

DOCUMENTATION

BDNA Extractor Instructions

Instructions to Configure Tanium 7 Extractor

April 27, 2017

LEGAL NOTICES

Use of the BDNA software and products are subject to the terms and conditions of a license agreement found in either a separately executed master license agreement or the click-through master license agreement that is accepted prior to delivery of the BDNA software and/or products.

Copyright © 2001-2017. BDNA Corporation

Information in this manual and all BDNA technical support policies are subject to change without notice. Check with your BDNA authorized representative to ensure that you have the most recent information.

BDNA®, the BDNA logo, Technopedia®, BDNA Discover™, BDNA Normalize®, and BDNA Analyze™ are trademarks or registered trademarks of BDNA Corporation in the United States and internationally.

The products described herein may be technically combined with third party products or other products not supplied by BDNA, including third party or customer software, hardware, and materials. Any combinations or potential combinations described herein are advisory only. BDNA expressly disclaims any liability, and any expressed or implied representation and warranty, resulting from any combinations of the BDNA products with any products not supplied by BDNA.

This document is provided “as is” and without warranty of any kind. BDNA and its licensors (hereinafter collectively referred to as “BDNA”) expressly disclaim all warranties, expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose and against infringement.

Oracle is a trademark or registered trademark of Oracle Corporation in the United States and in other countries. Red Hat Enterprise Linux (RHEL) is a trademark or registered trademark of Red Hat Incorporated in the United States and in other countries. Microsoft Internet Explorer is a trademark or registered trademark of Microsoft Corporation in the United States or in other countries. All other trademarks appearing herein are the property of their respective owners.

Confidential and Proprietary to BDNA.

BDNA Corporation
339 North Bernardo Avenue, Suite 206
Mountain View, CA 94043
USA
Phone +1 650 625 9530
Fax +1 650 625 9533
<http://www.bdna.com>
02500010101

Contents

- Overview 1
- Instructions to configure Tanium 7 Extractor:..... 1
 - Creating BDNA Saved questions in Tanium Console..... 1
 - Saved Questions List 1
 - Saved Question Creation Procedure 3
- Create JSON File connectors for BDNA Saved Questions..... 6
 - Connector Settings 6
 - File Connectors Creation Procedure 11
- Generate the Normalize input zip file 14
 - Using the BDNA Standalone Extractor 14

Overview

The document details the steps needed to configure extraction from Tanium 7 server with Tanium Connect 4.

Instructions to configure Tanium 7 Extractor:

This is a three-step process:

1. Create BDNA Saved Questions in Tanium Console
2. Create JSON File connectors for BDNA Saved Questions
3. Generate Normalize input zip file

Create BDNA Saved questions in Tanium Console

Create the following Saved Questions using the Tanium Console. This step is required to be performed once at the time of initial setup.

Saved Questions List

Saved Question Name	Saved Question Text	Sensors Used
BDNA_System	GET Computer ID and AD Domain and Username and Computer Name and Domain Name FROM all machines	Computer ID, AD Domain, Username, Computer Name, Domain Name
BDNA_AddRemove	Get Computer ID and Installed Applications from all machines	Computer ID, Installed Applications
BDNA_Bios	GET Computer ID and BIOS Vendor and Computer Serial Number FROM all machines	Computer ID, BIOS Vendor, Computer Serial Number
BDNA_CDROM	GET Computer ID and CD-ROM Drive FROM all machines	Computer ID, CD-ROM Drive
BDNA_ComputerSystem	GET Computer ID and Manufacturer and Model and Number of Processors and x64/x86? FROM all machines	Computer ID, Manufacturer, Model, Number of Processors, x64/x86
BDNA_DesktopMonitor	GET Computer ID and Monitor Details FROM all machines	Computer ID, Monitor Details
BDNA_Disk	GET Computer ID and Disk Drive Details and Disk Type of C: FROM all machines	Computer ID, Disk Drive Details, Disk Type of C:
BDNA_NetworkAdapter	GET Computer ID and Network Adapter Details FROM all machines	Computer ID, Network Adapter Details

