CRUZ TRAINING GUIDE
DAY 1-3

This guide outlines days 1-3 of the standard training for Cruz Operations Center.

AGENDA

DAY ONE

Introducing Cruz

- Pre-Installation/Startup
- Create Trainee Workstation Users
- Discovery
- Using
- Resource Monitors

DAY TWO

- File Management
- Alarms
- Network View
- Containers

DAY THREE

- Reports
- Actions/Adaptive CLI
- ProScan/Change Management
- Troubleshooting

EXERCISES

- Make Unique Users for Trainee Workstations
- Discover Your Network's Devices
- Create a Private Page
- Error! Reference source not found.
- Examine Device Details
- Create an ICMP Monitor
- Create a Dashboard
- Set up Flow Emulation
- Backup Configurations
- Restore Configurations
- Edit then Compare a Configuration
- Create Multiple Event History Portlet's
- Find Events Relevant to Your Use Case
- Create a Post-Processing Rule
- Create a Pre-Processing Rule
- Navigating Through a View
- Create and View Containers
- Create a New Report
- Actions: Perl Script Exercise
- Create Action using Embedded Script: Extracting a DateString
- Create and Run ProScan

DAY ONE – EARLY

Cruz Training Overview

Cruz training will introduce you to the product and includes a series of on hands exercises to familiarize you with how to use your new tool. After completing the following training sessions, Cruz features and troubleshooting should be clearer to you. Please refer to the first page of this document for the outline of the training.

Course Objectives

After completing this course, you will be able to do the following:

- Install Cruz on a single server
- Discover your Network's Device
- Understand the User Interface
- Monitor your Network's Performance
- Understand Traffic Flow Analyzer
- Manage (backup/restore) Configuration Files
- View Alarms/Events, and Automate actions
- Customizing Topology View
- Understanding Containers
- Create and configure Reports
- Create and configure Network Visualizations
- Use Adaptive CLI Actions & Change Management/Proscan
- Avenues to explore troubleshooting solutions
- Understand features of Multitenancy, Site Management, and Access Profiles
- Understanding Cruz; its features and use cases

CruzOC Automation Use Cases

Before beginning training, below are examples of the helpful things CruzOC can automate. Here are some typical use cases:

Alert when a device goes offline — You can configure responses to any alarm or event in Event Processing Rules (EPRs, see *Event Processing Rules*).

One key to automating responses is find the appropriate alarm or event by searching the Event Definitions portlet. See *Find Events Relevant to Your Use Case* .

Events that indicate a device has gone offline include the linkDown alarms, or the (configured) ICMP availability monitor threshold crossings (see *Resource Monitors*).

NOTE: You should configure thresholds even in the default ICMP monitor. They are not configured by default.

You can use advanced filters to search for monitor event names that contain redcell (a name common in Cruz's internal events) and ThresholdNotification.

Emit an Alert when latency is too high say for a period (Example: latency exceeds 200ms for 2+ minutes).

Because you can configure monitor thresholds you can also configure events triggered with those thresholds (see *Resource Monitors*). Configure the threshold to suit your requirements. For this example, one might configure the monitoring interval to one minute, and require two ICMP MaxRTT events of greater than 200ms to emit the ThresholdNotification event.

Emit an alert When CPU utilization, memory use, or temperature exceeds a threshold — SNMP notifications for CPU and memory utilization, as well as temperature thresholds are typically device-specific events. Force10 emits chAlarmExdCpuThreshold, for one example (from F10-CHASSIS-MIB). You can find such events in the Event Definitions by searching for CPU, memory or temperature. Monitoring such events with an SNMP monitor, and setting a threshold to emit an event is as described in *Resource Monitors* and the following pages.

The device's documents should clarify the exact meaning of such events, but you can also right-click an event when you have found it, and Edit to read the MIB text.

For example, the Force10 chAlarmExdCpuThreshold says “The agent generate [sic] this trap when cpu utilization exceeded [sic] 80%.” The spelling may not be the best, but you get the message.

Invalid login attempts — Searching for *login* in Event Definitions displays the available events for which one can automate responses. These include some device-specific events as well as generic (Redcell-Inventory MIB) events. These are available for EPRs to configure automated responses, or to monitor with thresholds.

Command Line Alternatives — If a command line to a device produces better information than the SNMP events cataloged above, then you can create an Adaptive CLI, monitor it, create a threshold to emit an event, and automate the response to the event. See *Actions/Adaptive CLI* for the training exercises about those.

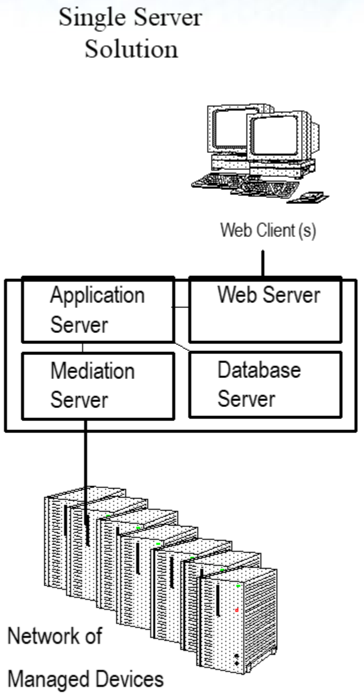
DOCUMENTS

The following documents are available with CruzOC.

Training Guide — A course outline and reference.
Quickstart — A brief manual to get new users started.
User Guide — The most comprehensive reference. Also, the source of online help. Includes troubleshooting information.
Release Notes — Another reference for those troubleshooting Cruz.

APPLICATION ARCHITECTURE

The following displays the components in a typical single-server installation:



The mediation server process handles and standardizes transactions with devices, application server processes any rules or automation associated with those devices, and passes the display information to web server process while preserving any needed data to the database server process. Clients view the results on their browsers.

Pre-Installation/Startup

Cruz installs with a standard installation wizard. But before you initiate installation, make sure you have consulted the *Cruz User Guide*.
Note the following files in the directories under the installation:
linux_install.sh win_install.exe — The installers for Linux and Windows, respectively.
version.txt — This file tells you the versions of various components (important for troubleshooting). You can also get this information from within the application with the *Manage > Show Versions* menu item.
owareapps — This directory contains files that reflect the various components to be installed, particularly device drivers supporting various vendors (dellpc.ddp for the Dell PowerConnect devices, for example).
extensions — This directory contains files that reflect additional components (example: automated topology with Visualize).

Best Practices: Single Server Hardware

The following describes hardware and sizing configuration for common Cruz deployments in both real and virtual machines. Before any deployment, best practice is to review and understand the different deployment options and requirements. Consider future growth of the network when estimating hardware sizes. You can often expand modern systems running Cruz by adding more RAM to the host server(s). Selecting expandable hardware may also be critical to future growth.

Minimum Hardware

The minimum hardware specification describes the least of what Cruz needs. In such minimum installations, traffic flowing from the network to Cruz may exceed the capacity of the hardware. When estimating the size of a deployment, it is important to understand the applications configurations in the target environment. For example, the most resource-intensive, demanding applications are typically Traffic Flow Analyzer (TFA), Event Management and Performance Monitoring.

REQUIRED Minimum hardware — 8GB RAM[5], dual core CPU, 3.0GHz or better, 200 GB 7200 RPM Disk.

Supports:

- Standalone installations (Single Server) are supported when you use high-resource demand applications minimally.
- Distributed installation of a single component server like application server only, Mediation server only, database server only or web server only.

RECOMMENDED Minimum hardware — 10GB RAM, four-core (or more) CPU (3.0GHz or better), 400 GB 10,000 RPM Disk

Supports:

- Standalone installations

NOTE: The above assumes you have dedicated a host to Cruz alone. Other applications may compete for ports or other resources and can impair the system's performance.

Sizing for Standalone Installations

The following are suggested sizing guidelines for your Cruz system.[1]

64-bit Operating System: Disks/RAM/Hardware	Max. Concurrent Users	Max. Managed Devices[2]	Performance Monitor Max. Targets[3]	Max. Traffic Flow Exporters[3]	Installation Changes to Heap Memory Settings
8GB[5] RAM, single disk, consumer level PC	5	25	2500	5	Use defaults: (2GB application server heap, 512M database, 2G Synergy Web Server[4])
10 GB RAM, single disk, consumer level PC	8	50	5000	5	3-6 GB application server heap, 512M database buffer, 2G Synergy Web Server
12 GB RAM, single disk, consumer level PC	10	100	10000	10	4-7GB application server heap, 1GB database buffer, 3GB Synergy Web Server
14GB RAM, single disk, business level PC	15	175-250	25000	25	4-9 GB application server heap, 1GB database buffer, 3GB Synergy Web Server
16GB RAM, single disk, business level PC	25	300-500	50000	50	5-10GB application server heap, 2GB database buffer, 3GB Synergy Web Server
18 GB RAM, multi-disk, server level PC	50 (Medium-large network)	1000	100000	100	8-12GB application server heap, 3GB database buffer, 5GB Synergy Web Server
32GB RAM, multi-disk, server level PC. Recommend fast disk array or SSD drive array for the large number of database actions.	100 (Large network)	2000	200000	100	10-14GB application server heap, 8GB database buffer, 8GB Synergy Web Server

Footnotes:

[1] Servers are assumed to have at least four cores (3.0GHz or better) and are no more than four years old. As memory and usage increases, the

number of CPU cores needs to increase. Dual core CPUs can work for the most basic installations, but such configurations are not recommended.

[2] Each device mentioned here is equivalent to a L2 or L3 switch with a total of 48 interfaces per device being monitored. For each device, not being monitored for 48 interfaces, you can add another 50 devices to the overall inventory for ICMP-only monitoring. Maximum monitor targets estimates are based on a 5 minute or longer polling interval. It assumes each monitor is polling the default number of attributes or less.

[3] Application Constraints are most relevant to Traffic Flow Analysis, Performance Management, and Event Management. Refer to the performance monitor Section of the user guide to best practices. In general, no single monitor should exceed 10000 targets. This is primarily for performance reasons. Actual physical hardware and monitor configuration will determine your system capacity for targets and overall system performance.

The Maximum Exporters assumes your Traffic Flow configuration does not exceed the capacity of the physical hard drive(s). refer to the Performance section of the Traffic Flow chapter.

Traffic Flow Analysis ratings map to constant throughput divided by sample rate, as in bandwidth/sample rate. 20G/2000 is easier to manage than 20G/1000. 20G/1 is a thousand times more demanding than 20G/1000. Best practice is to avoid such high sample rates. The bandwidth the hardware your Cruz installation can support is dramatically lower in such cases. Best practice is to sample a maximum of one traffic flow for every 1000 (1:1000). Higher sampling rates degrade database performance and increase network traffic without adding any significant statistical information.

Performance Management can support 600 inserts per second using a single disk (SSD) Drive. 1 insert = 1 monitored attribute. Expect better performance as you add more drives (and worse performance with slower drives).

Event Management can support a sustained 1200 traps /sec using a single (SSD) drive. Expect better performance as you add more drives (and worse performance with slower drives).

NOTE: Java JVM problems can generate over 10GB of thread dump in case of a memory error. To solve the problem of such files filling up your hard drive, delete the *.hprof files in the /oware/jboss-5.1/bin directory to free up the disk space. You can also clean out temporary directories. Finally, ensure your hardware has enough RAM for the tasks it has been assigned. The Server Statistics portlet displays performance information.

[4] Concurrent users determine the amount of RAM required for the web server. You can reduce the web server heap setting can if your system has fewer concurrent users.

[5] Although not recommended, 6 GB of RAM may be enough for systems with up to two users that are not using Traffic Flow Analysis or

Performance Monitoring. In such cases, adjust installation/settings to 1 GB Synergy web server rather than the 2 GB default.

If the network you manage exceeds the parameters outlined above, or your system is balky and unresponsive because, for one example, it monitors more devices than your hardware can handle, consult your sales representative about upgrading to a more robust or multi-server version of Cruz.

