

EMC Smarts Application Discovery Manager Data Security

Abstract: As EMC Smarts Application Discovery Manager is deployed, a common question is what data is collected and how secure the data is. This white paper describes what data is collected and stored in the Application Discovery Manager configuration management database (CMDB), as well as covers the security model employed to encrypt and store the information.

Copyright © 2007 EMC Corporation. All rights reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS IS.” EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

Sample Trademark page below.

EMC², EMC, ApplicationXtender, Celerra, CentraStar, CLARAlert, CLARiiON, Connectrix, Dantz, Direct Matrix Architecture, DiskXtender, Documentum, EmailXtender, EmailXtract, HighRoad, Legato, Navisphere, PowerPath, RepliStor, ResourcePak, Retrospect, Smarts, SnapView/IP, SRDF, Symmetrix, TimeFinder, VisualSAN, and where information lives are registered trademarks and EMC ControlCenter, EMC Developers Program, EMC OnCourse, EMC Proven, EMC Snap, EMC Storage Administrator, Access Logix, ArchiveXtender, Automated Resource Manager, AutoSwap, AVALONidm, C-Clip, Celerra Replicator, Centera, CLARevent, CopyCross, CopyPoint, DatabaseXtender, Direct Matrix, DiskXtender 2000, EDM, E-Lab, EmailXaminer, Engenuity, eRoom, FarPoint, FLARE, FullTime, InfoMover, MirrorView, NetWin, NetWorker, OnAlert, OpenScale, Powerlink, RepliCare, SafeLine, SAN Advisor, SAN Copy, SAN Manager, SDMS, SnapSure, SnapView, StorageScope, SupportMate, SymmAPI, SymmEnabler, Symmetrix DMX, and VisualSRM are trademarks of EMC Corporation.

All other brand names are trademarks or registered trademarks of their respective owners.

Part Number: S0076

Table of Contents

Overview	4
Application Discovery Manager Discovery Technologies	4
Passive Discovery	4
Detail Discovery.....	4
Information Collected	4
Information Not Stored	4
Application Discovery Manager Data Encryption.....	5
Application Discovery Manager Console Credentials	5
Active Discovery Policies Credentials	5
Graphical User Interface Encryption	5
Appliances Inter-Communication	5
Appliance Hardening	5
Summary	6
About EMC Smarts.....	6

Overview

As EMC Smarts Application Discovery Manager is deployed, a common question is what data is collected and how secure the data is. This white paper describes what data is collected and stored in the Application Discovery Manager configuration management database (CMDB), as well as covers the security model employed to encrypt and store the information.

Application Discovery Manager Discovery Technologies

Application Discovery Manager is the de facto standard in application discovery and dependency mapping. Application Discovery Manager uses a hybrid passive and active approach to perform a complete, end-to-end discovery of the application environment including network resources, servers, services, and business applications. As part of the discovery process, Application Discovery Manager also builds out a complete relationship and dependency model, as well as usage and demand models for the application environment.

Passive Discovery

Passive Discovery (PD) works by performing deep packet analysis of network packets that are collected through monitoring ports of switches. Since PD works without spidering, crawling or probing the network in any way, no load is placed on the network when performing PD. In fact, PD is completely passive in nature, as the name implies.

Detail Discovery

Detail Discovery (DD) works by using credentials to remotely connect to servers using a combination of SNMP, SSH, Telnet, or WMI protocols. Once connected, Application Discovery Manager runs commands on the remote servers to extract information required to populate the Application Discovery Manager CMDB.

Information Collected

Application Discovery Manager collects information and stores information about five types of entities:

- *Hosts*—For hosts, Application Discovery Manager collects information including hostnames, IP addresses, detailed hardware configuration information, operating system information and patches, and installed software and versions.
- *Services*—For services, Application Discovery Manager collects information, including install locations, configurations, and documented dependencies.
- *Dependencies*— For both hosts and services, Application Discovery Manager stores dependency information at the host-to-host level, as well as the service-to-service level. In each case, the information is determined by packet inspection, as well as examining configuration files using Detail Discovery as described above.
- *Usage and demand*— Since Application Discovery Manager is continuously examining network packets, it builds a usage and demand model that describes which hosts and applications are used by which other hosts and applications, as well as the number of transactions for each conversation.
- *Table and URLs accessed*— Application Discovery Manager also parses the payloads of some protocol packets to extract the URLs and the tables accessed in each of the conversations. This information is stored in relation to specific connections made between hosts and services.

