**Nuclear Smuggling Detection and Deterrence Program**

**Communications Systems Monitor**

***Daily File Specification***

February 2017

Revision 1.0

Office of Global Material Security

National Nuclear Security Administration

U.S. Department of Energy

This page intentionally left blank.

Table of Contents

[1 Introduction 1](#_Toc469580524)

[2 File Naming 1](#_Toc469580525)

[3 COMMON Daily File Fields 1](#_Toc469580526)

[3.1 Identification Field 1](#_Toc469580527)

[3.2 Collector Fields 1](#_Toc469580528)

[3.2.1 Collector Descriptions 2](#_Toc469580529)

[3.3 Type Field 6](#_Toc469580530)

**Tables**

[Table 1 - COMMON Collector Type IDs 6](#_Toc469580531)

**Abbreviations/Acronyms**

CDF COMMON daily file

COMMON Communications Systems Monitor

JSON JavaScript Object Notation

NSDD Nuclear Smuggling Detection and Deterrence

# Introduction

The Nuclear Smuggling Detection and Deterrence (NSDD) Program has developed the Communications Systems Monitor (COMMON) Tool to assess the status of communications systems by collecting data about the system. The COMMON daily file (CDF) is a text file in JavaScript Object Notation (JSON) that stores data collected each day for configured devices of communications systems. These items can include networked sensors, computers, cameras, network equipment, software and process, and databases. All of the data collected by COMMON and stored in the local COMMON database is written to the CDF for future analysis, which will assist in determining trends, issues, and overall system performance of NSDD communications systems. This document describes the data collected by COMMON and how is it represented and formatted in the CDFs.

# File Naming

CDFs are automatically named by COMMON based on the configuration of the system. CDFs are generated using the country code and site name that is entered into the COMMON configuration. Additionally, there is a date added to the end of the filename. For example, if the country code is “US” and the site name is “Port\_of\_Albuquerque” and the date is November 1, 2016 then the daily file name would result in “us\_port\_of\_albuquerque\_2016\_11\_01.json” with a different date in YYYY\_MM\_DD format changing for each day a CDF is generated.

# COMMON Daily File Fields

This section describes the COMMON daily file fields in detail.

## Identification Fields

The COMMON daily file contains four overall fields. The countryCode, siteName, day, and records fields are all contained at the top of the document.

**countryCode:** Country Code of the country that the software is running, used in generating the Daily File names.

**siteName:** Site Name of the site where the software is running, used in generating the Daily File names.

**day:** Day for which this daily file contains data

**records:** Items of interest that COMMON collects and maintains. Each record contains the “collector” name (label), type, the values collected, and the timestamp.

## Records Collector Fields

*device*.Memory

*device*.Disk

*device*.CPUUsage

*device*.NICUsage

*device*.Uptime

*device*.LastBootTime

*device*.Processes

*system.*Ping

*device*.InstalledApplications

*device*.Services

*device*.DatabaseSize (not used)

*device*.SystemErrors

*device*.ApplicationErrors

*device*.DatabaseSize

*device*.UPS

*device*.DiskSpeed

### Collector Descriptions

The following are the types of collectors that are used by COMMON.

1. **Memory** – The amount of free random access memory (RAM) on a computer.

{

"collector": "CAS Server.Memory",

"type": 0,

"value": "{\"Value\":{\"Memory Capacity\":\"4294361088\",\"Free Memory\":\"2479149056\",\"Memory Used\":\"1815212032\"}}",

"timestamp": "2016-10-04T23:55:30.414202-06:00"

}

1. **Disk** – The total capacity of a logical disk volume and its free and used space.

{

"collector": "CAS Server.Disk",

"type": 1,

"value": "{\"Value\":{\"C:\":{\"Capacity\":64055406592,\"Free\":36957339648,\"Used\":27098066944}}}",

"timestamp": "2016-10-04T23:55:30.4292003-06:00"

}

1. **CPUUsage** – Percentage of CPU cycles being used by all CPUs on a computer.

{

"collector": "CAS Server.CPUUsage",

"type": 2,

"value": "{\"Value\":\"5\"}",

"timestamp": "2016-10-04T23:55:30.4448212-06:00"

}

1. **NICUsage** – The percentage of available bandwidth currently being used in bits per second.