Also, see *Best Practices: Performance and Monitors* of the *Cruz User Guide* for more about tuning monitor performance. You can also monitor the application server itself. See *Application Server Statistics* and *Self Management/Self Monitoring: Default Server Status Monitor* in the *Cruz User Guide*.

For database information, see *MySQL Resizing, Starting, and Stopping* in the *Cruz User Guide*.

Best Practices: Pre-Installation Checklist

The following helps you avoid trouble in your Cruz installation.

Pre-Installation

- Select devices (IP addresses, or range) and ports to manage. Gather their authentications (login/passwords). Typically, these include SNMP communities and command line authentications. Determine what version of SNMP you are using, too.
- Select IP address for your server. Cruz requires a static IP address. When necessary, configure devices' access control lists (ACLs) to admit this application's access/management.
- Verify firewalls have open ports between devices and your server. Best practice is to take down the firewall, install the application, then put it back up.
- Review your devices' manuals and release notes.
- You will also need access to an FTP/TFTP server.

Installation

Installation Host — Log in as an administrative user with write access to the installation target directory.

- Do *not* log in with user name *admin, administrator*, or a name that contains spaces on Windows, or as user *root* on Linux. The installer confirms you are not one of those users. If you attempt this or other prohibited practices, you may see a message like the following:
- The installer cannot run on your configuration:
- Please verify that you are not logged in using the windows "Administrator" account or with the linux "root" account.
- The installation supports 64 bit Windows and Linux architectures.

Windows Server 2008, 2012, 2016 — You must disable User Account Control if installing on Windows Server 2008.

- Temporarily disable the system firewall or any anti-virus software prior to installing, too.
- Install this software and the wizard will walk you through initial setup. Cruz installs as a service and starts automatically. Refer to the *Cruz User Guide* and release notes for additional setup information.
- When installing on Windows Server 2012, right click win_install.exe and select *Properties* > *Compatibility.* Select compatibility mode for Windows 7 /Vista.

Directories — The source directory should not be the same as installation target directory

Clocks — Clocks on all hosts where you install must be synchronized.

Starting Cruz (After installation)

Database Running, Connected — Make sure your database is running. MySQL installs automatically as a service (daemon), Oracle must be started separately. Make sure your database connects to the application server if it is on a separate host. Do not install on Linux with MySQL already installed (uninstall any included MySQL first).

Start Application Server — If you installed this software as a service and application server is down, in Windows right-click the *startappserver* icon, and start application server. Sometimes, this icon may prematurely indicate application server has started. Wait a little, and the application server will catch up to the icon.

When initiated from the tray icon, startup changes its color from red to yellow to green, when complete. Once the icon has turned green, the web client may display the message "The server is currently starting up. This page will refresh when the server has fully started." This message indicates the application server requires extra time to start. When the message does occur connect the web browser again after a few minutes.

Login — Default Cruz login is *admin*, password *admin*.

NOTE: The first time you start the application after you install it, you may have to wait some additional minutes for Application to completely start. One indication you have started viewing your web client too soon is that the Quick Navigation portlet does not appear correctly. *Workaround****: Force Cruz to re-initialize the admin user. To do that: Login as Admin. Go To > Control Panel > Users and Organizations. Select and edit the Admin user. Edit any field (Middle Name for example). Save. Sign out. Log back in with admin.***

For Successful Discovery (After startup) Have the Following:

Connectivity — Ensure application server has connectivity to devices to discover. One easy way to do this is to ping the discovery target from the application server host. Right-clicking a discovered device and selecting *Direct Access* also lets you ping.

Backup/Restore/Deploy (After device discovery)

FTP/TFTP Server — Make sure an external FTP/TFTP server is running and has network access to the target device(s). Typically, FTP/TFTP servers must be on the same side of firewalls as managed devices. Cruz's internal FTP/TFTP server is for testing only. If these are separate processes, configure them so they write to the same directory.

Alarms/Monitoring

Minimize Network Traffic — Configure "chatty" devices to quiet down. Use *Suppress Alarms* to keep performance at acceptable levels, and configure database archiving so the database does not fill up.

NOTE: Some Cruz features do not work without internet access. In particular, Maps, because the maps Cruz uses need internet access to retrieve maps and plot locations. If you do not need functioning map portlet(s), then running Cruz without internet access works as exepected.

Also, make sure you have the following:

- Know the size of network you are planning to manage, and hardware suited to its size. Consult Best or the Cruz User Guide for specific hardware recommendations.
- A supported/recommended browser (Chrome, Firefox, and in a pinch, Internet Explorer) at the recommended minimum resolution (1280 x 1024 pixels or better).
- The above is typically done before training occurs.

The following exercise points out steps of interest during the installation process.

Install Cruz

- Follow the suggestions in the Best Practices above, and make sure you have the hardware recommended for the network you plan to manage as specified above.
- Start the installation wizard (win_install.exe or linux_install.sh)
- The initial screen displays the Cruz version; you should note this in case you need to contact support regarding installation.

- Click *Next* in the installation wizard. The next screen displays the minimum hardware requirements.
- Click *Next* to receive license agreement.
- You must accept the license. Click *Next* to proceed.
- Network Interfaces Screen Appears. If your host has more than one network interface, you must select which one is going to be Cruz's.
- Click *Next* to proceed. An Install Folder Screen Appears.

As a default; Cruz is installed on: **C:\\ProgramFiles\Dell\OpenManage\Network Manager**. You may want to change the installation directory by clicking on the *Chose* Button and selecting desired directory path.

- Click *Next* to proceed. A Heap Settings Screen Appears.

Set the application server heap (memory) settings. Essentially, best practice is to set heap as large as possible without interfering with other applications, particularly the operating system.

- After choosing your heap settings. Click *Next* to proceed.
- Once you determine your settings; Click *Next* to proceed. A Pre-Installation Summary Dialogue Box appears.
- This summary screen previews the selections made before installation triggers its progress bar. Click *Install*.
- A progress screen of installation will show. When completed "Confirming Database". will appear.
- The final screen: Install Completed Successfully will appear.
- Click *Done.* By default, the application starts automatically.

Starting Cruz

Once the installation wizard is done, you are ready to start your application.

This consists of two-parts:

Application Server — This displays an icon in Windows' tray to indicate it is fully initialized.

Web Portal Server — Another icon in the Windows tray turns green when this startup is complete.

Directions: Open a browser to [application server IP or host name]:8080, and sign in. The default login/password is *admin/admin*. Note: use the IP address of the system where it is installed.

NOTE: You must also enter a password reminder like your father's middle name the first time you log in. To get e-mail reminders about forgotten passwords, you must configure the SMTP server as described in the* **Cruz User Guide.**

NOTE: To watch the server log in real time, as Cruz starts, open a command shell in [application root]/oware/jboss-x.x/server/oware/log. Set the environment (oware in Windows; . /etc/.dsienv in Linux) and type tail -f server.log.

Create Trainee Workstation Users

Although the default user/password combination (admin/admin) provides easy initial access to your Cruz system after you have installed and started it, an entire classroom full of user "admin" can make performance sluggish. That is why we do the next exercise.

When making users, remember the function of the application's Roles. Roles determine permissions available to users assigned them. Manage Roles in the *Portal > Roles* screen.

Notice also that Roles support two types of permissions: the web portal's open source capabilities and the features within Redcell. Click the *Actions* button to its right to change a Role's open source portal capabilities. To configure Cruz's functional permissions, over and above the portal's capabilities, use the editor in *Redcell> Permission Manager* on the Control Panel.

Click *Add* to create a *Regular Role, Site Role,* or *Organizational Role.* A *Regular Role* assigns its Redcell permissions to its members. A *Site* or *Organizational Role* assigns portal permissions to a site or organization to which you can assign users. Other than for *Regular Role*, however, only web portal permissions (not Redcell permissions) are available for *Site Roles* and *Organizational Roles*. Only *Regular Role*s restrict a user's Cruz abilities.

Make Unique Users for Trainee Workstations

Follow these steps to make unique users for each workstation:

- Click *Go to > Control Panel*
- Click *Portal > Users and Organizations*
- Click *Add > User* at the left top of the screen.
- Enter unique user identifiers in the fields on this screen (at least *Screen Name, Email Address* and *First Name*).
- Click *Save.*
- You must create a password for any new user. Once the screen says, "Your request completed successfully" click the *Password* link to the right of the screen, and enter a password.
- Notice that those creating new users can also enable *Password Reset Required* so those users can make their own password after they log in for the first time (when they'll be asked to create a password reminder too).
- After creating your password, click *Save.*

> ***NOTE: Cruz automatically adds new users to the roles User and Power User, so make sure the sum of permissions (logical AND) from those roles is what you want for new users in your installation.***

- Click *Portal > Roles*.
- Click the *Actions > Assign Members* button to the right of the *Administrator* role.
- Click the *Available* tab, and select your newly added user by checking the checkbox to its left.

- Click *Update Associations.* When successful, your user appears in the role’s *Current* tab too.
- Although we created no new role, notice that you can do that in the *Portal > Roles* panels.

The way to limit permissions for users is by creating a role and assigning it permissions in Control Panel’s *Redcell> Permission Manager*. You can also alter existing roles’ permissions in portal roles.

Then, just as you assigned your new user to the Administrator role, you can assign users to the new roles you created (remembering that Redcell automatically assigns new users to *User* and *Power User* roles whose permissions you can also alter).

> ***NOTE: When an upgrade adds new permissions to the application, they are turned off by default. To locate new permissions, edit the Administrator role, and click the*** **Add** ***button. All added permissions from the upgrade appear there.***

- *Sign out* of your Cruz web client by clicking the link in the upper right corner of your browser, and then log back in as the user you just created.

> ***NOTE: One benefit of users having their own login is that they can configure the portlets and pages that appear after selecting*** **Go to > My Private Pages***, and those changes stick, even if they are not administrators.***

Discovery

Discovery brings network devices under management by Cruz, and is typically the first thing done after installation.
When you discover devices create authentications in the *Authentication portlet* with the authentications you have gathered from your devices. Then create *Discovery Profiles* in that portlet. Discovery profiles refer to the authentications you have created.

To save training time, your installation may have already discovered the devices on your network. This eliminates the need to create *Authentications*
as described below (although you can right-click and select *New* or *Edit* to see how they look).

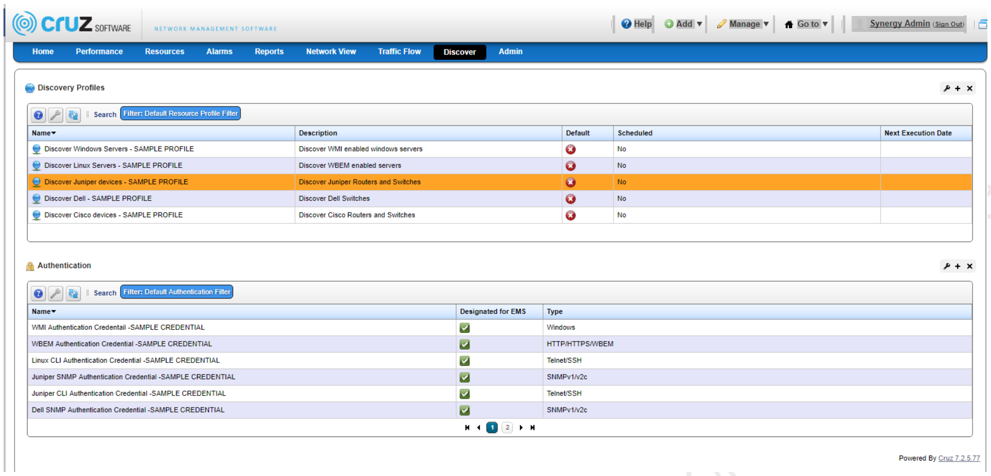
If you want to see Discovery in action, you cannot do so with devices Cruz has already discovered. You must delete a device that already appears in the *Managed Resources* portlet, then use its *Discovery Profile* to re-discover it.

You may have a lab and production environment for your Cruz system. Notice that you can right-click and export things like Authentications and Discovery Profiles (and many other items), so you can export once everything is validated in the lab, then import to production to use the validated items there.