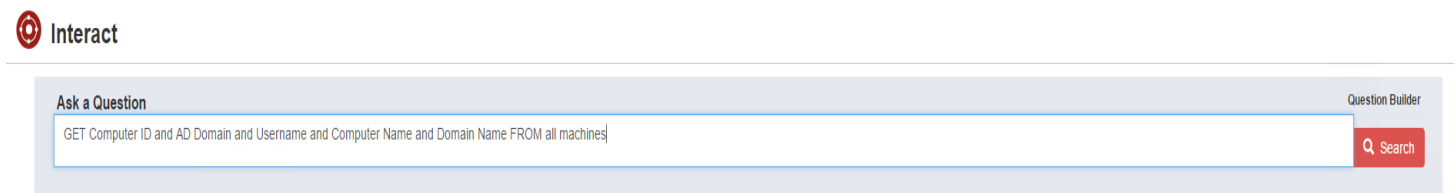
Saved Question Name	Saved Question Text	Sensors Used
BDNA_NetworkAdapterConfigur	GET Computer ID and Network IP Gateway and DHCP Enabled? and DHCP Server and IP Address and Subnet Mask and MAC Address FROM all machines	Computer ID, Network IP Gateway, DHCP Enabled?, DHCP Server, IP Address, Subnet Mask, MAC Address
BDNA_OperatingSystem	GET Computer ID and Boot Device and Operating System Install Date and Operating System and Operating System Language and System Directory and Operating System Boot Directory and Operating System Build Number and Country Code and Service Pack FROM all machines	Computer ID, Boot Device, Operating System Install Date, Operating System, Operating System Language, System Directory, Operating System Boot Directory, Operating System Build Number, Country Code, Service Pack
BDNA_PCMemory	GET Computer ID and Total Memory FROM all machines	Computer ID, Total Memory
BDNA_Processor	GET Computer ID and CPU Family and CPU Manufacturer and CPU Speed Mhz and CPU FROM all machines	Computer ID, CPU Family, CPU Manufacturer, CPU Speed Mhz, CPU
BDNA_RecentlyUsedApps_Host	GET Computer ID and Last Application Launch Date FROM all machines	Computer ID, Last Application Launch Date
BDNA_VideoController	GET Computer ID and Video Graphics Card RAM and Video/Graphics Card and Video Driver Version FROM all machines	Computer ID, Video Graphics Card RAM, Video/Graphics Card, Video Driver Version
BDNA_Passthrough	GET Computer ID and IP Routes and BIOS Release Date and Monitor Resolution and Number of Processor Cores and RAM and RAM Max Capacity and Total Swap and Sound Card and Virtual Platform and Disk Type of C: and DNS Server and Primary WINS Server and Network Adapter Type and System UUID FROM all machines	Computer ID, IP Routes, BIOS Release Date, Monitor Resolution, Number of Processor Cores, RAM, RAM Max Capacity, Total Swap, Sound Card, Virtual Platform, Disk Type of C:, DNS Server, Primary WINS Server, Network Adapter Type, System UUID

