

# Windows Server 2022: Monitor and Troubleshoot Server Environments

---

## Monitor Windows Server Using Local Tools



**Tim Warner**

Microsoft Azure Solutions Architect

@TechTrainerTim   TechTrainerTim.com



# Overview



**Manage event logs**

**Monitor Windows Server by using  
Performance Monitor**

**Data Collector Sets**

**Monitor servers and configure alerts by  
using Windows Admin Center**

**System Insights**



# Windows Server 2022: Monitor and Troubleshoot Server Environments

**Monitor Windows Server Using Local Tools**

**Monitor Windows Server Using Azure Services**

**Troubleshoot Windows Server Hybrid Networking**

**Troubleshoot Windows Server VM Deployment Failures**

**Troubleshoot Windows Server VM Connection Issues**

**Troubleshoot Active Directory**



# Windows Server Hybrid Administrator Associate

Take two exams



CERTIFICATION EXAM **AZ-800**  
**Administering Windows Server  
Hybrid Core Infrastructure**

AND



CERTIFICATION EXAM **AZ-801**  
**Configuring Windows Server  
Hybrid Advanced Services**

Earn the certification



ASSOCIATE CERTIFICATION  
**Microsoft Certified:  
Windows Server Hybrid  
Administrator Associate**

**One-year cert validity**



# Exercise Files

Timothy  
timothywarner316@gmail.com

## Troubleshooting with Microsoft Azure Network Watcher

by Tim Warner

Microsoft now gives you packet-level access to your Windows Server and Linux virtual machines (VMs) running in Azure. You'll learn how to use Network Watcher to troubleshoot network security groups (NSGs), perform packet captures, and much more.

Bookmark Add to Channel

Table of contentsDescriptionTranscript**Exercise files**DiscussionLearning CheckRecommended

These exercise files are intended to provide you with the assets you need to create a video-based hands-on experience. With the exercise files, you can follow along with the author and re-create the same solution on your computer. We find this to be even more effective than written lab exercises.

Course author

**Tim Warner**

Timothy Warner is a Microsoft Most Valuable Professional (MVP) in Cloud and Datacenter Management who is based in Nashville, TN.