Information Not Stored

Although Application Discovery Manager may be potentially exposed to sensitive information during the course of examining packets, none of the information is parsed or stored in any way. Application Discovery Manager fingerprints are designed to look for very specific data within a packet. For example, even though we may be exposed to credential information available when a client connects to another, this information is NOT parsed, captured, or stored in any way.

Specifically, the following information is not captured or stored:

- Usernames and passwords
- Transaction details
- Packets examined
 - Credit card information
 - Personally identifiable information
 - Other sensitive data visible in packets

Application Discovery Manager Data Encryption

Since Application Discovery Manager provides a role-based authentication model to access the information stored in the discovery CMDB, and also requires credentials for the Detail Discovery capabilities, this information is securely stored in the CMDB as follows:

Application Discovery Manager Console Credentials

The Application Discovery Manager console usernames and passwords are hashed using MD5. MD5 (Message-Digest algorithm 5) is a hash function using a 128 bit hash value to encrypt data. By nature, hashing algorithms are not reversible – you cannot “decrypt” the hash value and get the clear text password. Instead, when a password is used during the login process, it is padded and hashed using the MD5 algorithm and compared to the hashed value stored in the database. While the specific hashing algorithm varies from system to system, hashing is the standard method for storing login credentials.

Active Discovery Policies Credentials

For Active Discovery, Application Discovery Manager must be able to use the clear-text password with the server being discovered. Therefore, a hashing algorithm is not applicable here. Application Discovery Manager stores Active Discovery policies passwords encrypted using 56 bit key DES (Data Encryption Standard) in CBC mode with PKCS5 padding. Once required to perform discovery, the password is temporarily decrypted and used with the specified discovery protocol. The discovery protocol typically uses authentication and encryption to ensure password is not transferred in clear over the network. For example, Telnet may be using NTLM and SSH may use a wide set of authentication and encryption algorithms.

Graphical User Interface Encryption

Application Discovery Manager is used via a web based user interface. The user interface may be accessed either via an HTTP connection that does not use encryption, or via an HTTPS connection that utilizes SSL to encrypt all underlying communication. In case of HTTPS, sensitive information such as console’s credentials or Active Discovery Policies configuration is transferred in a secure, encrypted channel where the security level is matched to the browser’s ability.

Appliances Inter-Communication

When multiple Application Discovery Manager appliances are deployed, the appliances must communicate to transfer discovered information and discovery policies. The communication channel between the appliances is a secure and encrypted HTTPS channel.

Appliance Hardening

As described above, Application Discovery Manager stores and communicates sensitive information securely. The appliance’s operating system has also been hardened to block any attempts to hack into the appliance’s operating system. Redundant services has been disabled, latest up-to-date security patches are regularly deployed and distributed via product updates and an internal firewall is used to deny any access to non-required port. The product also regularly goes through a vulnerability scan using standard tools such as Nessus.

Summary

Application Discovery Manager, while potentially having access to sensitive information because of direct access to network packets, does *not* capture or store any of this information. In addition, where sensitive credential information is provided by users, this information is stored in the CMDB using strong encryption technologies to prevent unauthorized access to this information.

About EMC Smarts

EMC Smarts plays a crucial role in managing your information infrastructure by automating the discovery, understanding, and mapping of the complex relationships that exist among business processes, applications, and the IT infrastructure.

With EMC Smarts solutions, organizations gain the visibility needed to accelerate and increase ROI on their highest-priority IT service and cost management initiatives. Offering the easiest, most-comprehensive solution in the industry, EMC Smarts technology allows organizations to:

- Accelerate ITIL and CMDB standardization
- Reduce costs—up to 25 percent in the first year
- Maximize resource utilization
- Mitigate risks and ensure business continuity
- Enhance business agility and IT service delivery by accelerating and simplifying initiatives that support business service management and data center automation

Getting Started

To learn more about how the EMC Smarts Solution for Data Center Audits—and other EMC Smarts solutions—can positively impact your business and IT operations, contact your local EMC or EMC Smarts sales representative, or visit our websites at www.EMC.com and www.smarts.com.