Saved Question Creation Procedure

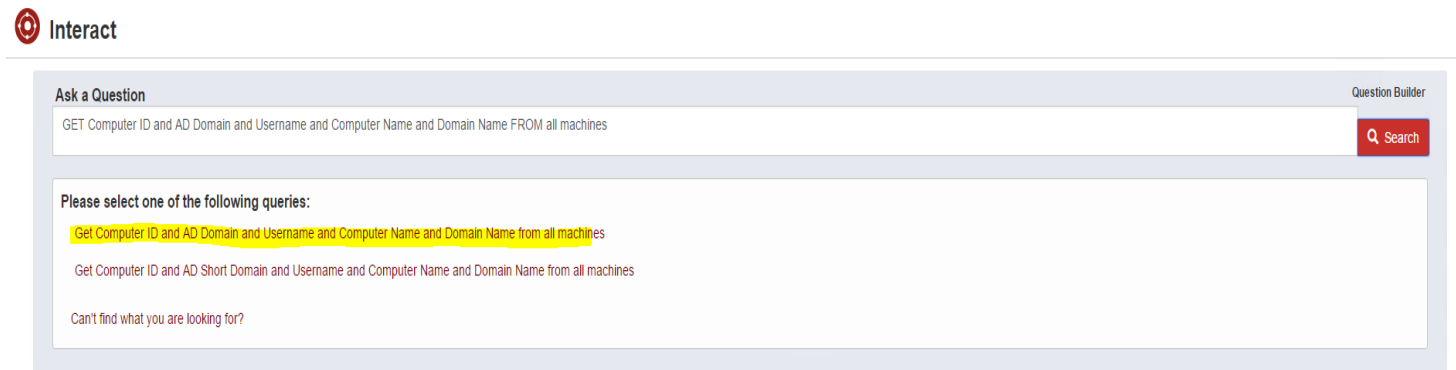
Step 1) Navigate to Interact tab of Tanium Console



Step 2) Refer to above table and copy “Saved Question Text” and Paste it into “Ask a Question” window.



Step 3) Click on “Search” button and it will show some suggestions. Pick the first one or the one which matches exactly with the “Saved Question Text”. Sequence and count of sensors should also remain same in “Saved Question Text” pasted in “Ask a Question” window and suggested query chosen.



Step 4) Based on **Step 3**, click on the most appropriate suggestion. It will run the Saved Question and show the output. Click on **“Save this question”** hyperlink at the bottom of **“Question”** window

The screenshot shows the Tanium Interact interface. At the top, there is a search bar with the text "Get Computer ID and AD Domain and Username and Computer Name and Domain Name from all machines". Below the search bar, there is a "Save this question" button. The main area displays a table with 4 items. The table has the following columns: Computer ID, AD Domain, Username, Computer Name, and Domain Name.

Computer ID	AD Domain	Username	Computer Name	Domain Name
2562718036	N/A on Linux	No User	vm350rh.(none)	(none)
3265254765	WORKGROUP	No User	vm098w	WORKGROUP
3788427316	WORKGROUP	No User	vm254w	WORKGROUP
986227570	WORKGROUP	No User	vm351w	WORKGROUP

Step 5) Refer to the above table and copy **“Saved Question Name”** for corresponding **“Saved Question Text”**. Paste it in **“Name”** window.

Step 6) Verify that Question Text matches with the **“Saved Question Text”** from above table. **Sequence and count of sensors should remain same in “Saved Question Text” in table above and “Question Text” below “Name” window**

The screenshot shows the "New Saved Question" window in the Tanium Interact interface. The "Name" field contains the text "BDNA_System". The "Question Text" field contains the text "Get Computer ID and AD Domain and Username and Computer Name and Domain Name from all machines".

Step 7) Click on “Preview” to see some data and then click on “Create Saved Question”

Question: Get Computer ID and AD Domain and Username and Computer Name and Domain Name from all machines

Items: 5 (5 total)

Computer ID ↑	AD Domain	Username	Computer Name	Domain Name
2562718036	N/A on Linux	No User	vm350rh.(none)	(none)
3021387401	Not joined to domain	root _mbsetupuser	tt643.	No Domain
3265254765	WORKGROUP	No User	vm098w	WORKGROUP
3788427316	WORKGROUP	No User	vm254w	WORKGROUP
966227570	WORKGROUP	No User	vm351w	WORKGROUP

[Create Saved Question](#) [Cancel](#)

Step 8) Repeat Steps 1-7 for all “Saved Questions” mentioned in table above.

Step 9) Once all “Saved Questions” have been created, click on “Saved Questions” under Authoring tab (from left side panel). Search for “BDNA” under Saved Questions. This should display all Saved Questions created. Total count of BDNA Saved Questions should be 15.