Also: See *Preventing* for more about troubleshooting discovery.

Discover Your Network's Devices

- Go to the *Discover* page



Discovery Profiles

Search Filter: Default Resource Profile Filter

Name	Description	Default	Scheduled	Next Execution Date
Discover Windows Servers - SAMPLE PROFILE	Discover WMI enabled windows servers	⊗	No	
Discover Linux Servers - SAMPLE PROFILE	Discover WBEM enabled servers	⊗	No	
Discover Juniper devices - SAMPLE PROFILE	Discover Juniper Routers and Switches	⊗	No	
Discover Dell - SAMPLE PROFILE	Discover Dell Switches	⊗	No	
Discover Cisco devices - SAMPLE PROFILE	Discover Cisco Routers and Switches	⊗	No	

Authentication

Search Filter: Default Authentication Filter

Name	Designated for EMS	Type
WMI Authentication Credentail -SAMPLE CREDENTIAL	✓	Windows
WBEM Authentication Credential -SAMPLE CREDENTIAL	✓	HTTP/HTTPS/WBEM
Linux CLI Authentication Credential -SAMPLE CREDENTIAL	✓	Telnet/SSH
Juniper SNMP Authentication Credential -SAMPLE CREDENTIAL	✓	SNMPv1/v2c
Juniper CLI Authentication Credential -SAMPLE CREDENTIAL	✓	Telnet/SSH
Dell SNMP Authentication Credential -SAMPLE CREDENTIAL	✓	SNMPv1/v2c

Powered By Cruz 7.2.5.77

Authentications

Create a new authentication, configuring authentications needed for access to your devices using the below instructions.

- Right-click in the Authentication portlet, and select *New*
- In the General Authentication Parameters > Type in an ID.

> ***NOTE: The Authentication Type is typically a command line (Telnet/SSH) > Fill in appropriate login/password combination, or SNMP community string. Some devices also require an enable login/password. WMI login/passwords (managing Windows hosts) may require a Domain. Consult with your network administrator for what you need.***

Notice that you can configure time-outs/retries for the authentications you create. Configure these as necessary to account for your network's latency. You can revise these Timeout/retry settings by right-clicking a device in Managed Resources and selecting *Edit.*

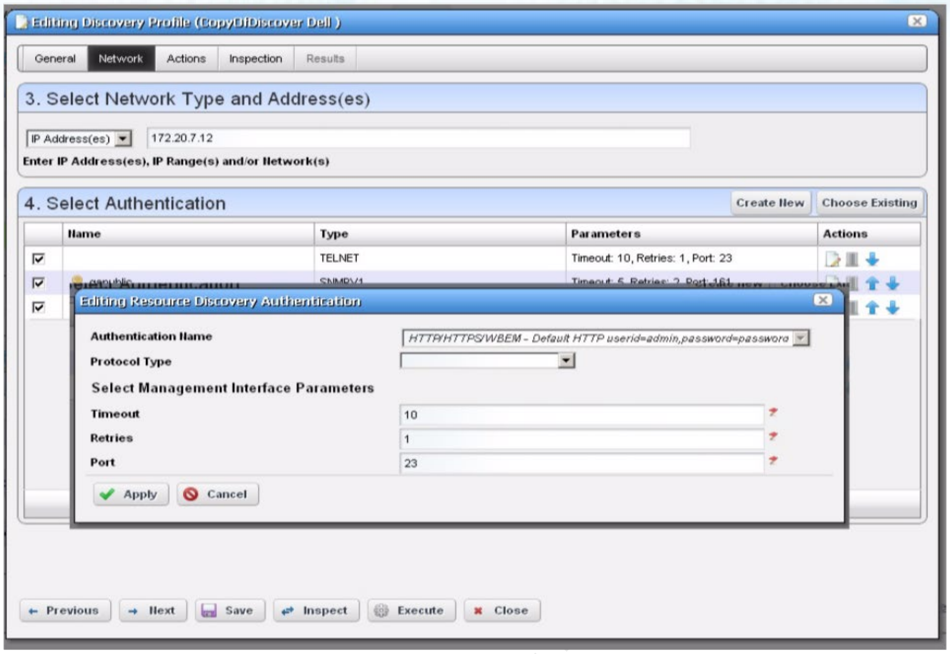
- *Save* each authentication. Each one should appear as a row in the Authentication portlet once you have configured them.

> ***NOTE: If you forget the IP Address you can retrieve it under my Alert/Action History.***

First Discovery

- Right-click in the Discovery Profiles portlet and select *New.*
- In the General (first) screen of the wizard, you must supply a name. All other parameters are optional.

- Click on the Network tab, supply the IP address range, hostname, subnet or CIDR address of the devices you want discovered.



Editing Discovery Profile (CopyOfDiscover Dell)

3. Select Network Type and Address(es)

IP Address(es): 172.20.7.12

Enter IP Address(es), IP Range(s) and/or Network(s)

4. Select Authentication

	Name	Type	Parameters	Actions
☑		TELNET	Timeout: 10, Retries: 1, Port: 23	
☑	public	SNMPV1	Timeout: 5, Retries: 2, Port: 161	
☑				

Editing Resource Discovery Authentication

Authentication Name: HTTP/HTTPS/WBEM – Default HTTP userid=admin,password=passworo

Protocol Type:

Select Management Interface Parameters

Timeout: 10

Retries: 1

Port: 23

- Go to Select Authentication. Click *Choose Existing. (S*elect from the authentications you configured in the Authentications steps above).
- In the pop up window; "Add Existing Authentication to Resource Discovery "verify settings and click *Apply.*
- Repeat exercise as necessary to add additional authentications.

NOTE: Most network devices need at least two authentications, an SNMP community, and a command line authentication (Telnet/SSH), although some require other types of authentications too.

If you have a range of devices with several different authentications, you can enter all relevant authentications. Just remember, Cruz sends these authentications in the top-to-bottom order they appear (and you can rearrange them with the arrows on the right).

- Click *Next.* For now, we observe that several actions occur in addition to Discovery, including adding the discovered equipment to an ICMP (heartbeat) monitor, discovering links, and resync (re-querying the device)
- Click > Inspection tab to proceed with discovery.
- When you initiate Inspection, it validates the authentications you have entered for a discovery profile. If authentications are incorrect, correct them before proceeding. You can save and re-open the Discovery profile without executing it. Click *Inspect.*
- Execute the Discovery profile. Either click *Execute*, or right-click a saved profile row in the Discover Profiles portlet to do this. Notice that you can also schedule Discovery to recur regularly, so your management system

can pick up any new devices. Note: All the discovered devices can be located under: Resources.

Re-Discovery

The following steps are for time-saving trainings when discovery has already occurred.

- Go to Resources > Managed Resource portlet, make a note of an already-discovered device's IP address, and right-click to *Delete* it.
- Go to Discover > Discovery Profiles portlet, right-click and *Copy* the profile that discovered the device you just deleted.
- Right-click the Discovery Profile copy, rename it. Go to *Network* tab, enter the IP address of the device you just deleted.
- Click *Inspect*, and confirm the device is online (ping), its hostname resolves (DNS), and its selected authentications are correct.
- Observe the *Actions* selected in that panel.
- Click > *Execute* button to initiate discovery of the device. Observe the Audit Trail/Job screen to see the message traffic between your system and the device.
- Confirm the device is in the Managed Resources portlet after discovery finishes.

Bonus Exercise

Examine the Audit Trail in *My Alerts* at the bottom left corner of the screen. Go to the Audit page, and view the discovery audit trail in the *Audit Trails* portlet.

Interface Capabilities

The home page in Cruz displays several portlets important to the initial stages of using this software. The following can help you tailor the screens you see in Cruz to suit your network management needs.

Drag-and-Drop — Notice you can drag-and-drop to move the portlets by clicking and dragging from the title bar.

Add and Delete Portlets — You can also click the “x” in the upper right corner to remove portlets, and click the *Add* > *Applications* menu at the top of the page to add them.

Expanded Portlets — Clicking the plus (+) in the upper right corner of a portlet makes an expanded version appear. The expanded portlet lets you create filters at the top, and select a row in the top panel to see details about it in the lower panel.

Portlet Defaults— Click the wrench in a portlet’s upper left corner to configure the portlet’s defaults. This includes the number of rows displayed per screen and the filter to apply to the contents of the page.

Create a Private Page

- Click Manage > *Page*. Click *Private Pages* (upper right tab).
- Click *Add Page* (Note available customizable page options
- Type in Desired Name of your Private Page.
- Note your Private Page will show on the Left Menu Bar.
- Click *Save*.

<u>Customize your Private Page</u>

- Select the private page you created. Go to *Add* > *Applications.* Type in “manage” in the search field to add a Managed Resources portlet to your page.
- Note that “Managed Resources” appears next to a green square in the list of available applications. This means you can add several such portlets to a single page. Purple squares appear next to applications limited to one per page.
- Click *Add* next to Managed Resource.
- Go to *Add* > *Applications.* Type in “Port” in the search field.
- Find Ports under Resource Management.
- Click *Add* next to Ports to add a Port portlet to your page.
- Close application dialogue box (on right upper screen).

- Move the Managed Resource portlet above the Port portal.

  NOTE: you can move portals up and down by drag and drop (note pointer changes to 4-way arrow and you can select the portal to move).

- When you are done customizing your options; click refresh page and note expanded portal view.

Using the Interface

The following steps let you explore the Cruz user interface. Remember, only changes made by administrators persist in non-private pages.

- Using the private page, you just created: expand the Managed Resources portlet by clicking the plus in the upper right corner. Notice that when you select a row in the expanded portlet, information about that row appears in the lower panel.
- Click the *Advanced* radio button at the top of the portlet, and create a filter that only displays a limited number of devices. (The default displays all of them).
- Make a filter for resources from the vendor Dell whose IP address contains a number in your training network. Go to Vendor (combo box on upper left top of screen). Click on the *Click to Select* button.
- Type in *Dell* in the search field and Click > *Go*. Select dell line item (will turn green) and then Click *Select* at the bottom of the page.
- Add a second filter. Go to green plus button on the upper left top of the screen. Click to add. *Select IP Address* is '*between*' on available combo boxes. Type in *Address Ranges*. Click > Go
- Click *Save As* to the right of the filter, and save it with a distinctive name (Example: "My Filter").
- Click the *Return to previous* link in the upper right corner of the screen. This should display the smaller portlet and the rest of the page where you added it.
- Click the wrench icon for the Managed Resources portlet.
- Select your filter in the *Current Filter* pick list.
- Click the *Columns* tab and look at the available columns. This screen allows you to *Show* some columns marked *Hide* and/or drag and drop the columns listed to re-order them.
- Click *Apply.* Notice that your Managed Resources portlet now displays only the devices your filter permits, and the columns you have configured.

  NOTE: To further customize your view, you can create additional Managed Resources portlets on the same page to display different filter settings.

- In addition to configuring the default list of devices, you can re-name the portlet. Click on the name "Managed Resources" and start typing (example: "Dell Devices"), then click the green check mark.

Bonus Exercise

- In the private page, you created; notice that when you click on a device in Managed Resources, the ports for that device appear in the Ports portlet. The *Context* label above the Ports portlet also displays the name of the selected Managed Resource.

Managed Resources

The Managed Resources portlet on the Resources page displays discovered devices. Right-click to act on a device.

> ***NOTE: You can multi-select in the expanded portlet with CTRL+Click.***

The following exercise opens a panel disclosing most device information.

Examine Device Details

- Click Resources. Right-click a device in the Managed Resources portlet.
- Select the *Details* menu item.
- Examine the subsequent panels for information about the device. The contents of these panels depend on the device discovered, and your interactions with it. The instructor may walk you through the panels visible here, explaining their origins.

