

Collection Station – Environment Requirements

Intel, Western Blue and Entisys have undertaken a project to gather server information on behalf of the State of California Department of Technology Services. The following requirements are necessary to proceed with said collection activity.

This document describes the requirements for installing the discovery tool (Ecora Auditor) and configuring the network to allow the tool to accurately discover all of the servers on the network.

Other documents will describe the process for actually configuring the Ecora software itself and executing the discovery.

Step 1 – Install Ecora Software

You will receive a set of CD-ROM disks from the project team. Once you've identified the discovery server system that you want to use to run the software (see platform requirements below), insert the first CD into that server's drive and follow the prompts to install.

Platform Requirements: Hardware and OS Environment

- Windows 2000 or better
- 1 GB –RAM, 512k free recommended
- 10 GB minimum drive space free
- CDROM (minimum requirement), or DVD ROM (preferred), or External USB 2.0 or 1394 CDROM drive is acceptable. (USB 1.0 throughput is too slow to be usable.)
- Network connection: Switched 100 Base-T (minimum) – faster preferred
- Two static IP addresses assigned (one for the server, one for the Ecora virtual machine).
- USB 1.1 Port (USB 2.0 preferred)
- Dual-Core CPU (> 2 GHz) preferred, can run on single-core CPU. AMD Turion processors are not supported.

This server needs to be able to access the public Internet (software module downloads may be necessary). In addition, the software activation process involves extracting key-files that are attached to an e-mail and placing them on the Ecora server.

The server on which the Ecora software is installed needs to be capable of accessing the installer's e-mail account and storing any attachments found there on the local system. Options for doing this include Web-based access to the installer's e-mail account, installation of the native e-mail client, USB thumb-drives for transferring the attachments between systems, etc.. The specific choice of mechanisms is left to the installer.

Note: slower collection hardware and network connections will increase collection times.

Step 2 – Configure the Infrastructure

In order for the Ecora tool to accurately discover the hardware and software configuration of your servers, certain infrastructure elements must have the settings described below, for each of the asset types being discovered. Ecora is capable of discovering substantially more information than this list implies – but these are the only configuration items (CI's) that this project requires.

Supporting Infrastructure

- The host system on which you install the Ecora software must have two available IP addresses. One is required for the physical server (probably already assigned), the other is required for the virtual machine running the collection software environment. You should have these two addresses available to you when you install the Ecora software.
- Available DNS – the Ecora software should be able to reach the DNS server using its assigned IP address.
- Optional: Remote access for consulting personnel to console and work environment. The default approach will be for the consultants to provide phone-based remote assistance to on-site in-house personnel who will actually perform the necessary software configuration steps with assistance from Entisys.
- Outbound internet connection - Needed in the event of a need to download and install patches or other supporting software.

Collection Port Access

Bi-directional port access will be required as follows:

Service	Port
Windows Management Instrumentation (WMI)	445
Remote Procedure Call (RPC)	135
SNMP Agent	161
Linux/Unix Telnet	23
SSH (preferred mode of monitoring)	22
Mail Server SMTP Server	(Default: 25)
Web Server	(Default: 80)
Service Monitoring of HTTP	(Default: 9090)
SNMP HTTP Port of SNMP	(Default: 161)
DNS	(Default: 53)

Please note, if the above values have been modified from the above default values, they should be recorded and provided to the project team to ensure that an accurate inventory can be gathered.

Collection Station – Module Requirements

- Active Directory - In order to do an Active Directory scan, the collection station needs to be a member of the domain.
- Cisco – No additional requirements needed.
- Citrix – In order to do a Citrix scan, the collection station needs to be a member of the domain, and the user account needs Citrix admin rights.

Server Study Project

- MS Exchange – In order to do an Exchange scan, the collection station needs to be a member of the domain, and the user account needs Exchange admin rights.
- Novell Netware – Novell Netware client (if detailed Novell environment information is to be collected). The correct client must be made available before the Ecora module can be installed. Then, Server Consolidation Team must be able to contact the collection station via the internet to license the module.
- Unix/Linux - No additional requirements needed.
- MS Windows - No additional requirements needed.
- VMware – VmCOM Scripting API. (VMWare VI-3 is not yet supported)

Note: IIS, MS-SQL and Oracle detailed discovery modules will not be used. It is sufficient for the project's purpose to discover the physical attributes of these servers. Detailed information regarding how the software is configured isn't relevant to this phase of the project. So these discovery types are omitted from this document.

Target Machine - Collection Environment

Active Directory – Required

- Active Directory 2000, 2003
- Remote Registry Service enabled
- RPC Service
- Server Service enabled
- NetBIOS (over TCP/IP) protocol support or AD
- Domain Administrator rights for domains containing reported systems

Cisco - Optional

- Cisco IOS version 11.x or higher
- RPC Service
- Routers & Layer 3 Switching Devices/Modules (RSM, RSFC, MSFC) running Cisco IOS version 11.x or higher
- Access to Privileged EXEC Mode or a security level with access to the following commands: show version, show running-config, and show startup-config on all devices to be documented

Citrix – Optional (Desirable if Citrix is used)

- Citrix MetaFrame XP SP2 or higher
- Remote Registry Service enabled
- RPC Service
- Server Service enabled
- View-only administrator rights

MS Exchange – Required if Exchange servers exist in the environment)

- Exchange 5.5, Exchange 2000, Exchange 2003
- Remote Registry Service enabled
- RPC Service

Server Study Project

- Server Service enabled
- NetBIOS (over TCP/IP) protocol support

Novell NetWare – Required only if Netware in use at site

- Console Operator access
- Supervisor rights to the portion of the NDS tree to report
- RPC Service
- Server Service enabled

Unix/Linux (Required only if UNIX or Linux systems are in use at site)

- Solaris (2.5.1-9), HPUX (10.20, 11, 11i), Linux (7.0 or higher), AIX (4.3 or higher), Red Hat Enterprise Linux 2.1, 3.0, 4.0 (AS/EW/WS)
 - Shell-level access to each target system using a standard user account
 - The user account startup must be non-interactive. No user input required to get to a standard shell command line
 - When the user account on the target system is a member of group 'sys' more configuration data can be reported
 - When the 'root' password is provided, the user account is used to make the initial connection and a /bin/su command is issued to become root. If root password is not provided only the data available to the user account can be reported, which is frequently somewhat limited.
 - Each target system must support SSH (preferred) or telnet communications

MS Windows (Required)

- NT 4.0 SP4 or higher, Windows 2000, XP, 2003
- Remote Registry Service enabled
- RPC Service
- Server Service enabled
- NetBIOS (over TCP/IP) protocol support or Active Directory (AD)
- To collect and report Domain AND System level information completely in one report
- Client for Microsoft Networks
- RPC Service
 - Domain (or Enterprise) Administrator rights for all the domains containing systems to be documented

Note: To report on machines in Workgroups, an administrator account is required on all machines to be reported that MATCHES the login/password of the domain admin account of the domain on which machine where the software is installed.

VMware (Required only when VMWare ESX or GSX used at site)

- Remote Registry Service enabled (VMware GSX Server for Windows)
- VMware VmCOM Scripting API
- VMware VI-3 is not currently supported
 - Manual investigation is required for any such VMWare hosts identified.