Authoring | Sensors | Packages | **Saved Questions**

Items: 1 of 110

Name ↑	Owner	Public	Reissue	Tags	Last Modification	Modified By
<input checked="" type="checkbox"/> BDNA_AddRemove	administrator	Yes	Never		11/4/2016, 9:07:10 PM	administrator
<input type="checkbox"/> BDNA_Bios	administrator	Yes	Never		11/4/2016, 9:07:10 PM	administrator
<input type="checkbox"/> BDNA_CDROM	administrator	Yes	Never		11/4/2016, 9:07:10 PM	administrator
<input type="checkbox"/> BDNA_ComputerSystem	administrator	Yes	Never		11/4/2016, 9:07:10 PM	administrator
<input type="checkbox"/> BDNA_DesktopMonitor	administrator	No	Never		11/4/2016, 9:07:10 PM	administrator
<input type="checkbox"/> BDNA_Disk	administrator	Yes	Never		11/4/2016, 9:07:10 PM	administrator
<input type="checkbox"/> BDNA_NetworkAdapter	administrator	No	Never		11/4/2016, 9:07:10 PM	administrator
<input type="checkbox"/> BDNA_NetworkAdapterConfigur	administrator	Yes	Never		11/4/2016, 9:07:10 PM	administrator
<input type="checkbox"/> BDNA_OperatingSystem	administrator	Yes	Never		11/4/2016, 9:07:10 PM	administrator
<input type="checkbox"/> BDNA_Passthrough	administrator	Yes	Never		11/4/2016, 9:07:10 PM	administrator
<input type="checkbox"/> BDNA_PCMemory	administrator	Yes	Never		11/4/2016, 9:07:10 PM	administrator
<input type="checkbox"/> BDNA_Processor	administrator	Yes	Never		11/4/2016, 9:07:10 PM	administrator
<input type="checkbox"/> BDNA_RecentlyUsedApps_Host	administrator	Yes	Never		11/4/2016, 9:07:10 PM	administrator
<input type="checkbox"/> BDNA_System	administrator	Yes	Never		11/4/2016, 9:07:10 PM	administrator
<input type="checkbox"/> BDNA_VideoController	administrator	Yes	Never		11/4/2016, 9:07:10 PM	administrator

Selected Saved Question

Question Name: **BDNA_AddRemove**

Question Text: Get Computer ID and Installed App Name from all machines

Visibility: Restrict this question to only owner and administrators

Saved Question Text

```
GET
Computer ID
and
Installed App Name
FROM all machines
```


Create JSON File connectors for BDNA Saved Questions

Create the following file connectors using the Connect plugin from the Tanium Console. This step is required to be performed once at the time of initial setup.

Below tables cover settings for Tanium Connect 4.x.

Connector Settings

General Information:
Name: Add Remove JSON File Connector Description: JSON File Connector for BDNA_AddRemove
Source and Destination:
Source: Saved Question Saved Question Name: BDNA_AddRemove
Destination: File Destination Name: AddRemove.json File Name: AddRemove.json
Format:
JSON

General Information:
Name: System JSON File Connector Description: JSON File Connector for BDNA_System
Source and Destination:
Source: Saved Question Saved Question Name: BDNA_System
Destination: File Destination Name: System.json File Name: System.json
Format:
JSON

General Information:
Name: Computer System JSON File Connector Description: JSON File Connector for BDNA_Computer System
Source and Destination:
Source: Saved Question Saved Question Name: BDNA_ComputerSystem
Destination: File Destination Name: Computer System.json File Name: ComputerSystem.json
Format:
JSON

General Information:
Name: LogicalDisk JSON File Connector Description: JSON File Connector for BDNA_Disk
Source and Destination:
Source: Saved Question Saved Question Name: BDNA_Disk
Destination: File Destination Name: LogicalDisk.json File Name: LogicalDisk.json
Format:
JSON