Bonus Exercise

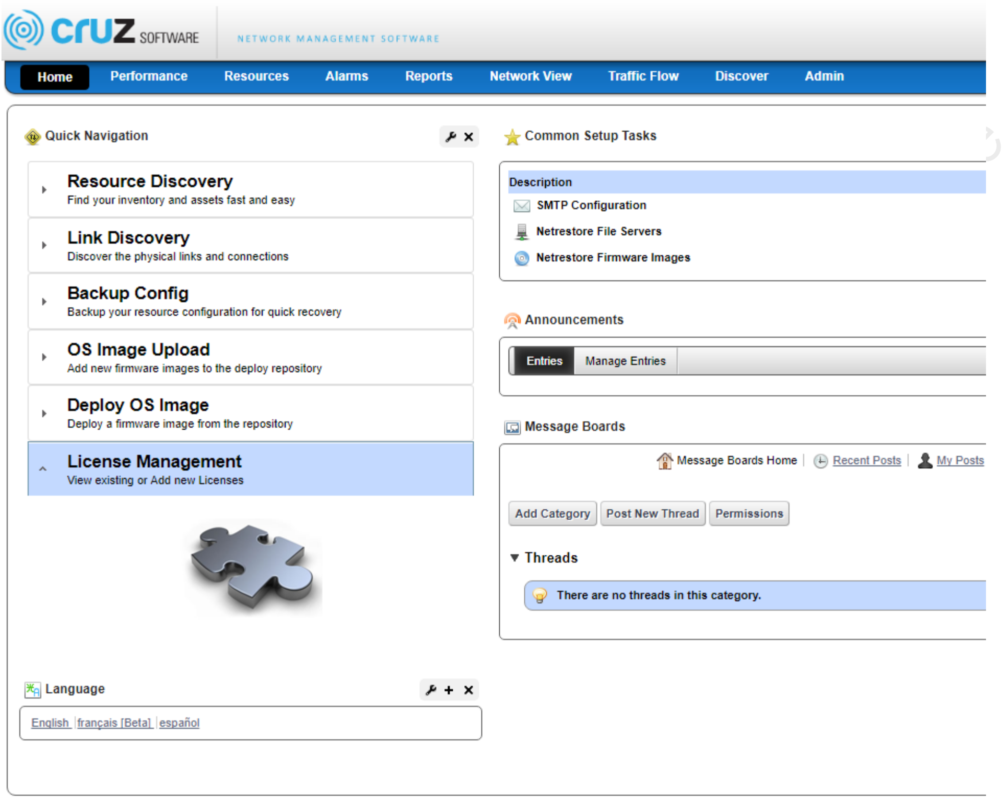
- Click Resources > In the Managed Resources Portal right click any device.
- Select the options available in the Direct Access right-click menu to ping the device, open a Telnet session or an SNMP session (MIB Browser) to examine the device directly.

> ***NOTE: Notice that right-clicking in the Event Definitions portlet, or a button in the MIB browser lets you load MIBs. This means, after you load a new MIB, you can even monitor events for devices or models not in your existing device drivers.***

DAY ONE – LATE

This continues the discussion of the User Interface Capabilities. Next, we will examine *Resource Monitors*.

Quick Navigation



Quick Navigation

Resource Discovery
Find your inventory and assets fast and easy

Link Discovery
Discover the physical links and connections

Backup Config
Backup your resource configuration for quick recovery

OS Image Upload
Add new firmware images to the deploy repository

Deploy OS Image
Deploy a firmware image from the repository

License Management
View existing or Add new Licenses

Language
English | français [Beta] | español

Common Setup Tasks

Description
SMTP Configuration
Netrestore File Servers
Netrestore Firmware Images

Announcements

Message Boards

▼ Threads

There are no threads in this category.

This portlet has links to several commonly used functions:

Resource Discovery — This initiates a pre-configured version of the wizard described in the Exercise: *Discover Your Network's Devices,* but only if you have configured a Discovery Profile to be the default. Right-click in the Discovery Profiles portlet. This skips additional discover steps like Actions.

Link Discovery — Initiates Link Discovery between discovered devices. Also requires a working FTP/TFTP Server. A subsequent screen lets you select the type of links (the more links you select, the more processing is required).

Backup Configs — By default backs up all configurations. You must have the FTP/TFTP server configured for this to work. We discuss this and the next two topics beginning with the *Day 2: Early session*.

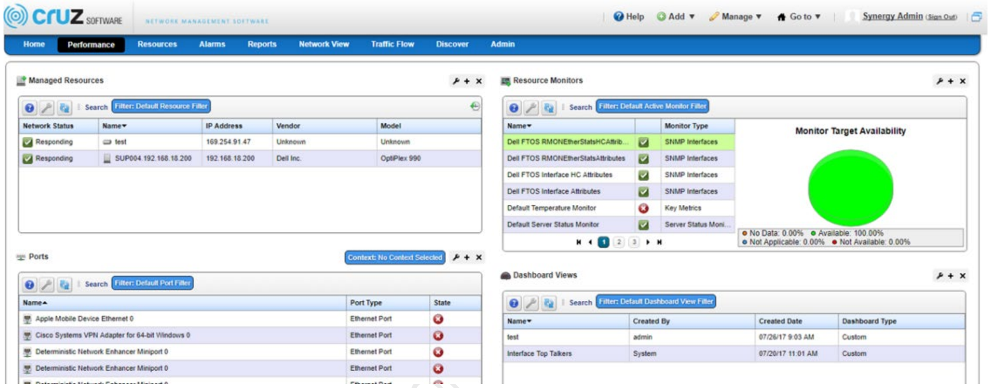
OS Image Upload — Uploads a device firmware/operating system image to ready it for deployment to devices your Cruz manages.

Deploy OS image — This pushes an OS Image/Firmware to the selected devices. Some devices require you to manually update their firmware.

License Management — This feature lets you view existing license, and add more licensed capabilities. The *Product Licenses* tab lets you view installed licenses for product capabilities, their dates of expiration and the types of permissions. The *Device Licenses* tab lets you see how many of which type of device are licensed for management.

Resource Monitors

To access Resource Monitors: Select > *Performance Menu*. Resource monitors will appear in the Resource portlet. Right click to Enable/Disable monitors in this portlet. You can also right click one of the existing monitors and select *Edit Monitor* to examine its contents.



Managed Resources

Filter: Default Resource Filter

Network Status	Name	IP Address	Vendor	Model
☑ Responding	test	169.254.91.47	Unknown	Unknown
☑ Responding	SUP004.192.168.18.200	192.168.18.200	Dell Inc.	OptiPlex 990

Ports

Context: No Context Selected

Filter: Default Port Filter

Name	Port Type	State
Apple Mobile Device Ethernet 0	Ethernet Port	☒
Cisco Systems VPN Adapter for 64-bit Windows 0	Ethernet Port	☒
Deterministic Network Enhancer Miniport 0	Ethernet Port	☒
Deterministic Network Enhancer Miniport 0	Ethernet Port	☒

Resource Monitors

Filter: Default Active Monitor Filter

Name		Monitor Type
Dell FTOS RMONEtherStatsHCAttrib...	☑	SNMP Interfaces
Dell FTOS RMONEtherStatsAttributes	☑	SNMP Interfaces
Dell FTOS Interface HC Attributes	☑	SNMP Interfaces
Dell FTOS Interface Attributes	☑	SNMP Interfaces
Default Temperature Monitor	☒	Key Metrics
Default Server Status Monitor	☑	Server Status Moni...

● No Data: 0.00% ● Available: 100.00%
● Not Applicable: 0.00% ● Not Available: 0.00%

Dashboard Views

Filter: Default Dashboard View Filter

Name	Created By	Created Date	Dashboard Type
test	admin	07/26/17 9:03 AM	Custom
Interface Top Talkers	System	07/20/17 11:01 AM	Custom

There you can see the following:

General Monitor Options

- Polling intervals

Monitor Options

- Select targets and Monitor Options

Calculated Metrics

- You can add formulas to normalize device-reported

Thresholds

- Configure thresholds to emit notifications

Inventory Mappings

- Standardize parameter terminology

Conditions

- Filter to create alarms.

Create an ICMP Monitor

The following steps create an ICMP (ping) monitor.
Monitoring can have a significant performance impact, so careful planning is an essential part of such systems' success.

Examining Retention Policies

- Select a monitor and right-click and selecting *Manage Retention Policies*. In the screen that appears next, notice the Default policy, and the editor (pencil and paper) button that appears to its right. These policies configure how much and how long Cruz retains data. When creating a monitor, we will accept the defaults, but remember: You can change the defaults with the editor, or add more such retention policies.

Creating a Monitor

- In the *Resource Monitors* portlet, create a new monitor by right-clicking within the portlet and selecting *New Monitor*.
- Select the type of monitor from the submenu—for this example, an *ICMP* monitor. Consult the *Cruz User Guide* for more specific instructions about other types of monitors.
- In the *General* screen, enter a name (“Test ICMP Monitor”), and a polling interval (5 minutes is the default). To get immediate feedback, select 30 seconds and accept the remaining defaults for checkboxes and the retention policy.
- Select one entity to monitor by clicking the *Add* button in the top portion of the *Monitor Options* screen.
- Press *Go Button* to see devices; Select the devices you want to ping (*CTRL+Click* to add more than one), then click *Add Selection* then click *Done* to confirm your entity.
- The ICMP Monitor Options panel allows the end user to modify Packet Size, Packet Count, and timeout. Otherwise, accept the default.
- In the Thresholds tab, click *Add* to select an attribute. (MaxRTT, or maximum round trip time for example). The “Adding new Threshold Information” screen will appear. Click *Add*
- Input the following threshold parameters:
    - A. Name *High* color red (click on color to change), Lower Boundary 200 and Upper Boundary [blank] Severity *Critical.* The related notification: monitorHighThresholdNotification
    - B. Name *Low* color green, Lower Boundary 0 and Upper Boundary 200 Severity *Informational*.
    - Configure this example to emit a notification. This means an alarm of the configured severity would accompany crossing the threshold. The *Event Processing Rules* configure automated reactions to such events/alarms.

> ***NOTE: To find monitor-related alarms, go to the Event Definitions portlet, expand it, and search for system events related to your topic (example: “threshold”).***

Here, **monitorHighThresholdNotification** might be one event appropriate to report a threshold crossing, but several others may be of interest. For example, you may respond to monitorTargetNotReachable, or MonitorTargetDown to report a device that is offline. Notice that you can also monitor device-emitted SNMP events (Examples: CPU use, memory utilization, temperature, and so on) and respond to them with Event Processing Rules.

Find the related events by searching the Event Definitions portlet, your device's documents or MIBs in the MIB browser.

Combining threshold events with polling intervals can alert you when latency becomes too high for too long. For example, if average ping response (latency) exceeds 200ms for more than two minutes. If polling were at 30-second intervals and four such intervals indicated the excessive latency, you can create an alarm by emitting an event.

- Accept the other defaults and click *Apply.* Then Click *Save.*
- "Test ICMP Monitor" now appears in the portlet.
- You can now display the data by right-clicking and selecting *View Monitor Data*. Notice that you can also *Enable/Disable* a monitor with a right-click.
- The *View Monitor Data* menu item simply displays whether monitor data is coming from the device. If you want a more informative view, do the next exercise.

Bonus Exercise

Create a monitor of another type (SNMP Interface, for example).

Dashboards

Dashboards provide a more user-friendly way to display data than the *View Data* option in monitors. You can see previews of such displays by right-clicking resources and selecting *Performance* > *Show Performance.* A *Performance* tab also appears when you right-click a device and select *Details*.
Neither dashboards nor Top N portlets can display data not collected. If monitors appropriate to the requested data are disabled, or not configured, then these displays, though they may exist, are empty.

Create a Dashboard

- Right-click in the Dashboard Views, and select *New* > *Simple Dashboard*
- Enter a *View Name*. (like "ICMP Dashboard")
- Push *Go* in the next screen, then select the desired device; then select *Add* > *Done.*
- Enter a time period and click *Add Entity* to the Entities panel.
- Click the Dashboard View Attributes, moving them from *Available* to *Selected.*

Cruz retrieves attributes from monitors targeting the selected devices.

- Click *Save.*
- To view the dashboard, right-click the newly created dashboard, and select from the *Launch* alternatives.

Complex dashboards let you display multiple dashboards side-by-side, so you could display the monitored MaxRTT next to the monitored AvgRTT.