{

"collector": "CAS Server.NICUsage",

"type": 3,

"value": "{\"Value\":{\"BPS\":\"5158\",\"Capacity\":\"250025000\",\"Avg\":\"0.0\"}}",

"timestamp": "2016-10-04T23:55:31.1031587-06:00"

}

1. **Uptime** – The total uptime since a computer was last rebooted.

{

"collector": "CAS Server.Uptime",

"type": 4,

"value": "{\"Value\":\"1 14:15:07\"}",

"timestamp": "2016-10-04T23:55:31.1031587-06:00"

}

1. **LastBootTime** – The last time a computer was rebooted.

{

"collector": "CAS Server.LastBootTime",

"type": 5,

"value": "{\"Value\":\"2016-10-03T09:40:23.4914540-06:00\"}",

"timestamp": "2016-10-04T23:55:31.3843967-06:00"

}

1. **Processes** – List of processes and the amount of CPU (in percentage) that they are using.

{

“collector": "CAS Server.Processes",

"type": 6, "value":"{\"Value\":{\"chrome\":\"0\",\"COMMON\":\"0\",\"COMMONConfig\":\"0\",\"conhost\":\"0\",\"csrss\":\"0\",\"dllhost\":\"0\",\"dwm\":\"0\",\"explorer\":\"0\",\"GoogleUpdate\":\"0\",\"lsass\":\"0\",\"LVSTest\":\"0\",\"mmc\":\"0\",\"msdtc\":\"0\",\"prime95\":\"0\",\"services\":\"0\",\"smss\":\"0\",\"spoolsv\":\"0\",\"sqlceip\":\"0\",\"sqlitebrowser\":\"0\",\"sqlservr\":\"0\",\"sqlwriter\":\"0\",\"svchost\":\"0\",\"System\":\"0\",\"taskeng\":\"0\",\"taskhostex\":\"0\",\"Taskmgr\":\"0\",\"TPAutoConnect\":\"0\",\"TPAutoConnSvc\":\"0\",\"TSARPMSimulator\":\"0\",\"VGAuthService\":\"0\",\"vmacthlp\":\"0\",\"vmtoolsd\":\"0\",\"w3wp\":\"0\",\"wininit\":\"0\",\"winlogon\":\"0\",\"WmiPrvSE\":\"0\"}}",

"timestamp": "2016-10-04T23:55:31.3979011-06:00"

}

1. **Ping** – The device’s IP address, the last time COMMON attempted to Ping a device on the network, whether or not it was successful, and the average response time of the ping in milliseconds.

{

"collector": "System.Ping",

"type": 7, "value":"{\"Value\":[{\"Address\":\"192.168.0.2\",\"IsPingable\":true,\"AvgTime\":1},{\"

Address\":\"192.168.0.3\",\"IsPingable\":false,\"AvgTime\":1000},{\"Address\":\"192.168.0.10\",\"IsPingable\":true,\"AvgTime\":0},{\"Address\":\"192.168.0.11\",\"IsPingable\":true,\"AvgTime\":200},{\"Address\":\"192.168.0.20\",\"IsPingable\":true,\"AvgTime\":0},{\"Address\":\"192.168.0.21\",\"IsPingable\":true,\"AvgTime\":0}]}",

"timestamp": "2016-10-04T23:55:25.6502747-06:00"

}

1. **InstalledApplications** – List of installed applications on a computer and their version number.

{

"collector": "CAS Server.InstalledApplications",

"type": 8,

"value": "{\"Value\":[{\"Name\":\"Microsoft .NET Framework 4.5.1 Multi-Targeting Pack\",\"Version\":\"4.5.50932\"},{\"Name\":\"Microsoft .NET Framework 4.5.2 Multi-Targeting Pack (ENU)\",\"Version\":\"4.5.51209\"},{\"Name\":\"Microsoft Visual Studio 2015 Shell (Isolated) Resources\",\"Version\":\"14.0.23107\"},{\"Name\":\"Microsoft Visual Studio 2015 XAML Designer - ENU\",\"Version\":\"14.0.23107\"},{\"Name\":\"SQL Server 2016 Database Engine Shared\",\"Version\":\"13.0.1601.5\"}}]}",

"timestamp": "2016-10-04T23:55:31.7103832-06:00"

}

1. **Services** – List of running services on a computer.