General Information:
Name: PCMemory JSON File Connector Description: JSON File Connector for BDNA_PCMemory
Source and Destination:
Source: Saved Question Saved Question Name: BDNA_PCMemory
Destination: File Destination Name: PCMemory.json File Name: PCMemory.json
Format:
JSON

General Information:
Name: Network Adapter JSON File Connector Description: JSON File Connector for BDNA_Network Adapter
Source and Destination:
Source: Saved Question Saved Question Name: BDNA_NetworkAdapter
Destination: File Destination Name: NetworkAdapter.json File Name: NetworkAdapter.json
Format:
JSON

General Information:
Name: Network Adapter Configure JSON File Connector Description: JSON File Connector for BDNA_Network AdapterConfigure
Source and Destination:
Source: Saved Question Saved Question Name: BDNA_NetworkAdapterConfigure
Destination: File Destination Name: NetworkAdapterConfigure.json File Name: NetworkAdapterConfigure.json
Format:
JSON

General Information:
Name: Operating System JSON File Connector Description: JSON File Connector for BDNA_Operating System
Source and Destination:
Source: Saved Question Saved Question Name: BDNA_OperatingSystem
Destination: File Destination Name: OperatingSystem.json File Name: OperatingSystem.json
Format:
JSON

General Information:
Name: Processor JSON File Connector Description: JSON File Connector for BDNA_Processor
Source and Destination:
Source: Saved Question Saved Question Name: BDNA_Processor
Destination: File Destination Name: Processor.json File Name: Processor.json
Format:
JSON

General Information:
Name: BIOS JSON File Connector Description: JSON File Connector for BDNA_Bios
Source and Destination:
Source: Saved Question Saved Question Name: BDNA_Bios
Destination: File Destination Name: BIOS.json File Name: BIOS.json
Format:
JSON

General Information:
Name: CD ROM JSON File Connector Description: JSON File Connector for BDNA_CDROM
Source and Destination:
Source: Saved Question Saved Question Name: BDNA_CDROM
Destination: File Destination Name: CDROM.json File Name: CDROM.json
Format:
JSON

General Information:
Name: Desktop Monitor JSON File Connector Description: JSON File Connector for BDNA_Desktop Monitor
Source and Destination:
Source: Saved Question Saved Question Name: BDNA_DesktopMonitor
Destination: File Destination Name: DesktopMonitor.json File Name: DesktopMonitor.json
Format:
JSON

General Information:
Name: Recently Used Apps Host JSON File Connector Description: JSON File Connector for Recently Used Apps Host
Source and Destination:
Source: Saved Question Saved Question Name: BDNA_ RecentlyUsedApps_Host
Destination: File Destination Name: RecentlyUsedAppsHost.json File Name: RecentlyUsedAppsHost.json
Format:
JSON

General Information:
Name: Video Controller JSON File Connector Description: JSON File Connector For Video Controller
Source and Destination:
Source: Saved Question Saved Question Name: BDNA_VideoController
Destination: File Destination Name: VideoController.json File Name: VideoController.json
Format:
JSON

General Information:
Name: Pass Through JSON File Connector Description: JSON File Connector For Pass Through
Source and Destination:
Source: Saved Question Saved Question Name: BDNA_PassThrough
Destination: File Destination Name: PassThrough.json File Name: PassThrough.json
Format:
JSON