Bonus Exercise 1

- Right-click to create a Custom Dashboard that displays MaxRTT next to AvgRTT.

Bonus Exercise 2

- Right-click to create a Performance Template, and assign it to a device. These override the default performance graphs that appear when you right-click a device in Managed Resources and select *Performance > Show Performance*. Confirm your template appears on the device you selected.

Top N

- Click on your own page you created in previous exercise (Create a Private Page)
- To see the available Top N portlets, click Add > *Applications*,
- Enter “Top” in the search field at the subsequent panel’s top. Click and drag one of these to the page where you want to see it. Alternatively, you can open Top N on the Left Menu bar and click *Add* on the desired item you wish to add.

> ***NOTE: By default, several Top N portlets appear on the Top N page under Performance.***

Some of these portlets require active monitors. For performance reasons, many monitors are not enabled by default, and you can add and enable additional monitoring later, so the appearance of data in Top N portlets may be uneven.

Traffic Flow Analyzer

The Traffic Flow Analyzer lets you monitor Flow transmissions from devices. Supported versions include sFlow v5, and NetFlow/JFlow v5 and v9, but not previous versions (for example, v2).

Troubleshooting Traffic Flow

Most problems with Traffic flow are related to device setup and license limits. To receive Traffic Flow data, devices must register the Cruz server as an authorized receiver. Force10 devices can only register two such receivers.

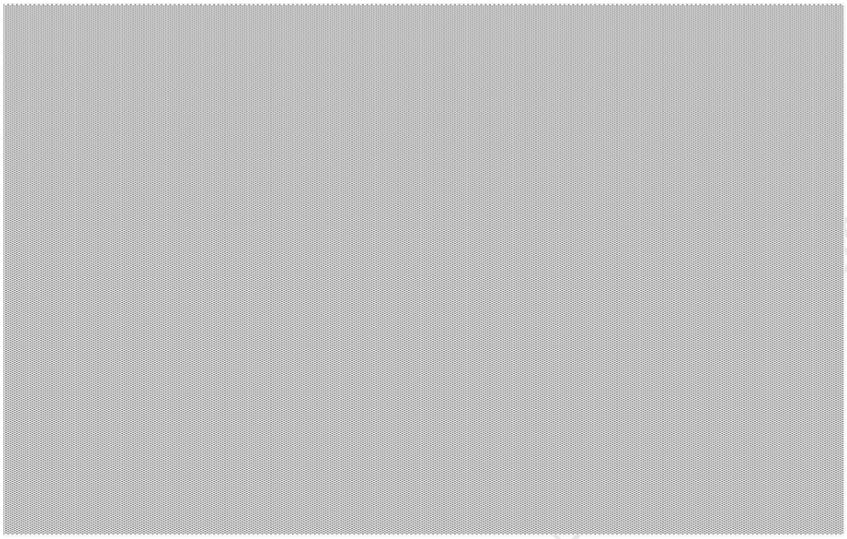
Make sure the device sending traffic flow is a router, and you have registered it. To register for flow information, right-click the device in Managed Resources, and select *Traffic Analyzer > Register.* Notice that you can also select *Show traffic* to see a snapshot of flows from the selected device (if the period you select also has flows).

The number of exporters available for your system are limited through licensing. Review your Traffic Flow Analyzer license setting in the license viewer under Product Licenses tab, the license detail section (MaxExporterCount=n, where “n” is the number of exporters licensed.) After reviewing recommendations for performance tuning and hardware sizing, you can request a license allowing more exporters from your sales representative.

Finally, after setting it up, traffic flow may take some time to appear in the portlets that display it. Network latency and processing times are at the root of this problem. Patience is the remedy.

Flow for Flow...

- How does it work?



- The NetFlow/sFlow exporting router monitors traffic traversing it ...and the router becomes an Exporter of NetFlow/sFlow data.
- It forwards information to the NetFlow/sFlow Collector
- Collector stores, correlates, and presents the information about
- Traffic bottlenecks in networks.
- Applications responsible for bandwidth utilization.
- Setting up and monitoring sFlow lets you monitor things other than SNMP reports, to/from endpoints, etc.

Set up Flow Emulation

- Discover your application server. (Create authentications, and a Discovery Profile, and execute it). Note: See previous exercise *Discovery*
- Edit the server in your Managed Resources Portlet so that it is a Router. Right-click *Edit* and in the General tab, Properties sub-tab, change the *Equipment Type* to Router. Then click *Save*.
- Right click the “Router” you just made and register it to receive Traffic Flow.
- Locate the Traffic Flow emulator in [installation [root]\owareapps\trafficanalyzer\simulator.
- Decompress this file and run NetflowSimulator.exe
- Click the... button to the right of the Data field in the Simulator, and load the NetFlow_v5_RawData.dat file.
- Uncheck *Raw Data*.
- Enter your application server host’s IP address in the *Address* field, and check *Repeat.* Select any number of repeats.
- Click *Send Data*.

- Wait a minute or two, then open the Traffic Flows page in your Cruz.
- Change the time to the last 15 minutes for the portlets that appear there with the clock icon in the upper right corner of the portlet.

DAY TWO – EARLY

This day begins with a look at Cruz's configuration file management capabilities.

File Management

Use Cruz's File Management capabilities to manage device configuration files, and several other functions, like Link Discovery.

FTP/TFTP File Server

The internal file server is exclusively for testing. Install an external FTP/TFTP server. Open source servers include Filezilla and tftpd64. You must have a configured file server installed before you can proceed with this section.

Since your system requires only one FTP and/or TFTP server (although you can configure more), doing so is not an exercise. To configure these servers, go to the Resources > File Management page and right-click in the File Servers Portlet. Configure the IP address and login/password for the configured server. Remember: If you have separate processes for FTP and TFTP, they must write to the same (shared) director, with sufficient permissions to read, write and execute there. Use the *Test* button on the File Server editor to confirm any server you configure works.

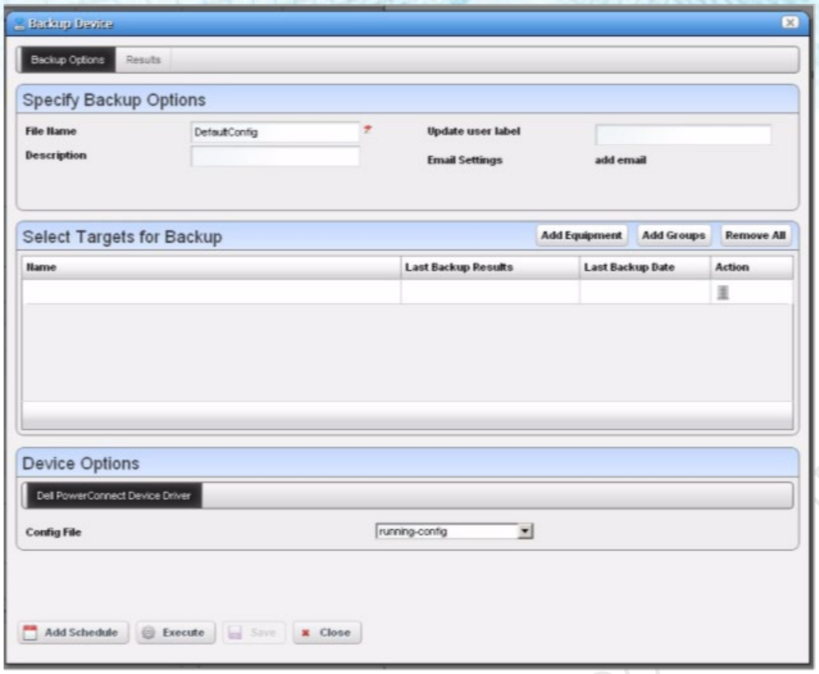
Backup Configurations

Cruz simplifies backing up devices, so you always have their configuration files, even if the one on the device becomes corrupted or out-of-date.

> ***NOTE: You can back up several devices at once for what amounts to a "group operation." Select more than one device by CTRL+Click in the expanded portlet, then right-click as outlined below. You must expand portlets to multi-select. You can also back up several devices at once by right-clicking Managed Resource Groups in that portlet on the Groups & Locations page.***

Here are the steps to back up a device:

- Right-click a device in the *Managed Resources* portlet.
- Select File Management > Backup.
- Configure the subsequent *Backup Device* screen.



File Name: DefaultConfig

Description:

Config File: running-config

This screen lets you configure the following:

File Name — A text identifier for the file.

Description — A text description of the file.

Update User Label — A label for the file. Entering such a label creates it, and makes it available for later restoration, comparison, and so on.

Email Settings — Click *add email* to configure an email notification about this backup.

Select Targets for Backup — This screen defaults to the device you selected in *Managed Resources.* You can also click the *Add Equipment* to add individual devices, or *Add Groups* to add groups, or *Remove All* to manage devices that appear in this list of targets.

Device Options — This portion of the *Backup Options* screen displays detailed configuration options available for the selected target. For example, you could select between backing up the running-config and the startup-config. Click one of the buttons at the bottom of the screen to initiate the next backup action.

Add Schedule opens the scheduling screen to let you automate the backup you have configured on a specified date, time, or repetition.
Execute performs the backup immediately. The *Results* tab in this screen opens, displaying the message traffic between Cruz and the device(s). See *Audit Trail Portlet* on page 187 of the *Cruz User Guide*.
Save preserves this configuration without scheduling or executing it.
Close closes this screen without saving the configured restoration.

- After you have executed backup, the file you back up should appear in the *Configuration Files* Portlet (Select: Resources > File Management).

Bonus Exercise

- Right-click after you have selected a file, and you can *View* or *Edit* it. If you *Edit* and save it, Cruz makes another version (Note: the version column indicates which is the most recent).
- Notice that unlike most summary portlets, you can *CTRL Click* in the Configuration Files portlet and select two files (usually you must expand the portlet to do this).
- Right-click after you have selected more than one file, and you can view a file comparison with differences highlighted.

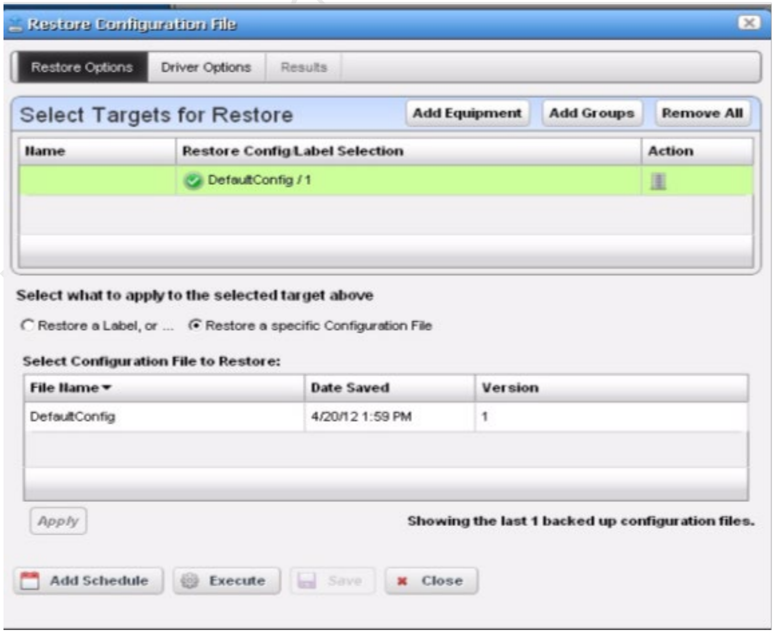
Restore Configurations

> ***NOTE: Configuration file restoration is not something to take lightly. If you have altered the configuration it has an impact on the device to which you restore it. To be extra safe, you can conclude this exercise before restoring the file.***

How To Restore

The following are the steps to restore a config file to a device:

- Right-click a device in the *Managed Resources* portlet. Note: Pick the same device as your previously backed up.
- Select *File Management* > *Restore.*
- Configure the subsequent *Restore Device* screen.