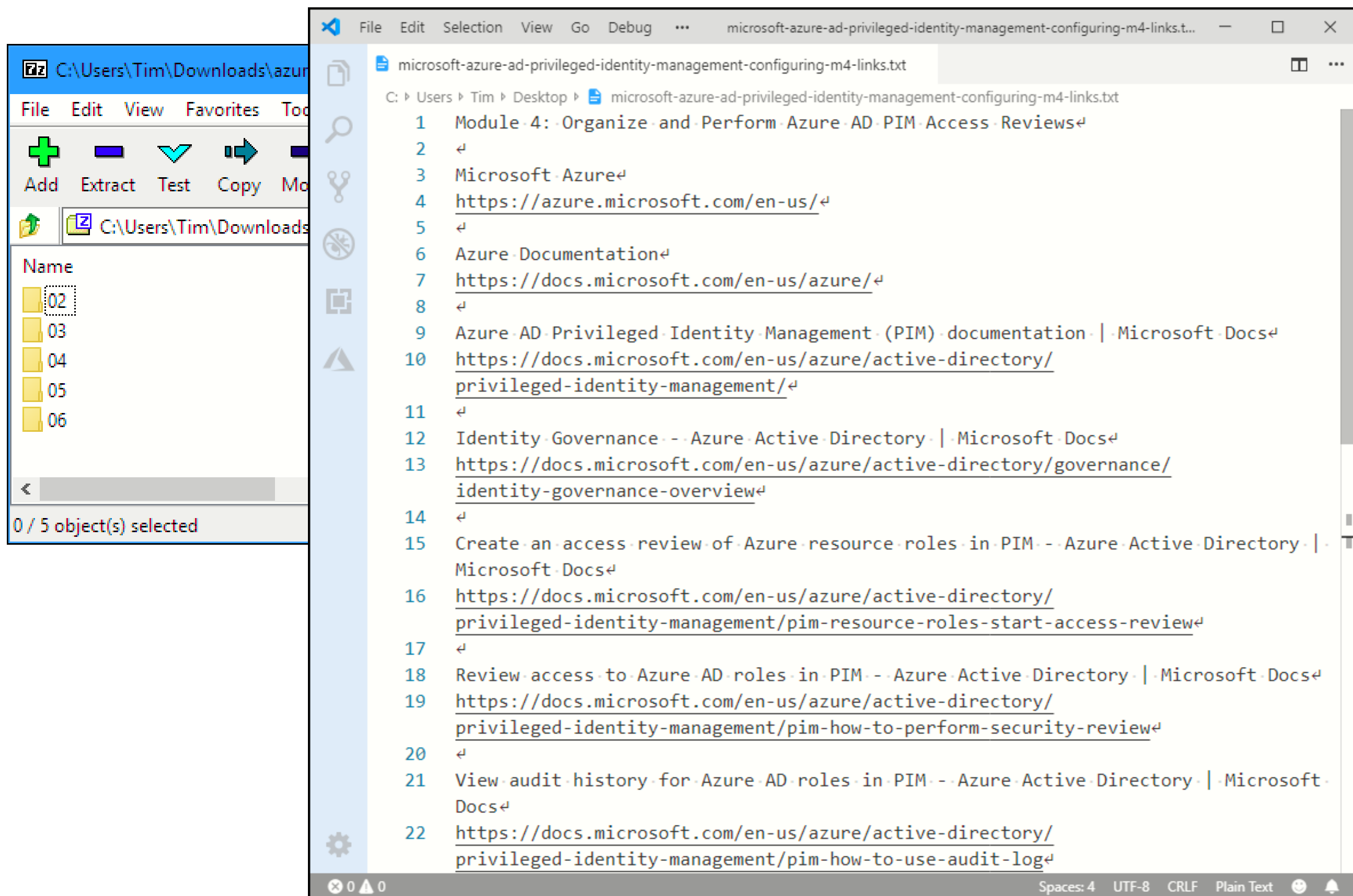
Course info

Level	Intermediate
Rating	★★★★★
My rating	★★★★★
Duration	2h 12m
Released	31 Oct 2017

Share course



# Exercise Files



# Event Logs



# Event

**Notification of a state change as programmed by an application developer.**





# Event Logs - Event Viewer

The screenshot shows the Windows Event Viewer application. The left-hand pane displays the 'Event Viewer (Local)' tree with 'Applications and Services Logs' highlighted in a red box. The right-hand pane shows a list of events under the 'Application' log, with 5,413 events in total. The selected event is 'Information' level, dated '5/3/2022 7:38:05 AM', from the source 'Windows Error Reporting', with Event ID '1001' and Task Category 'None'. Below this list, the 'Event 1001, Windows Error Reporting' details are shown in the 'General' tab. The details include a fault bucket, event name 'DPMException', and a problem signature with parameters P1 through P6. At the bottom, a summary table provides key information about the event.

Level	Date and Time	Source	Event ID	Task Category
Information	5/3/2022 7:38:33 AM	CAPI2	4097	None
Information	5/3/2022 7:38:14 AM	Windows Error Reporting	1001	None
Information	5/3/2022 7:38:05 AM	Windows Error Reporting	1001	None
Information	5/3/2022 7:38:05 AM	Windows Error Reporting	1001	None
Information	5/3/2022 7:28:23 AM	Security-SPP	16384	None
Information	5/3/2022 7:27:47 AM	Security-SPP	16394	None

Event 1001, Windows Error Reporting

General Details

Fault bucket, type 0  
Event Name: DPMException  
Response: Not available  
Cab Id: 0

Problem signature:  
P1: cbengine  
P2: 2.0.9245.0  
P3: cbengine.exe  
P4: 2.0.9245.0  
P5: System.Configuration.ConfigurationErrorsException  
P6: System.Configuration.BaseConfigurationRecord.EvaluateOne

Log Name:	Application		
Source:	Windows Error Reporting	Logged:	5/3/2022 7:38:05 AM
Event ID:	1001	Task Category:	None
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	mem1.timw.info
OpCode:	Info		
More Information:	<a href="#">Event Log Online Help</a>		