File Connectors Creation Procedure

Instructions to create Connectors for **Tanium Connect 4.x:**

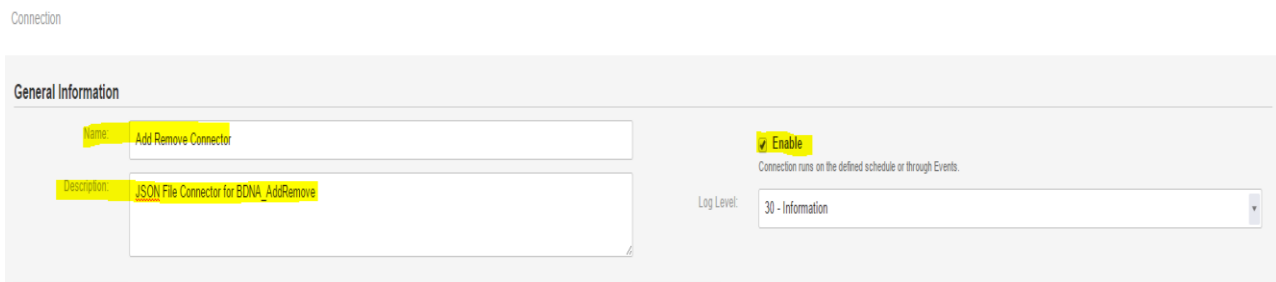
Setting 1)

These settings need to be repeated for each Saved Question. Please refer to appropriate table above to get settings for corresponding saved question. For example, screenshots below show settings done for BDNA_AddRemove saved question.

Connection:

General Information:

- Select “**Enable**” checkbox
- Enter Connector Name and Description as shown in snapshot below



Setting 2)

Source and Destination:

- Select Source as **“Saved Question”**. Advanced Settings will show up.
- Select Saved Question Name from drop down menu. **Connector Name and the corresponding Saved Question and File Name are shown in table above. Please refer to that table while creating connections.**
- Select Computer Group as **“All Computers”**
- Under Advanced Settings, select **“Flatten”**, **“Hide Errors”** and **“Recent”** checkbox.
- Select Answer Complete Percent as **“100”**
- All other values should be same as default ones.
- Select Destination as **“File”**
- Enter Destination Name by referring to [table](#) above. It is not a drop-down menu. User has to type a file name in that box.
- **Enter File Name where saved question data needs to be dumped. File Names should be same as shown in table above. Please refer to that table while creating connections. File Names should not have any spaces.**
- **All files are created in the \Tanium Module Server\services\connect-files\output folder.**
- Under Advanced Settings, keep Filename Timestamp Format as empty i.e. “ ”
- Select **“Replace File”** checkbox.

Source and Destination

Source: Where is the data coming from?

TANIMUM

Saved Question: **Saved Question**

Saved Question Name: **BDNA_SYSTEM**

Computer Group: **All Computers**

Advanced Settings

Use Cached Data
Do not ask endpoints the Saved Question. Pull Saved Question results from the cache on the Tanium Server.

Flatten
When enabled, results that contain multiple values per row for a column are broken out into individual rows.

Hide Errors
Answers with errors are not sent to the connection destination.

Recent
Include answers from machines that are not currently turned on.

Answer Complete Percent: **100**
Percentage of machines that must answer the Saved Question before processing of answers occurs.

Timeout: **10**
Minutes to wait for clients to reply before returning processed results.

Batch Size: **1000**
Rows returned from the server at a time.

Destination: Where is the data going?

TANIMUM

File: **File**

Destination Name: **System.json**
Enter the name of a new destination or choose an existing destination.

File Name: **System.json**
All files are created in the \Tanium Module Server\services\connect-files\output folder. You can create or link sub-folders and use a relative path in the file name.

Advanced Settings

File Name Time Stamp Format: **File Name Time Stamp Format**
Select or enter a date and time format to append to the file name.

Replace File
When selected, the file is replaced each time the connection runs. When not selected, the results are added to the existing file.

Compress File
Compress resulting file.

Allow No Results
Create file with no results.

Format:

- Select Format as “**JSON**”
- Select **Enriched JSON** checkbox
- Select row delimiter as “**\r\n**”
- Uncheck “**Wrap Data with Source**” option

Schedule:

- Select Schedule of running Saved Question by consulting Tanium TAM. This value needs to be set in such a way that maximum assets get discovered during the run. Tanium Trends could be referred before setting this value.