Select Targets for Restore

Name	Restore Config/Label Selection	Action
	✓ DefaultConfig / 1	

Select what to apply to the selected target above

○ Restore a Label, or ... ● Restore a specific Configuration File

Select Configuration File to Restore:

File Name	Date Saved	Version
DefaultConfig	4/20/12 1:59 PM	1

Showing the last 1 backed up configuration files.

This screen lets you configure the following:

Select Targets for Restore — This portion of the screen lets you *Add Equipment, Add Groups,* or *Remove All* target devices. Listed targets appear with their *Restore Config/Label Selection*. Note that you can click the icon in the *Action* column to remove the listed target.

Select what to apply to the selected target — This portion of the screen lets you select either a label (like *Current, Compliant,* and so on—a selector listing available labels appears onscreen once you click this option), or Click *Restore a specific Configuration File*. The latter lists available files and lets you click to select. Click *Apply* to configure the selected target, or *Apply to All* to configure all targets.

Click one of the buttons at the bottom of the screen to initiate the next restore action.

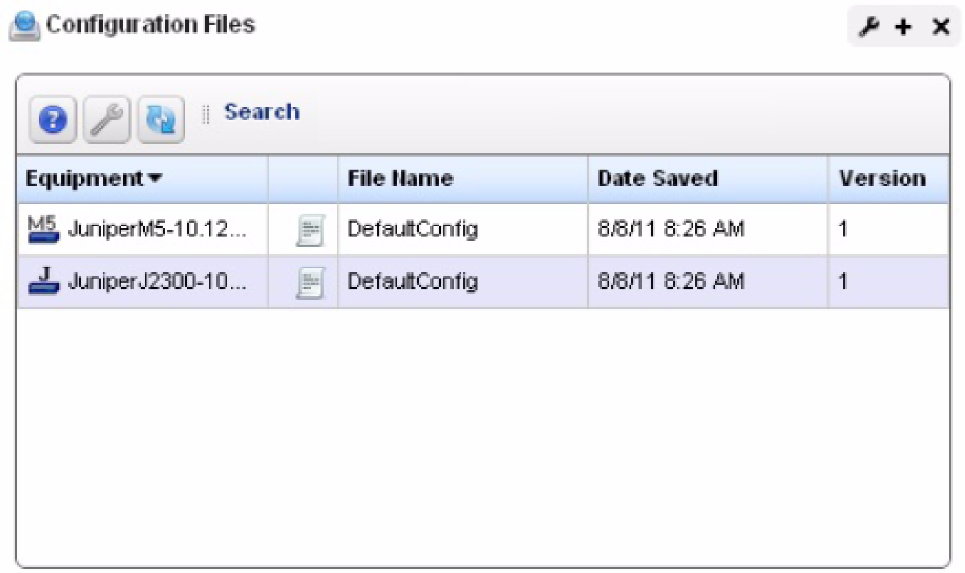
Add Schedule opens the scheduling screen to let you automate the restoration you have configured on a specified date, time, or repetition.

Note that *Execute* performs the restoration immediately. The *Results* tab in this screen opens, displaying the message traffic between Cruz and the device(s).

Save preserves this configuration without scheduling or executing it.

Close closes this screen without saving the configured restoration.

Configuration Files



Equipment		File Name	Date Saved	Version
JuniperM5-10.12...		DefaultConfig	8/8/11 8:26 AM	1
JuniperJ2300-10...		DefaultConfig	8/8/11 8:26 AM	1

Go to Resources > File Management > Configuration Files Portlet. Note the backed-up configuration files in this portlet. Right-clicking offers you the following options (all options listed may not be available):

View/Edit — See or edit the backed-up configuration file, if it is not a binary file. See the end of the section labeled *File Management* for a description of these capabilities.

Assign Labels — Label a single selected configuration file. A label selector appears that lets you select an existing label and create a new one. If you assign one file the *Current* label, others from the same device cannot have it. Cruz automates moving *Current* from one file to the other, if another has it. You can delete non-system labels from devices in the selector this menu item produces.

Compare to Label/Compare Selected — Compare labeled configuration files to the current selection. You can create labels when you back up a config file, or you can compare to the default labels *(Change Determination, Current, Compliant)*. If you select two configuration files in the expanded portlet, you can also *Compare Selected*.

Backup/Restore — Back up the device (again) related to the selected file, or restore the selected file.

Aging Policy — Configure the retention of this config file. See *Database Aging Policies (DAP)* of the *Cruz User Guide*.

Archive — Save the selected file to disk, and optionally delete it from this list.

Import/Export — Export the selected config file to disk, or import it from disk.

Delete — Removes the file from the Cruz database without exporting it.

NOTE: You can use the browser's "Find" function (typically initiated with CTRL+F) to locate text within the view.

Aging Policy — Opens the Aging Policy selector. See the *Cruz User Guide* for more about these. You can configure them in Control Panel.

You can also import and export a selected config file.

Edit then Compare a Configuration

- Right-click a configuration file in that portlet and select *Edit.*
- Find a description within the configuration file. Alter it.
- Save the file.
- Notice that the file re-appears in the Configuration Files portlet now as version 2.
- *CTRL+Click* to select version 1 and version 2 of the configuration file.
- Right-click and select *Compare.*
- The comparison appears onscreen, highlighting the change you made.

Image Repository

This portlet is found under Resources > File Management and stores firmware images and configuration files. You can right-click to download the latest Dell Power Connect firmware, and some firmware may ship with your package.

Some explorations:

- Right-click to create a *New* firmware entry. Notice that you can load a file from a local disk or a URL.
- Select *Deploy* (without executing it) and observe the fields on the subsequent screen. Notice you can schedule firmware deployment.

DAY TWO – LATE

This portion of the training deals with Alarms, Events, and Event Processing Rules.

Setting up an SMTP Server

To set up an SMTP server:

- Click *Admin* > Go to Common Setup Task Portal > SMTP Configuration > Click *Edit*
- A screen called *SMTP Configuration* will pop up.
- Provide the appropriate information required (provided by your administer/end-user).
- When data is entered; Click *Test*
- Once test is successful; Click *Apply*

NOTE: If unable to set up an SMTP server for this training, the end user will not be able to receive an email alert created in exercises below.

Alarms

All alarms are events; not all events are alarms. These messages typically come from monitored devices. Some devices require you to configure them so your Cruz is an authorized recipient of traps so alarms and events appear in your system.

Right-click an alarm, and notice that you can acknowledge it, assign it and even e-mail it to another user.

Notice also that, like Managed Resources, you can select a *Details* screen to view information about the alarm, the event on which it is based, and, if available, a performance dashboard from the device where it originated.

Event History

By default, the Event History portlet displays events that occurred in your system over the last hour. Expand the portlet with the plus in the upper right corner to create more filters.

Create Multiple Event History Portlet’s

1. From the Event History portlet, click the plus (+) in the upper right corner to display the Expanded Event History portlet
2. Click the *Advanced* radio button to create filters, create a filter for events in the last 1 day. Click *Save As* > *Save*.
3. Return to the page with the Event History summary portlet. *Add* > *Applications* to add another Event History portlet.
4. Search “event” (Add Event History> Refresh Screen). Drag screen (up/down) next to existing events portlet.

5. Click the *Settings* button (wrench icon) for this portlet, and select your Last 1 day filter as its default.
6. Click the title of this second Event History portlet, and rewrite it to be “Events in the last day” Click *Save* > *Apply*
7. Notice the difference between the two Event History portlets.

Event Definitions

Alarms are all events, but not all events are alarms. On the Definitions and Rules page, in the *Event Definitions* portlet, you can right-click to set behavior and the alarm severity (Critical, Major, and so on) of events with the right-click menu.

Set Behavior – *Reject* – Every received message is rejected.

Suppress – The message is tracked in Event History and then ignored.

Alarm – The message is tracked in Event History and then processed, with Correlated events and Event Processing Rules of any type other than Syslog.

These definitions also let you set their alarm severity, see their MIB, and *Edit* them. All the information that appears by default in the editor screen comes from the device MIB.

NOTE: Although MIBs are most often English only—as far as we can tell, Cisco does not provide a French MIB, for example—you can enter Advisory Text when you edit Event Definitions, in these other languages. You can even copy the MIB text into something like Google translate and copy the translated text to Advisory Text. This text then appears along with the event, for example in the Alarm Details screen.

Find Events Relevant to Your Use Case

1. Go to Alarms > Definition & Rules > In the Expanded Event Definitions portlet, (click + to expand) create a filter for all System events (events for Cruz).
2. Click *Go* and observe how many events Cruz provides.
3. Add more filters to find system events related to monitors, thresholds, logins, and so on.
4. After you have filtered to find events in a specific area, select the row and then right-click to examine a relevant event. Then Select *Edit*.

5. Events can automate responses (described below in Event Processing Rules

6. Formulate the kinds of responses you might need for known use cases. Responses permitted include sending e-mail, SMS, forwarding traps, and any Actions/Adaptive CLI

Event Processing Rules

Event Processing Rules configure automated responses to events or alarms in Cruz. Right-click and select *New* in the Event Processing Rules portlet to make either pre- or post-processing rules.

Pre-processing rules sometimes create Events for things that may not currently trigger them. For example: The *Device Access* type of rule creates an Event for occasions like user login/logout.

Examine the individual screens in the Event Processing Rule editor to see how this works.

Post-processing rules automate event responses after an event occurs. For example, such a rule could send e-mail to a relevant responder in after Cruz receives an alarm.

For post-processing rules, the *Actions* tab in the Event Processing Rule editor lets you specify what occurs after the triggering event arrives at your system. The *Custom* action lets you specify anything that appears in the Actions portlet. (See *Actions/Adaptive CLI*.)

If you have set up your system to use an SMTP Server, you can send e-mail in response to an event. For the sake of simplicity, the exercise below automates assigning an example alarm to a user.

Create a Post-Processing Rule

The triggering event for this post-processing rule could be the standard linkDown notification (IF-MIB contains the Critical alarm), however, to demonstrate the rule's operation more conveniently, we specify redcellNetConfigBackupFailure-Notification. One can create backup failures by disabling the FTP server in the File Servers portlet (right-click, and select *Disable* for your server).

Create the Rule

1. Go to Alarms > Definitions & Rules. Right-click in the Event Processing Rules portlet and select *New* > *Post-Processing.*
2. Name the rule *MyTestRule.* Make sure *Enabled* is checked (the default). Click *Next*.
3. Go to Filtering Tab > Specific event (s). Click *Add.* Under event name search *backup* and then select > redcellNetConfigBackupFailureNotification. Select *Add Selection* > Click *Done.*
4. Go to Filter Conditions; Select *Add Filter*. Notice you can further filter the selected event, triggering the rule only if it comes from a specified IP address, for example, in the lower panel. Click *Next*.

NOTE: We have selected an event that is easy to emit (just disable your FTP/TFTP server[s]), but you may find other events more useful. One example:

redcellEquipmentLoginFailureNotification. You may also want to alter the default behavior of the event (Suppress/Warning for redcellEquipmentLoginFailureNotification) and configure the appropriate automated response with an Event Processing Rule.

5. In the *Actions* tab, select *Add Action* > *E-mail*, and configure the mail to go to yourself for testing purposes. Fill in Description; configure email settings and Click *Apply*.

   Notice that you can specify several recipients (Click green + to add recipients), and the text of the mail, including variables. For the complete list of variables, refer to online help or the *Cruz User Guide*
6. *Save* this rule.

Create the Alarm

1. Disable the FTP server in File Servers portlet (Found in Resources > File Management) Right-click > Select *Disable.*
2. Right-click a device in the Managed Resources portlet and select File Management > Backup.
3. “Execute” the backup.

Check for Automation

Look at your email server to see the email notification associated with a specific alarm parameters (see previous exercise).

Create a Pre-Processing Rule

The following exercise creates a pre-processing rule that turns the Minor alarm about a failed backup into a critical if it comes from a single device.