{

"collector": "CAS Server.Services",

"type": 9,

"value": "{\"Value\":[\"Application Host Helper Service\",\"Background Intelligent Transfer Service\",\"Background Tasks Infrastructure Service\",\"Base Filtering Engine\",\"COM+ Event System\",\"COM+ System Application\",\"COMMONService\",\"Credential Manager\",\"Cryptographic Services\",\"DCOM Server Process Launcher\",\"Device Setup Manager\",\"DHCP Client\",\"DHCP Server\"

"timestamp": "2016-10-04T23:55:33.6321646-06:00"

}

1. **SystemErrors** – System errors from a computer generated by the Microsoft Windows Event Log.

{

"collector": "CAS Server.SystemErrors",

"type": 11,

"value": "{\"Value\":{\"Message\":\"DCOM was unable to communicate with the computer 192.168.0.3 using any of the configured protocols; requested by PID d78 (C:\\\\COMMON\\\\Service\\\\COMMON.exe).\",\"TimeGenerated\":\"2016-10-04T23:55:20.6504830-06:00\"}}",

"timestamp": "2016-10-04T23:55:33.7727802-06:00"

}

1. **ApplicationErrors** - Application errors from a computer that were generated by the Microsoft Windows Event Log.

{

"collector": "CAS Server.SystemErrors",

"type": 11,

"value": "{\"Value\":{\"Message\":\"DCOM was unable to communicate with the computer 192.168.0.3 using any of the configured protocols; requested by PID d78 (C:\\\\COMMON\\\\Service\\\\COMMON.exe).\",\"TimeGenerated\":\"2016-10-04T23:55:20.6504830-06:00\"}}",

"timestamp": "2016-10-04T23:55:33.7727802-06:00"

}

1. **DatabaseSize** – Size of database(s) on a given computer in MegaBytes. Database systems may have multiple database and be Microsoft SQL Server, Oracle, or PostgreSQL.

{

"collector": "CAS Server.DatabaseSize",

"type": 13,

"value": "{\"Value\":[{\"Name\":\"SLDCommDB\",\"Size\":\"592\"},{\"Name\":\"tempdb\",\"Size\":\"16\"},{\"Name\":\"model\",\"Size\":\"16\"},{\"Name\":\"msdb\",\"Size\":\"15\"},{\"Name\":\"master\",\"Size\":\"6\"}]}",

"timestamp": "2016-10-04T23:55:36.560083-06:00"

}

1. **UPS –** Amount of runtime remaining on an uninterruptable power supply (UPS) for a UPS being monitored and controlled by a Windows. UPS devices using third party software, such as APC Powerchute cannot be monitored by COMMON.

{

"collector": "CAS Server.UPS",

"type": 14,

"value": "{\"Value\":{\"BatteryStatus\":\"The system has access to AC so no battery is being discharged. However, the battery is not necessarily Charging.\",\"EstimatedChargeRemaining\":\"100\",\"EstimatedRunTime\":\"350\",\"Name\":\"Smart-UPS 1000 FW:UPS 09.3 / ID=18\",\"Status\":\"OK\"}}",

"timestamp": "2016-12-06T21:39:07.4452026-05:00"

}

1. **DiskSpeed** – Number of read/write requests that had to be queued to a logical volume. Values should be between 0-2. Values larger than 2 indicate difficulty reading/writing to the disk indicating the possibility of disk problems such as bad sectors which requires the hard disk controller to find alternate sectors to store data increasing the read/write queue length of a particular disk.

{

"collector": "CAS Server.DiskSpeed",

"type": 15,

"value": "{\"Value\":{\"Disk Time %\":\"0\",\"Avg Disk Q Length\":\"0\",\"Disk Name\":\"C:\"}}",

"timestamp": "2016-10-04T23:55:36.8434508-06:00"

}

## Type Field

The type field is use to categorize data collector types and how they are stored and referenced in the COMMON database. Each type of collector has a unique Type ID to reference the category of data being collected.

|  |  |
| --- | --- |
| **Collector Type** | **Type ID** |
| Memory | 0 |
| Disk | 1 |
| CPUUsage | 2 |
| NICUsage | 3 |
| Uptime | 4 |
| LastBootTime | 5 |
| Processes | 6 |
| Ping | 7 |
| InstalledApplications | 8 |
| Services | 9 |
| DatabaseSize (not used) | 10 |
| SystemErrors | 11 |
| ApplicationErrors | 12 |
| DatabaseSize | 13 |
| UPS | 14 |
| DiskSpeed | 15 |

Table - COMMON Collector Type IDs