# Event Logs - PowerShell

```
PS C:\> get-winevent -ListLog system, security, application
```

LogMode	MaximumSizeInBytes	RecordCount	LogName
Circular	20971520	16844	System
Circular	20971520	25480	Security
Circular	20971520	5413	Application

```
PS C:\> Get-EventLog -LogName System -Newest 5
```

Index	Time	EntryType	Source	InstanceID	Message
16844	May 03 08:02	Information	Service Control M...	1073748860	The AppX Deployment Service (AppXSVC) service ent...
16843	May 03 08:02	Information	Service Control M...	1073748860	The AppX Deployment Service (AppXSVC) service ent...
16842	May 03 08:01	Information	Service Control M...	1073748860	The Device Management Wireless Application Protoc...
16841	May 03 07:58	Information	Service Control M...	1073748860	The Network Setup Service service entered the sto...
16840	May 03 07:57	Error	DCOM	10028	The description for Event ID '10028' in Source 'D...



# Event Logs - Server Manager

The screenshot displays the Windows Server Manager interface. On the left-hand navigation pane, the 'DHCP' option is highlighted with a red rectangular box. The main content area is divided into two sections: 'SERVERS' and 'EVENTS', both of which are also highlighted with red rectangular boxes.

**SERVERS Section:**

- Header: SERVERS, All servers | 1 total
- Filter: [Filter] [Search icon] [List icon] [Refresh icon]
- Table:

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
MEM1	10.1.10.165,172.25.160.1	Online - Data retrieval failures occurred	5/3/2022 7:36:55 AM	00456-50300-40731-AA697 (Activated)

**EVENTS Section:**

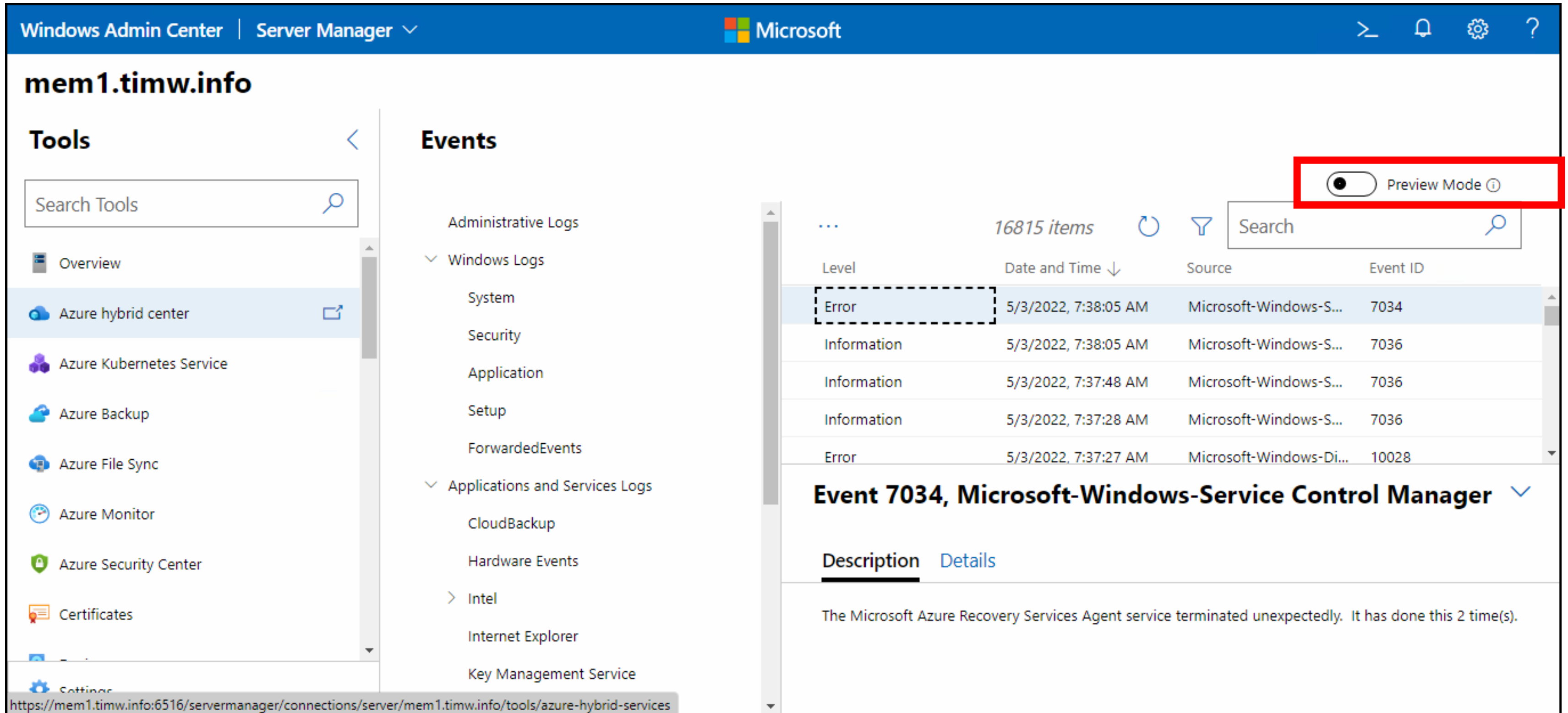
- Header: EVENTS, All events | 9 total
- Filter: [Filter] [Search icon] [List icon] [Refresh icon]
- Table:

Server Name	ID	Severity	Source	Log	Date and Time
MEM1	1036	Error	Microsoft-Windows-DHCP-Server	System	5/3/2022 7:07:07 AM
MEM1	1035	Error	Microsoft-Windows-DHCP-Server	System	5/3/2022 7:07:07 AM
MEM1	10020	Warning	Microsoft-Windows-DHCP-Server	System	5/3/2022 6:59:15 AM

Below the table, a message is displayed: "This computer has at least one dynamically assigned IPv6 address. For reliable DHCPv6 server operation, you should use only static IPv6 addresses."



# Event Logs - Windows Admin Center



Windows Admin Center | Server Manager

mem1.timw.info

**Tools**

Search Tools

- Overview
- Azure hybrid center
- Azure Kubernetes Service
- Azure Backup
- Azure File Sync
- Azure Monitor
- Azure Security Center
- Certificates
- Settings

**Events**

Administrative Logs

- Windows Logs
  - System
  - Security
  - Application
  - Setup
  - ForwardedEvents
- Applications and Services Logs
  - CloudBackup
  - Hardware Events
  - Intel
  - Internet Explorer
  - Key Management Service

16815 items

Level	Date and Time	Source	Event ID
Error	5/3/2022, 7:38:05 AM	Microsoft-Windows-S...	7034
Information	5/3/2022, 7:38:05 AM	Microsoft-Windows-S...	7036
Information	5/3/2022, 7:37:48 AM	Microsoft-Windows-S...	7036
Information	5/3/2022, 7:37:28 AM	Microsoft-Windows-S...	7036
Error	5/3/2022, 7:37:27 AM	Microsoft-Windows-Di...	10028

**Event 7034, Microsoft-Windows-Service Control Manager**

Description Details

The Microsoft Azure Recovery Services Agent service terminated unexpectedly. It has done this 2 time(s).

Preview Mode

https://mem1.timw.info:6516/servermanager/connections/server/mem1.timw.info/tools/azure-hybrid-services



