PHASE 16: Monitoring & Alerts

This phase focuses on implementing real-time monitoring and alerting across your hybrid infrastructure using only free or built-in tools. The goal is to gain visibility into device health, security events, system performance, and service availability across your environment — both on-prem and cloud — without relying on paid tools.

Tools Used:

- Intune Endpoint Analytics (cloud)
- Windows Event Viewer & Event Forwarding (on-prem)
- Windows Performance Monitor
- Custom PowerShell alert scripts

I. Intune Endpoint Analytics Setup (Cloud Monitoring)

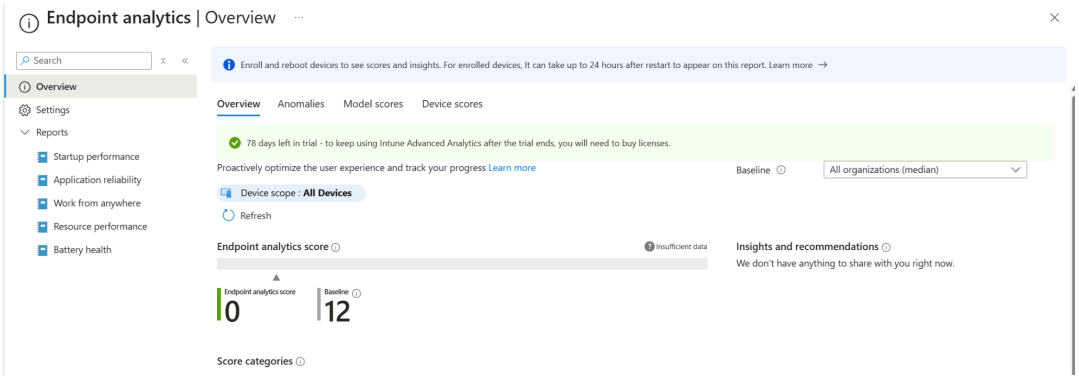
Actions Completed:

Step 1: Enable Endpoint Analytics

- Go to: https://endpoint.microsoft.com
- Navigate to: Reports → Endpoint Analytics
- Click Start → Assign it to an existing device group (e.g., "Autopilot Devices" or “Cloud Devices”)

Step 2: Wait for 24–48 Hours for Initial Data

Data such as startup times, crash metrics, and compliance will populate over time.



Step 3: Monitor Device Health

From the Endpoint Analytics dashboard, review:

- Startup score (boot time, last restart)
- App reliability (crash frequency)
- Device compliance and encryption
- Antivirus & firewall health

🧪 Validation:

Open a managed device → Restart it → Wait for data to sync.

On the dashboard, verify the device appears with telemetry details.

🛠️ Common Issue:

❌ Devices not showing up

✅ Resolution: Ensure they are enrolled in Intune, assigned to the analytics group, and rebooted once.

II. Event Viewer + Windows Event Forwarding (On-Prem)

Centralize logs from all important VMs (DC01, CA01, FS01, JumpBox) to one server (LOG01).

Actions Completed:

Step 1: Configure LOG01 as Collector

- Open Event Viewer → Click Subscriptions (enable event forwarding if prompted)
- Click "Create Subscription"

  Name: "Infra Logs"

