected Results:** Load is evenly distributed across all active Mid-Servers.

Conclusion

This test plan covers the key areas necessary to ensure that your ServiceNow **Mid-Servers** are set up correctly and functioning at their best. Testing these scenarios helps ensure reliable **discovery**, **orchestration**, and **overall performance**. By conducting these tests, you'll ensure your ServiceNow platform is running smoothly, securely, and efficiently.

Remember, testing is your best defense against those "oops" moments that pop up when you're least expecting them.

About Mana'o Pili ↘

Building a Solid ITOM Mid-Server Architecture in ServiceNow: A Step-by-

'ike (knowledge) level: Novice

Rev. February 9, 2025

Mana'o Pili is a Hawai'i based technology consulting firm specializing in business automation through ServiceNow. Mana'o Pili provides its customers with individualized solutions. We reject the notion of one-size-fits-all solutions. Instead, we partner with you to craft a tailored plan that aligns with your unique needs, budget, and objectives. Our approach focuses on optimizing your existing platform while minimizing customization and reducing technical debt.

Here at Mana'o Pili, we treat our customers as 'ohana (family), listen closely to your challenges and deliver tailored attention with exceptional service.