# Event Log Management

**Group Policy**

**Event Log subscriptions**

**System Center Operations Manager**

**Azure Log Analytics**

**Third-party solutions**



# Performance Monitor





# Performance Monitor



**Native Windows system monitoring tool**

**Real-time statistics**

**Data Collector Set (DCS)**

- Performance counters
- Event traces
- System configuration information

**Best to capture remotely**

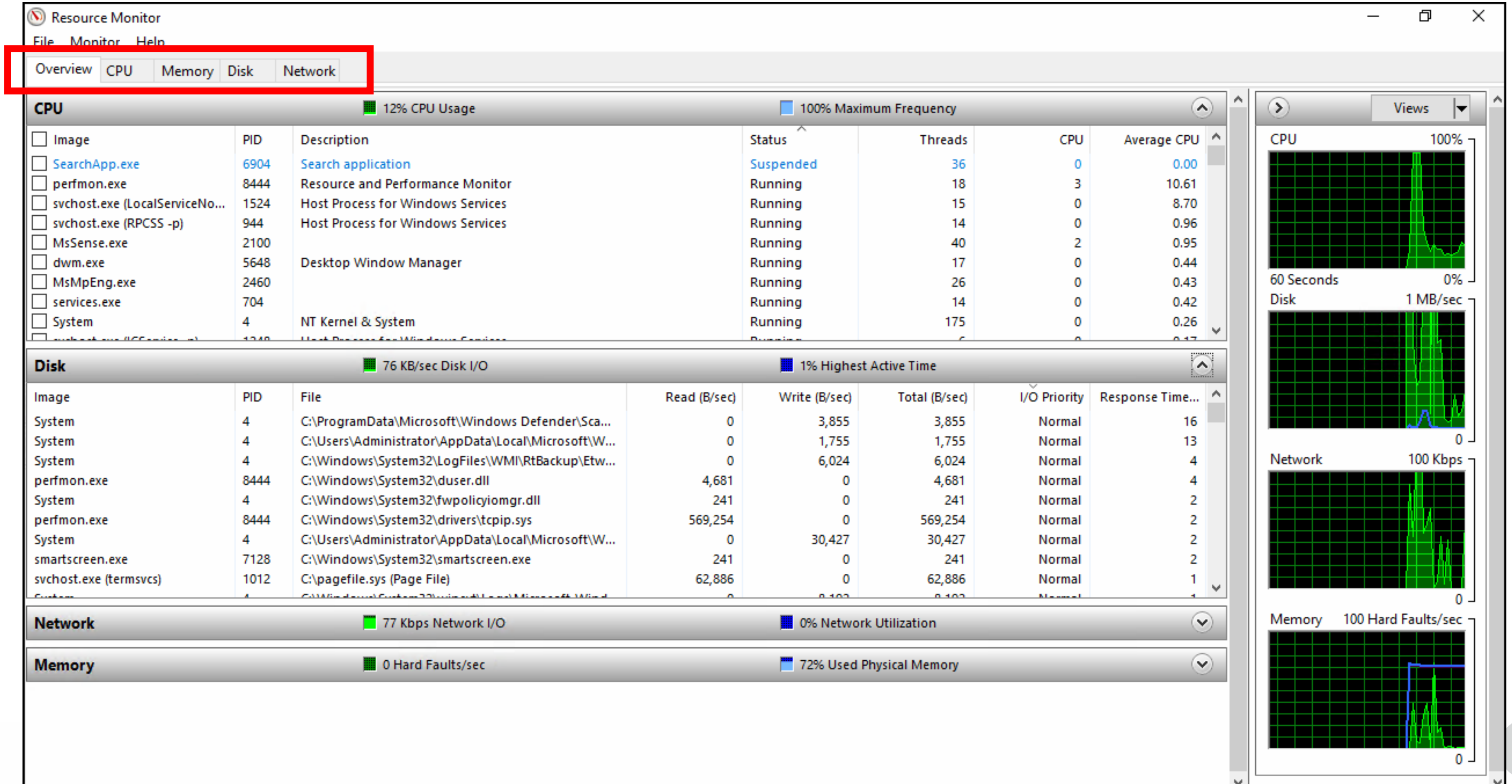


# Performance Monitor Terminology

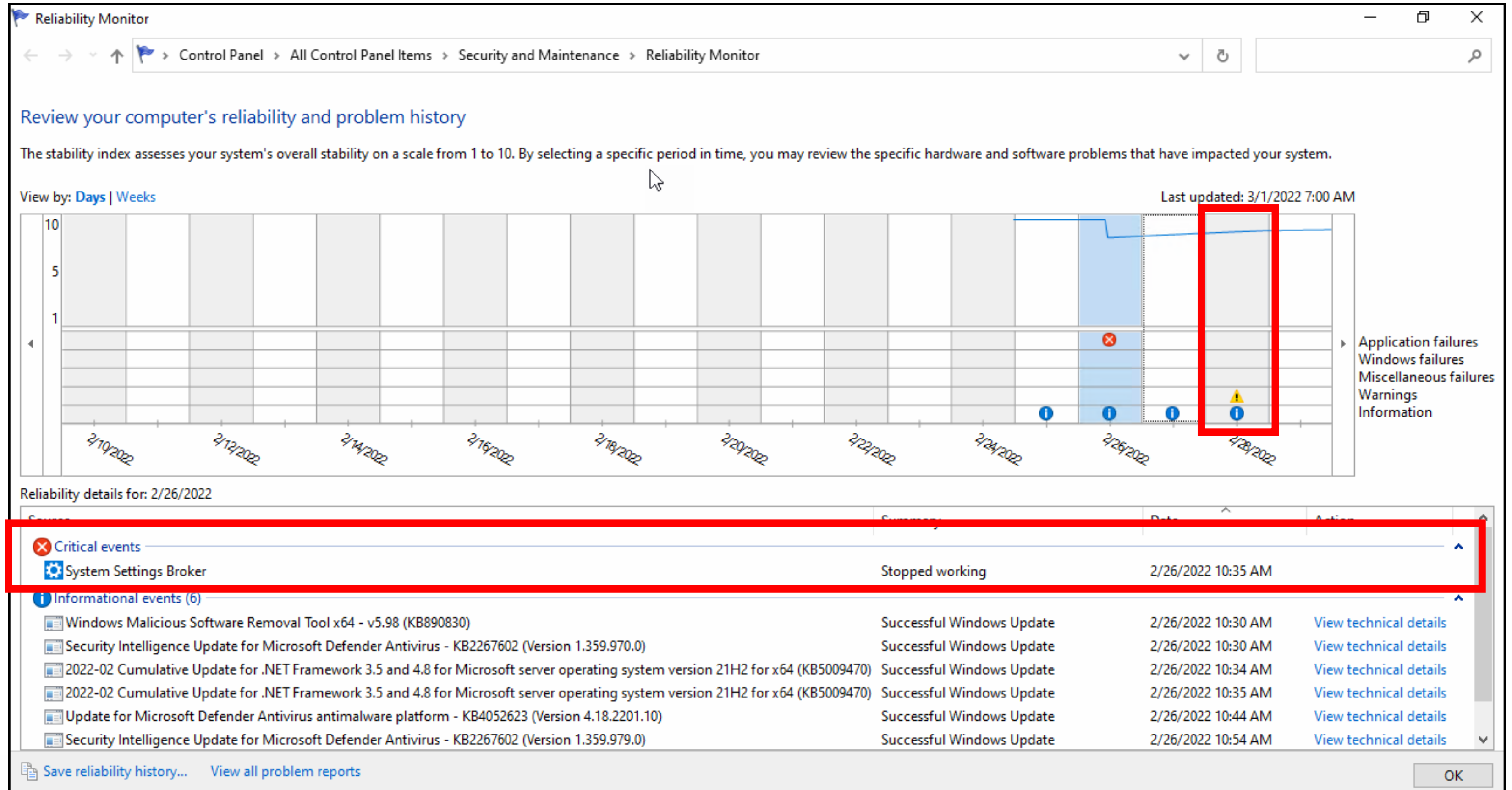
```
Get-Counter -Counter "\Processor(_Total)\% Processor Time"  
            -SampleInterval 2 -MaxSamples 3
```



# Resource Monitor



# Reliability Monitor



Demo



1

**Task Manager**

**Resource Monitor**

**Reliability Monitor**

**Performance Monitor**

**DCS**

**Event log**

**Log Analytics agent configuration**



# Windows Admin Center and System Insights





# System Insights

**Runs locally on  
Windows Server**

**Predictive analytics  
with no cloud  
dependency**

**One year data  
retention**

**Configure with WAC**

**CPU & network  
capacity  
forecasting**

**Storage & volume  
consumption  
forecasting**



Demo



2

**View System Insights data**



## Summary



**Strongly consider using Azure Log Analytics for centralized hybrid cloud event management**

- Azure Arc-enabled servers

**Kusto Query Language (KQL) is used universally across the Microsoft Cloud Platform**



Up Next:

Monitor Windows Server Using Azure Services

---