1. Go to Alarms > Definitions and Alarms > Right-click in the Event Processing Rules portlet and select Pre-processing > Set Severity.
2. Name this (for example: Test Severity Setter)
3. Click *Next* and *Add* the RedcellNetConfigBackupFailureNotification event. Notice that you can add more than one.
4. With *Add Filter,* configure a filter so only a specified IP address responds to this rule. Make a note of the devices name you configure.
5. Click *Next* and select the severity you would like applied to the minor-by-default RedcellNetConfigBackupFailureNotification event. For contrast, select *Critical.*
6. Make sure your FTP server is still disabled.
7. Go to Managed Resources, and right-click the device you specified with the *Add Filter* step. Select File Management > Backup > Execute.

8. Notice that the Job viewer (Audit Trail) lets you know this failed, generating the RedcellNetConfigBackupFailureNotification event.
9. The Critical alarm should appear in the Alarms portlet.

NOTE: Rather than showing duplicate alarms, the Alarm portlet updates the Count column (the DateOpened column documents the time/date for the initial alarm). With its default filter, the Event History portlet displays only an hour’s worth of events, but the events appear individually.

DAY THREE – EARLY

This session focuses on Cruz's reports, automated topology Network View, along with Traffic Flow, the Admin page, and Schedules.

Network View

This automated topology provides a quick look at all discovered devices, by default, and lets you delete/add devices and links for a quick look at device status. The following are some important features:

- ***Devices and links*** appear colored with their highest alarm state.
- Hover your cursor over a device or link for a quick ***tooltip*** summarizing its description.
- Right-click to ***expand/collapse*** devices and see all interfaces.

  Navigation Note: The + or - magnifying glasses let you zoom in and out. Click and drag to select an area to magnify. The hand cursor lets you click and drag to move the view. The arrow lets you view tooltips. See the Exercise *Navigating Through a View*.
- Right-click to *"**drill in**"* and isolate a device and its subcomponents. Click the breadcrumb menu at the top of the screen at the location to which you want to "collapse" a drilled in view. ***Stacked nodes*** expand twice to get to interfaces.
- Click the disk icon to ***Save*** an arrangement. If you have the *Visualizer Views* portlet on the same page, selecting a view listed in that portlet makes it appear in the *Visualize My Network* portlet.
- Right-click to open the ***Details*** panel with very detailed information about a device.
- **Customizing:** Click the pencil icon (far left) to permit adding labels and links between views.

  After you click the pencil, the Properties > Background Settings on the lower right lets you upload a background image, change its opacity, color the background, and so on. You could upload a map, drag, and drop devices to their correct locations on that map, then save that as a view.
- ***List Devices:*** The far right lower tab lets you see a complete, nested list of devices. Click one to see it highlighted in the logical topology on the left.
- The *Shortest Path* tool lets you select two devices, then automates selecting the shortest path between them.
- The *Bifocal effect* tool lets you magnify selected portions of the topology.
- You can search with the search magnifying glass, and determine which is the default view with the wrench.

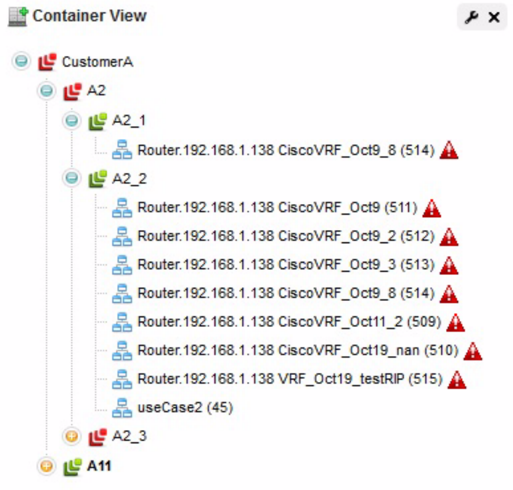
Navigating Through a View

1. Go to Network View. Click the hand icon, and click and drag the topology that appears in Visualize My Network

2. Click the arrow icon and hover the cursor over a device or link. The tooltip appears to describe that item.
3. In the *Overview* notice that while you have selected the arrow cursor, a rectangle appears in a miniature of the view. Click and drag that rectangle to move throughout the view.
4. Click the + magnifier tool, and drag it to a rectangle to magnify within the view.
5. Click the - de-magnifier, and click the view to zoom out.
6. Go to the right >> tab and open. Use the - to + slider in the *Overview* on the right to zoom out and in.
7. Click the right most tab under *Overview* to see a list of the devices within the view.
8. Click the magnifying glass (no + or -) to search for a device. Highlight and center the device once you have found it.

Containers

Containers are, in effect, visual filters. Put them on a page with other portlets, and those other portlets' contents reflect what you click in the Container View Portlet. Containers are created in the Container Manager portlet, and view them, and their effects, with a Container View portlet.



Container View

- CustomerA
  - A2
    - A2_1
      - Router.192.168.1.138 CiscoVRF_Oct9_8 (514)
    - A2_2
      - Router.192.168.1.138 CiscoVRF_Oct9 (511)
      - Router.192.168.1.138 CiscoVRF_Oct9_2 (512)
      - Router.192.168.1.138 CiscoVRF_Oct9_3 (513)
      - Router.192.168.1.138 CiscoVRF_Oct9_8 (514)
      - Router.192.168.1.138 CiscoVRF_Oct11_2 (509)
      - Router.192.168.1.138 CiscoVRF_Oct19_nan (510)
      - Router.192.168.1.138 VRF_Oct19_testRIP (515)
      - useCase2 (45)
    - A2_3
  - A11

The filtering effect of clicking on a container, or sub-container, occurs in other portlets on the same page as the Container View.

Create and View Containers

1. Go to Admin. Locate the Container Manager portlet and right-click to create a *New* container.
2. Under Container Details type "Top Container Practice". Go to Authorizations > Add Role > Select *All* (to offer all access). Select All > *Apply*.
3. *Click Save*.
4. Click *Add Child*. Name this sub-container > Location 1

5. Go to the Membership tab. Select > *Static.* Click *Add.* Select three devices (Left click on a device and Add Selection, repeat) Click *Done* > *Save.*
6. Click on Top Container Practice > *Add Child.* Name this sub container > Location 2. Add three differences devices (see step 6)
7. Go to Alarms > Alarms by Location page and see the Container View and Alarms portlets together.
8. Click on one sub-container, then another. Notice how the Alarms portlet reflects the alarms on devices within each sub-container.

Bonus Exercise

Right-click the Location # sub-containers and Tag them with a map location. Go to Add Application > Search *map*. Click on Map Context > Add. Notice the Map Context portlet to see the tagged locations.

NOTE: The application server(s) for your system must have internet access for maps and tagging to work.

Reports

Reports are easy to use. Right click one in the Reports portlet. Note *Execute and Advanced Execute options. Execute* starts running the report right away, displaying the Job Viewer/Audit trail, while the *Advanced Execute* selection allows you to e-mail the report, save it, or export it as a file. Of note: *Execute* the report, and its progress appears in the *My Alerts* portion of the status bar. Click the magnifying glass to the right of its announcement of completion.

Create a New Report

Here are the steps to create a new report:

First the Template

1. Go to the Report Templates portlet, and right-click to create a *New* > *Table* report template.
2. Name the template: *TestCardTemplate*.
3. Go to the *Source* tab and select *Inventory Resource (A - DD)* > *Card.* Once you select this, potential inventory columns appear in the lowest panel of the editor.
4. Enter the columns to appear in the report by selecting a type/attribute, then clicking the right arrow(s) to move it to *Selected Columns*.
5. After you have configured these columns, you can further modify their appearance and order in the *Layout* tab. The top column is leftmost. Select a column to refine its label, font, color and so on.

NOTE: Selecting too many columns can sometimes cause problems for PDF-formatted reports. Execute

Advanced lets you create CSV reports for numerous columns. Any standard spreadsheet program can open these reports.

6. Click *Save* to preserve that template.

Then the Report

7. Right-click in the *Reports* portlet. Select > *New* to create the report based on this recently created template. Notice it automatically selects the last template (TestCardTemplate) you worked on. Enter an identifier for this report in *Name > TestCardReport.*
8. In the Filter tab, click *Add Filter* > *Create New*.
9. Name the filter (Ethernet Cards), noting that the entity type selected on the right matches the template's selection (Card).
10. Click *Add Conditions* and select *Card Type is Ethernet Card.*
11. Click *Apply.* Then click *Save to save filter. Click Save.*
12. Right-click and either *Execute* or *Execute Advanced* your new report. The pdf of the report appears ready for viewing when you click the *My Alerts.* If you have set up SMTP, you can send e-mail to yourself with the report attached with *Execute Advanced.*

Bonus Exercise
Expand the Reports portlet and explore the History panel.

NOTE: The format of a report matters. For example, if your report needs to capture 100 columns, use CSV (comma-separated values) instead of a PDF format. You can import CSV files into spreadsheets to view or edit them in a user-friendly way.

Admin

The admin page displays the Application Server Statistics portlet and others (Common Setup Tasks, where you can set up SMTP, FTP/TFTP servers, and firmware images).

Audit — This portlet on the *Audit* child page lists all the Job Viewer/Audit trails you have run (before DAP archives them)

Groups and Location — These portlets include default groups (*Dell, All Devices*, and so on) and default locations. Groups can be Static (to which you add devices by selecting them manually) and Dynamic (to which you add devices by filter). Group operations let you run operations like file management (backup, restore, deploy) on several devices at once.

Schedules — Notice some schedules are already seeded, like running Data Archiving Policies (configure those in Control Panel). You can manually create schedules too.

Actions/Adaptive CLI

Adaptive CLI/Actions are command lines sent to devices. Cruz manages device login, and keeps an audit trail of who initiated the action, and the messages and responses received.

These commands amount to “mini-scripts” to query and configure those devices. Adaptive CLI’s Attributes capabilities let you insert variables in scripts. Two types of Adaptive CLI are available: Perl Script and Embedded Script.

Actions: Perl Script Exercise

Use Existing Action

1. Go to Resources > Actions. In the Actions portlet; search for “show start config” Click on Dell Networking (FTOS) Show Startup Config.
2. Right-click and select *View Scripts*
3. Observe the (Perl) script contents (println “show startup config”). Cruz sends show startup config to the device selected when you execute this Action.
4. Close the pop up window.
5. Right-click and select *Execute.*
6. Select one or more Dell Networking (FTOS) devices. Click *Add* > *Selection* > *Done*. In the next screen Parameters; Click > *Execute.*
7. Observe the Job Viewer Audit Trail which catalogs the message traffic between Cruz and the device(s).
8. Observe the output in the *Results* tab.

Create a New Action to Extract Data

1. Go to Resources > Actions. Right click in the Actions portlet. Select *New* > *Adaptive CLI.*
2. In Name Field Type; *Training Show Interfaces*. In Type; Select CLI Show Command. In Target Type; Select > Managed Devices.
3. Select Scripts Tab. Click > *Add New Script* > *Perl.* In Script Content tab; Type; println “show interfaces”;
4. Click *Enter* > Click *Apply.*
5. Click *Save.*

Execution of Created Action

6. In Actions Portlet; Search: *training show interfaces* Click: *Enter.* Select it, right Click, and Click *Execute.*
7. Select any device from table and click *Add Selection.* Click *Done.* Under Input tab: Click *Execute.*
8. Note in the Executing Action screen under results tab; show interfaces command executed against selected device. Close the screen.

Creating Parameters for Existing Action

9. In Actions Portlet; Select Training Show Interfaces action you previous created above. Right click and Select *Edit.*

10. In Action Associations screen (bottom) Click *Add*. Select Dell Networking (FTOS) and Click *Apply.*
11. Under the Attributes tab; Select *Create a New Parameter Schema*. Click *Create New*. In the Entity Type Name Field type; Interface Name.
12. Click on Attributes Settings tab, Click *New* > *String.* Type in Interface Name in Label Field. Click *Save.*
13. Select Scripts Tab. Under Script Settings; Edit the Action.
14. Under Script Content tab note the existing script (Script 1). For this training exercise, under existing script type: println “show interfaces”;
15. Position the cursor after the s of interfaces before the double quote. Press space bar. Go to Parameter; double click on Interface Name. Notice the indictor on the left side of Interface Name is red (Mark as Not Used). Go to Show (below) and click on green (Add as Required).
16. Go to Target Filter > *Click to Select.* Type *Force*. Click *Go*. Select Resource Group Filter Dell Force10 and Click *Select.*
17. Note: Now the action is only going to be executable against that are within the filter. Click *Apply* > *Save.*

<u>Executing Action Against a Valid Device</u>

18. In Actions Portlet; Select Training Show Interfaces action you previous created above. Right click and select > *Execute.*
19. From the table select any Dell Force10 device. Select the device; Click *Add Selection >Done*. In Interface Name Field: type Interface Name. Click *Execute*. Notice in Results screen execution of specified interface. Click *Close*.