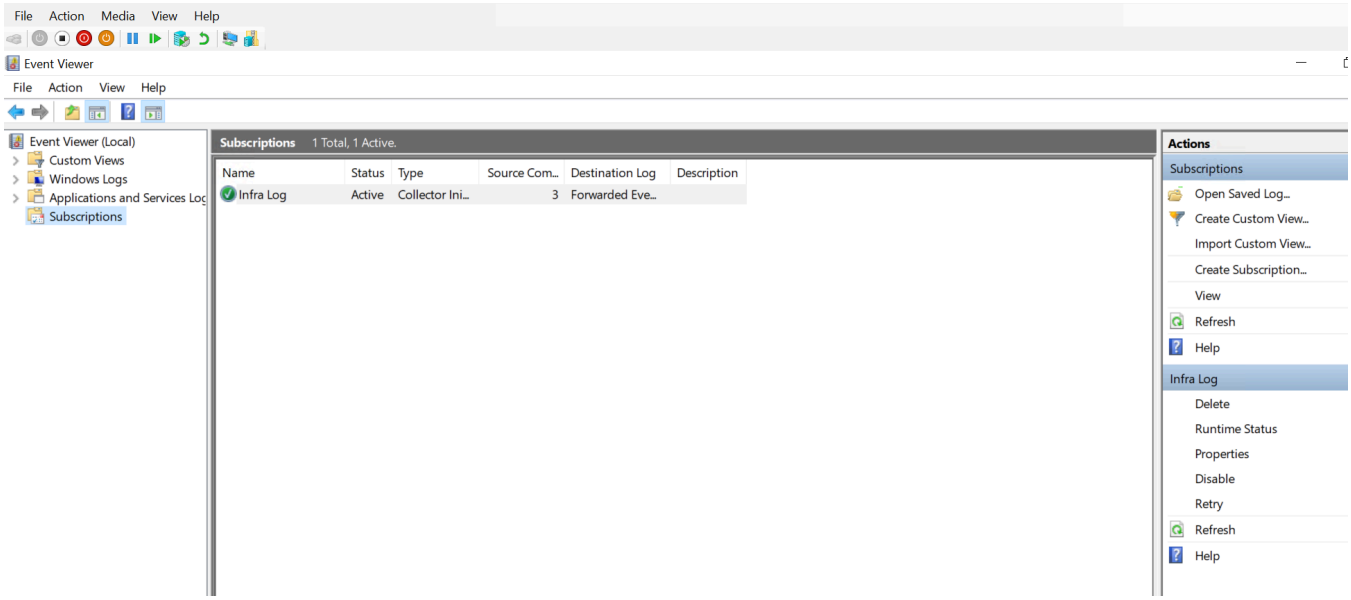
  Collector: LOG01

  Source Computers: Add DC01, CA01, JumpBox

  Events:

  - Logon events
  - RDP failures

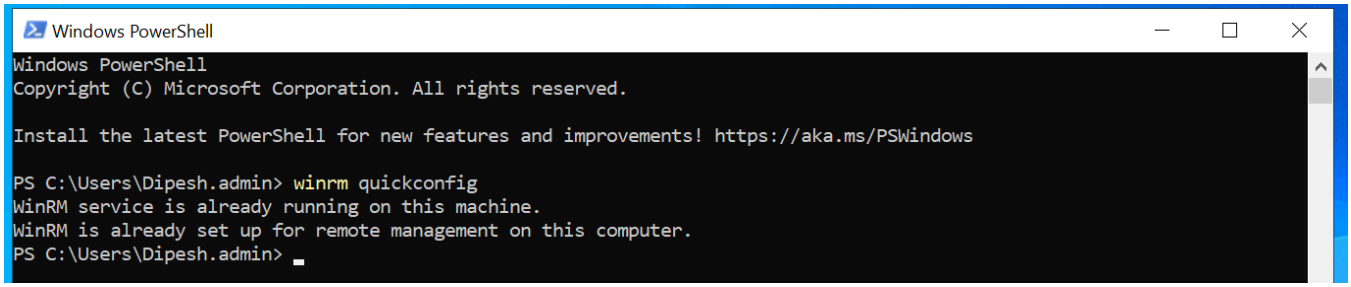
- Application errors
- Service crashes (e.g., osTicket, Exchange)



Step 2: Enable WinRM on Each Source Server

Run the following in Poweshell on DC01, CA01, FS01, JumpBox:

- winrm quickconfig



Step 3: Enable via Group Policy

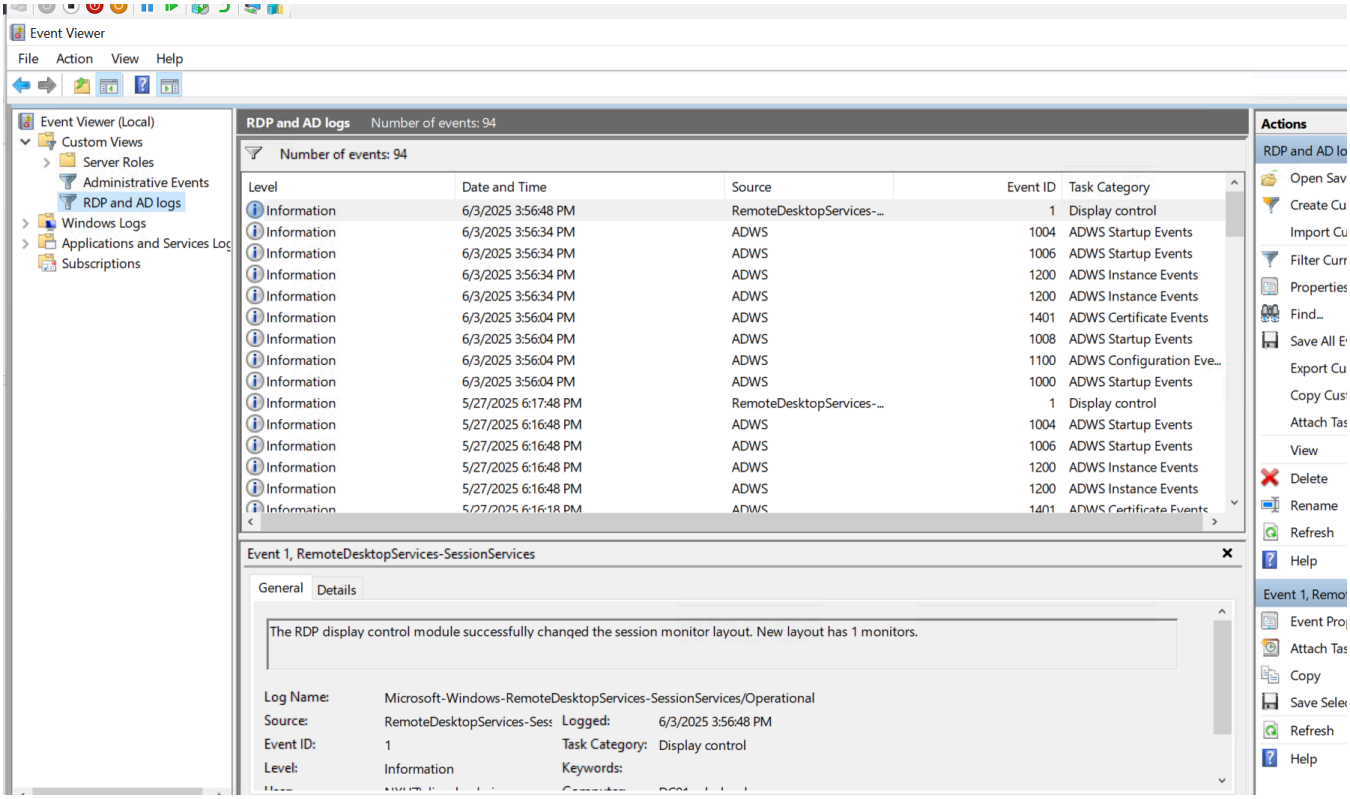
On DC01:

- Go to Group Policy Management → Create a new GPO: “Enable WinRM for Event Forwarding”
- Computer Configuration → Policies → Administrative Templates → Windows Components → Event Forwarding → Enable “Configure target Subscription Manager”

Step 4: Create Custom Views (LOG01)

Inside Event Viewer on LOG01:

- Create views for:
  - RDP login failures (Event ID 4625)
  - AD account lockouts (Event ID 4740)
  - osTicket crash (ID varies by service)



🛠️ Common Issue:

❌ No logs appearing in LOG01

✅ Resolution: Ensure the firewall is open on port 5985 (WinRM) and that source machines trust the collector.

III. Performance Monitoring (Built-in)

Actions Completed:

Step 1: Launch Performance Monitor

Run: `perfmon.msc`

Step 2: Create a Data Collector Set

- Right-click Data Collector Sets → User Defined → New → Data Collector Set
- Name: “InfraHealth”
- Choose: “Create Manually”
- Add Counters:
  - Processor → % Processor Time
  - Memory → Available MBytes
  - PhysicalDisk → Disk Read/Write
  - Network Interface → Bytes Sent/sec

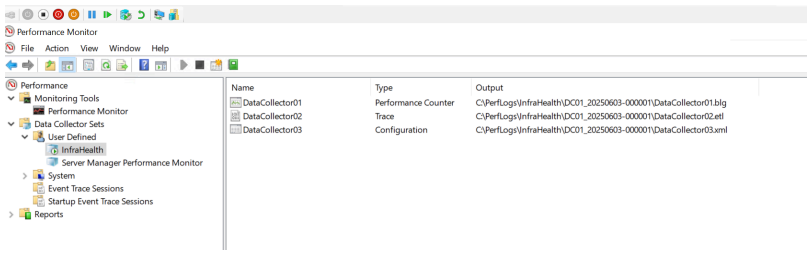
Step 3: Set Sample Interval

- Set: 30 seconds or 1 minute
- Set output to folder: `C:\PerfLogs\InfraHealth`

Step 4: Start Collection

Right-click → Start

Run for a few hours → Stop → View report under “Reports”



IV. PowerShell-Based Alerting Scripts

Actions Completed:

Script: Alert for Failed Login Events

```
$events = Get-WinEvent -FilterHashtable @{LogName="Security"; ID=4625;
StartTime=(Get-Date).AddMinutes(-10)}

if ($events.Count -gt 5) {

    Send-MailMessage -To "admin@dipeshcorp.com" -From "monitor@dipeshcorp.com"
-SmtpServer "smtp.office365.com" -UseSsl `

    -Subject "ALERT: Too many failed logins" -Body "$($events.Count) failed
logins in 10 mins"

}
```

Step 1: Save as MonitorFailedLogin.ps1

Step 2: Use Task Scheduler to run every 10 minutes

Task Trigger: Daily → Repeat every 10 minutes

Action: Start a program → powershell.exe -File "C:\Scripts\MonitorFailedLogin.ps1"

🛠️ Common Error:

❌ Send-MailMessage fails

✅ Fix: Use valid SMTP settings + Use App Password if MFA is enabled