Finally, click on “**Create Connector**” to create connection for a Saved Question.

To test JSON file Connector, open that connector and click on “**Run Now**”

The screenshot displays the configuration interface for the Tanium 7 Extractor. It is divided into two main sections: **Format** and **Schedule**.

Format Section:

- A dropdown menu is set to **JSON**.
- The **Wrap Data with Source** checkbox is unchecked. Below it, the text reads: "Generates data where the source name surrounds data."
- The **Enriched Json** checkbox is checked. Below it, the text reads: "Generates rich JSON output."
- The **Row Delimiter** is set to **\r\n**. Below it, the text reads: "Character to use to separate lines."
- A **Columns** section is visible with the text: "Select and name columns to send."

Schedule Section:

- The **Schedule** section is titled "Schedule View schedule chart".
- The **Summary** is "At 04:47 PM (Schedule currently enabled.)".
- There are two buttons: **Generate Cron** and **Edit Cron Expression**.
- The **Schedule Type** is set to "One run per day, every day". Below it, the text reads: "Choose between one or multiple runs per day on selected days of the week or month."
- The **Time** is set to 04:47 PM.

Generate the Normalize input zip file

After the connectors are created, JSON files for all BDNA Saved Questions will be saved at the location chosen in above step. You can now use the BDNA Standalone Extractor to extract Tanium data from these JSON files.

Using the BDNA Standalone Extractor

From a workstation with file access to the JSON file location, run the BDNA Normalize Standalone Extractor.

NOTE: Standalone Extractor Version 5.3 or higher is required.

1. Click the Browse button in the Configuration File section to and select the json.Tanium.config file.
2. Click the Browse button in the Input JSON File section and select the folder where Tanium JSON files are located.
3. Click on Test button to test connectivity.
4. Click Browse button in the Output Path section to select the path to save the Normalize input zip file.
5. Click on Execute button to start the extraction.
6. After extraction completes, the saved Normalize input zip file can be loaded into BDNA Normalize by creating a new Normalize Process from the BDNA Data Platform Admin Console

Create Process

Process Type > IT Discovery Tool

Select IT Discovery Tool

Select a discovery tool you want to normalize.

<input type="radio"/> BDNA Discover	<input type="radio"/> LANDesk
<input type="radio"/> BMC ADDM	<input type="radio"/> Lansweeper
<input type="radio"/> BMC BladeLogic Client Automation	<input type="radio"/> ManageSoft Enterprise Compliance Manager (ECM)
<input type="radio"/> BMC BladeLogic Server Automation	<input type="radio"/> Microsoft Assessment and Planning Toolkit (MAP) 7
<input type="radio"/> CA IT Client Manager (ITCM)	<input type="radio"/> Microsoft Assessment and Planning Toolkit (MAP) 8
<input type="radio"/> CiscoWorks LAN Management Solution (LMS)	<input type="radio"/> Microsoft SMS 2003
<input type="radio"/> Dell KACE	<input type="radio"/> Microsoft System Center Configuration Manager 2007
<input type="radio"/> HP Client Automation	<input type="radio"/> Microsoft System Center Configuration Manager 2012
<input type="radio"/> HP DDMI	<input type="radio"/> Novell ZENworks
<input type="radio"/> HP DDMa	<input type="radio"/> OCS
<input type="radio"/> HP Server Automation	<input type="radio"/> SolarWinds Orion
<input type="radio"/> HP Universal Discovery	<input type="radio"/> Scalable
<input type="radio"/> HP Universal Discovery (XSF)	<input type="radio"/> VMware vCenter Protect
<input type="radio"/> IBM License Metric Tool	<input type="radio"/> ServiceNow Discovery
<input type="radio"/> IBM TCM	<input type="radio"/> Other: Database Connection
<input type="radio"/> IBM Tivoli Application Dependency Discovery Manager	<input checked="" type="radio"/> Other: Normalize Zip File

Prev Next