Bonus Exercise: Executing Action Against Invalid Device
In Actions Portlet; Select Training Show Interfaces action you previous created above. Right click and Select *Execute.* From the table select a non-Dell Force10 device. Click *Add Selection.* Click *Done*. Note invalid target error pops up in the upper right corner.

Create Action using Embedded Script: Extracting a DateString

1. Right in Action Portlet; Select *New* > *Adaptive CLI.*
2. Name the Adaptive CLI; Date Extract. Select *Type*: CLI Show Command, and *Target Type*: Managed Devices).
3. Under the Attributes tab > Select Create a new Parameter Schema. Click *Create New*. In Entity Type Name Field Enter *DateString*.
4. In the Attributes Settings tab Click *New* and Select *String*. In Label Field Type: *DateString*. Click *Save*.
5. In Scripts Tab; Click *Add New Script*. Select *Embedded CLI*.
6. In the *Script Content* tab; type: show startup-config | grep date
7. Click *Enter.*
8. In the Value Extractions tab: Click *Add*. Go to Parse Exression Field and Type: (\w{3}\s+\w{3}\s+\d{2}\s+\d{2}:\d{2}:\d{2}\s+\d{4}).

9. Click *Apply* > Click *Apply* (to save the script).

10. Click *Save* (to save the Adaptive CLI.).

11. Right-click this Adaptive CLI, and select *Execute*.

12. Select a (Force10) target device. In Executing Action Form Click *Execute*. Note: The job Viewer displays an audit trail of the message traffic between Cruz and the selected device.

13. When the Adaptive CLI completes its run, the *Results* panel displays the script sent the device(s), and what returned.

14. Click the Job Viewer tab to see what was extracted to the configured attribute., click the *Job Viewer* tab. Click the last message: “Set attribute extraction results, click here for details.”

15. Notice the lowest panel shows the datestring extracted results.

DAY THREE – LATE

ProScan/Change Management

ProScan is part of Change Management. Running the Change Management process essentially compares configurations currently on devices that have experienced change with those left from the previous Change Management process run. These are outlined in the *Configuration Change Report*, a pre-made report you can run on a schedule to track where changes are occurring in your network.

Create and Run ProScan

The following steps create a ProScan typical for many networks. It scans configurations, or the results of Actions/Adaptive CLI

, and looks for things out of compliance with your business rules. SNMP community = public is a typical out-of-compliance items. This may be the factory default for your device(s), and users may get this default if they reset the device. It is a security problem, and should be dealt with immediately.

1. Go to Resources. Right-click in the ProScan portlet and select *New* > *Policy* (Policy Groups let you run several ProScans)
2. Name the ProScan (example: Community Not Public)
3. Under Input Source; Select *Current Config*.
4. Click *Targets* tab, and click *Add Targets*. Select your discovered Dell devices and ensure it is located under current explicit targets.
5. In the *Criteria* tab, click *Add Criteria*.
6. For the Criteria Match Type, select *does not contain.* Notice this can also be Regular Expressions (Regex), Perl or Java Groovy too.
7. Enter snmp-server community public as the *does not contain* term.
8. Click *Apply,* then *Save*.
9. Right-click your ProScan and select *Execute Compliance* (note the possibility to schedule this too). Scheduling this regularly once you have the policies you need is best practice.
10. Click the plus sign in the upper right corner of the ProScan portlet to expand it.
11. Select the policy you just configured, and you can see a pie chart labeled *Compliance Policy Chart* in the lower right corner that gives you an overview of your network’s compliance. The *Compliance Policy Summary* in the middle of the lowest screen shows compliance device by device.

Troubleshooting

The following section discusses both brief and more extension trouble shooting tips.

Upgrade Installation Halts

The installer now prevents installation as user root (Linux) or administrator (Windows). This may halt an upgrade installation on Windows if you installed the previous version as administrator.

To work around this difficulty, create a new user in the administrator group. Then navigate to the target installation directory and change ownership of all directories, subdirectories, and files to the new user. Right click the directory and select Properties > Security > Advanced > Owner tab. Then add the new user as an owner. Make sure to check the check box for “Replace owner for sub-containers and objects.” After applying the changes, login as the new administrator user and proceed with the upgrade.

Mini Troubleshooting

Suggested mini-troubleshooting steps for a balky application that is already installed and running:

1. Refresh the browser. If that doesn’t work...
2. Clear the browser’s cache (Firefox in particular loves persistent old pages), then refresh. If that doesn’t work...
3. Stop and start the browser.
4. Delete the contents of the oware/temp directory.
5. Stop and start the web server

   For Windows, to start the web server manager: oware\synergy\tomcat-X.X.X\bin\startsynergy. For Linux.

   /etc/init.d/synergy start or /etc/init.d/synergy stop

   Worth noting: The tray icon for the web server (▶) is “optimistic” about both when the web server has completely started and completely stopped. You cannot re-start web server when its Tomcat process still lingers. If you lack patience, kill the (large) Tomcat process then re-start web server. The smaller one is that tray icon.
6. Stop and start application server. Command lines for this:

   startappserver or stopappserver

   If that doesn’t work...
7. Reboot the host and re-start the application server, web server and browser.

When troubleshooting (or contacting technical support), you may find pertinent information in logs located in the following directories:

..\oware\jboss-3.0.8\server\oware\log

..\oware\temp\soniqmq.log

..\app_setup.log

```
..\db_setup.log
```

You can also run getlogs from a command line.

> ***NOTE: If you see errors that say your Linux system has too few threads, make sure you have set the file handles correctly.***

Troubleshooting Flow

As part of the troubleshooting process, you can often determine the culprit for problems by a process of elimination. The following questions may help determine what is the real issue:

Discovery/Resync

The following are bullet points. For a little more detail, see *Preventing* D and *Discovery Issues*

.

- Can you ping the device?
- Is your Cruz system permitted access to the device (on the Access Control List)?
- Is SNMP correctly set up? (check with Cruz's Network Tools and MIB browser or a tool like iReasoning's MIB browser)
- Check Telnet with a shell or an application like puTTY. See *Telnet*

> ***NOTE: Some devices support SSHv2 access only, not SSH.***

- Are firewalls blocking access to the device(s)?

Backup/Restore/Deploy

- Is your FTP server installed, up and running?
- Do FTP and TFTP servers write to the same directory, and have permissions to read/write/execute to that directory?
- Is that FTP server on the same side of the firewall as the devices it addresses?
- Do your authentications grant privileged access? The prompt is typically #, not > at this level of access.

Alarms/Monitors/Performance

Consult the *Cruz User Guide*'s recommendations, particularly for Monitoring and for Traffic Flow Analysis.

- Do you have the recommended hardware to handle the number of devices you are managing?
- Is your database configured correctly for the expected load? (Consult the *Cruz User Guide* for tips about configuring MySQL, and its my.cnf file.)
- Have you tailored your monitoring to the available capacity of your hardware?
- Are the devices you are monitoring sending only the relevant traps to Cruz?

Services

- If you cannot discover services, is the FTP server functioning correctly?

Hardware

- Does your hardware match the system recommendations for the number of devices managed, monitoring and concurrent users as described in *Best* ?
- Have you followed the installation recommendations (particularly important for Linux) in the *Cruz User Guide* and *Installation Guide*?

Advanced Troubleshooting

- Contact technical support (When you contact them, create a logs.jar file with the *getlogs* command, so you can forward it to them.)
- Refer to the *Cruz User Guide* and/or Troubleshooting document

Preventing Discovery Problems

Ensure your firewall is not blocking network access to equipment you are trying to discover. The following describes more preventive practices to do when you discover a mixed vendor/mixed class network.

Telnet

1. Manually telnet to a device to verify that you have the correct authentication information (although Discovery Profiles' *Inspect* function does this too).

   NOTE: Later versions of Windows do not include telnet by default. In addition to free telnet programs you can download and install, like PuTTY, you can open a shell (Start > Run cmd) and type oware to get telnet capabilities.

2. If you know the device, look at its configuration file and verify that the SNMP community string is correct.
3. Discover the device.
4. If there are any problems with any devices, then ping them, and/or telnet to problem devices and verify that telnet works/authentication is good.
5. If SNMP problems arise, use this application's MIB browser tool to troubleshoot them.

To verify SNMP and WMI connections are working between Cruz and the devices in the network, use the following tools:

SNMP

1. Open MIB Browser in the web client's Network Tools portlet, or by right-clicking the device.
2. Select RFC1213, system, from the RFC Standard Mibs branch
3. If necessary, fill out the Authentication tab
4. Select the device tab and information appears as soon as the device answers the query.

WMI

If you are discovering WMI systems on your network, the following may be helpful.

1. Launch the wmiutil.exe command line tool from \owareapps\wmi\bin\

2. You need to supply a user and a password along with an IP or hostname

   Typing *wmiutil.exe* with no arguments returns launch the WMIUtil User Interface.

   ```
   c:\Dorado\owareapps\wmi\bin\wmiutil.exe -user <user> -password <password> -host <IP or Hostname>
   ```

   Typing '*wmiutil.exe ?'* on the command line returns what parameters are available for the command line version.

   NOTE: Even if you do not need a domain to log into your WMI device, the graphic interface for this utility does not work if the domain field is blank. Any content makes it work correctly.

Discovery Issues

Discovery may fail if its parameters do not match the configuration of devices discovered. Here, the results panel typically displays a message like No Devices were detected with selected Discovery Parameters. Use the *Inspect* function in Discovery Profiles to validate credentials entered. Some potential sources of Discovery issues, and their solution:

- Equipment with management IP Addresses in the selected subnet, range, and so on does not exist. Correct the selected range and retry.
- The equipment in the selected range has already been discovered.

  Managed devices can only be discovered once. Those devices that have already been discovered appear in the Discovery Results section of the Discovery Wizard. Update the state of previously discovered devices by selecting *Resync* from the right-click menu. If you want to re-discover these devices, delete them from the Managed Resources portlet
- The SNMP community strings/authentication on the equipment do not match the default values used by this application. Correct the SNMP authentication selected for discovery.

HTTP Authentication

Often, an HTTP session with devices that support it exchanges data with the device after discovery. This process fails if the HTTP Authentication information is incorrect. Create HTTP authentications that match your devices' in the Authentications portlet and use it in discovery.

Device O/S Overrides

The device driver installed must support the Operation System version on that device. Verify the equipment's firmware and operating systems are among those supported. Supported firmware and operating systems appear listed in the release notes, or in *Manage > Show Versions*.

Example: Override driver-unsupported operating systems for the Juniper devices in /owareapps/juniper/lib/juniper.properties. Change com.dorado.juniper.supported.OS.dc.default.max

This revision does not support new features. Other device drivers have similar override mechanisms.

If devices appear in Managed Resources as Discovered Entities, rather than specific vendors' devices. This can mean the following:

- The equipment's driver is not installed.
- The driver installed but not seeded to database. Workaround: Run ocpinstall -s on a command line.
- Monitored devices must be configured to connect and send SNMP traps to the element management system. Make sure this is configured correctly.

If Cruz discovers only top-level equipment, this can mean the following:

- Devices do not have components (interfaces, ports, and so on).
- An incorrect telnet/SSH authentication can have an incorrect password or no enable password. **Workaround:** You can right-click and edit the equipment with this problem to add the telnet/SSH authentication. Make sure you also add a management interface, then resync the device.