Discovery Tool Agent – V1

Discovery Agent Overview

1. Introduction

The Discovery Agent is an automated tool designed to identify and collect information from infrastructure resources within an enterprise environment. It gathers system-level and database-level details from on-premises servers and workstations to support monitoring, optimization, and migration planning. The agent supports both Windows and Linux platforms.

2. Deployment Model

• Installation: Deployed on a machine within the network.

• Execution: Runs with administrator privileges to allow scanning of remote systems using provided credentials.

3. Scanning Capabilities

3.1 Machine Discovery

• Performs network ping to detect live machines across defined IP ranges.

• Supports both single and multiple credential configurations.

• Windows: Uses WMI and PowerShell remoting.

• Linux: Uses SSH access.

3.2 System Information Collection

Windows Systems

• Machine name
• Operating system version
• Installed RAM capacity
• CPU core count
• RAM utilization
• CPU utilization
• Storage details (optional)

Linux Systems

• Hostname
• OS distribution and version (e.g., Ubuntu 22.04, RHEL 9)
• Installed RAM capacity
• CPU core count
• RAM utilization
• CPU utilization

• Disk usage
• Running services summary (optional)

3.3 Application Discovery

• Collects installed applications and components.
• Captures application name, version, publisher, and installation date.

3.4 Roles and Features Discovery

• Enumerates Windows roles and enabled features.
• Captures role or service names and their status.
• Provides insight into server workloads such as IIS, Active Directory, and Hyper-V.

3.5 Network Connection Analysis

• Executes netstat or equivalent commands to capture open ports and listening services.
• Identifies active TCP and UDP connections, local and remote addresses.
• Highlights potential security risks from unauthorized network services.

3.6 Database Connectivity Validation

The agent validates connectivity to supported databases when IP address, credentials, and port are provided. Automatic database discovery is not included. Database servers must have TCP/IP enabled.

3.7 Supported Databases & Default Ports

Database Type	Default Port	Notes
Microsoft SQL Server	1433	Requires valid DB credentials
MySQL	3306	Requires valid DB credentials
PostgreSQL	5432	Requires valid DB credentials

3.8 Collected Database Information

When database connectivity is established, the following details are collected:
• Instance name
• List of available databases
• CPU and RAM usage of the database process
• Additional relevant metadata

4. Security Considerations

- Credentials are encrypted and handled securely during execution.
- Connections follow least-privilege principles.
- All collected data remains within the organization's environment.

5. Limitations

- Databases must be manually specified with IP, credentials, and port.
- Non-domain or domain-leave machines are not supported.
- Requires WMI and PowerShell remoting for Windows.
- Requires SSH access for Linux.
- Administrator or root credentials are required for complete data collection.

6. Key Features

- Lightweight installation on a single domain machine.
- Network scanning via IP range or hostname list.
- Flexible credential management (single or multiple).
- Unified system and database discovery.
- Cross-platform support for Windows and Linux.

7. Flow Diagram