

BMC Atrium Discovery and Dependency Mapping Explained

TABLE OF CONTENTS

INTRODUCTION 1

WEBLOGIC DISCOVERY 2

WEBSHERE DISCOVERY 4

SAP ENTERPRISE APPLICATIONS DISCOVERY 6

DATABASE DISCOVERY 11

DNS SERVER AND WEB SERVER DISCOVERY 14

WEB SERVICES DISCOVERY 15

EXCHANGE MESSAGING SYSTEMS DISCOVERY 16

VIRTUAL SYSTEMS DISCOVERY 17

UNIVERSAL APPLICATION DISCOVERY 22

NETWORK DISCOVERY 25

INTRODUCTION

ABOUT DISCOVERY

IT organizations need to identify assets and how they are configured. Today's number of IT components, their configurations, relationships among them, and the constant changes introduced by business and technology needs make manual tracking difficult. It is impractical and costly to conduct manual audits and maintain IT service relationship and application dependency mapping information.

Discovery automates the process of gathering required information and populating and maintaining a CMDB. This is done by discovering IT hardware and software and creating instances of configuration items and relationships from the discovered data. A configuration item can be physical (such as a computer system), logical (such as an installed instance of a software program), or conceptual (such as a business service).

BMC ADDM discovers network devices, enterprise applications, and business processes. BMC ADDM automatically generates impact relationships for use in BMC Service Impact Manager Service models.

DISCOVERY TASKS

Discovery uses various technologies and methods to access and query computers and network devices. Discovery tasks define what to discover, the systems to explore for data collection, the technology to use for exploring the systems, and the credentials to use to access the systems.

DISCOVERY SYNCHRONIZATION WITH BMC ATRIUM CMDB

The discovered configuration items and relationships are stored in the discovery data store. From the discovery data store, you can export the configuration items and relationships to BMC Atrium CMDB for reconciliation with the production dataset. Once the configuration data has been reconciled with other CMDB data sources, it can be used by consumers of the CMDB, such as the BMC Remedy IT Service Management Suite of products.

WEBLOGIC DISCOVERY

WHAT IS WEBLOGIC

BEA Systems' WebLogic is an application server that runs on a middle tier, between thin clients and back-end databases. An application server is a server that is designed for, or dedicated to, running specific applications. It provides the business logic for a Web application.

WebLogic server is based on Java 2 Platform, Enterprise Edition (J2EE), the standard platform used to create Java-based, multi-tier enterprise applications.

WebLogic, which was developed by BEA Systems (later acquired by Oracle), is a leading e-commerce online transaction processing platform. The main features of WebLogic server include connectors that make it possible for any legacy application on any client to interoperate with server applications, Enterprise JavaBean components, resource pooling, and connection sharing. This allows building distributed, scalable, and secure applications.

HOW WEBLOGIC DISCOVERY IS DONE

COMMUNICATION

BMC ADDM uses HTTP (Hypertext Transfer Protocol) as a transport for communication with WebLogic servers. HTTP is a standard Internet protocol, which is simple, fast, lightweight, and supported by almost all environments. Typically most companies allow HTTP requests through a firewall. Thus, no additional firewall tuning is required to enable WebLogic discovery and there is no need to compromise firewall settings.

However, HTTP was designed to display data (Web pages), with a focus on how data looks and was not designed for application communication. BMC ADDM uses Simple Object Access Protocol (SOAP) over HTTP to combine advantages of HTTP and SOAP's ability to communicate with applications.

- DEFINITIONS**
- » **SOAP** (Simple Object Access Protocol) is a protocol that allows applications to communicate using HTTP and XML messages. SOAP specifies exactly how to encode an HTTP header and an XML file so that an application in one computer can call an application in another computer and pass it information. It also specifies how the called program can return a response.
 - » **XML** (Extensible Markup Language) is a markup language similar to HTML which is designed to carry data, not to display data.

SOAP is language- and platform-independent, simple and extensible protocol. Since SOAP is used over HTTP, SOAP requests are usually allowed through firewalls.

To provide open and extensible management services, BEA Systems' WebLogic implements the Sun Microsystems, Inc. Java Management Extensions (JMX) specification.

- DEFINITION**
- » **JMX** (Java Management Extensions) is a set of specifications for managing and monitoring applications and services. It defines a management architecture, design patterns, APIs, and services for building Web-based, distributed, dynamic, and modular solutions to manage Java-enabled resources.

The Java Management Extensions specification is native to the Java programming language and offers efficient, lightweight management extensions to Java technology-based functions. All WebLogic Server resources, third-party services, and applications that run within WebLogic Server can be managed through JMX-based services

JMX is the only data source for WebLogic discovery. JMX provides management information for Java technology-based resources, such as a business application, a device, or the software implementation of a service or policy. BMC ADDM uses JMX technology over SOAP for WebLogic discovery.

SECURITY

If WebLogic server is configured for security, BMC ADDM automatically uses SSL (Secure Sockets Layer) technology with no configuration of the discovery. The SSL protocol supports a variety of cryptographic algorithms. BMC ADDM uses Triple-DES encryption – the strongest cipher supported by SSL.

- DEFINITIONS**
- » **SSL** (Secure Sockets Layer) is a standard security technology for establishing an encrypted connection between a server and a client. This connection ensures that all data passed between the server and the client remains private and integral. By default, secure connections start with "https" instead of "http" in Web browsers. SSL is an industry standard and is used by millions of Web sites in the protection of their online transactions with their customers.
 - » **3DES** Also called Triple DES or EDE (encrypt, decrypt, encrypt), a secret key encryption algorithm based on repeated application of the Data Encryption Standard (DES). 3DES works by applying the DES algorithm three times in succession to 64-bit blocks of plaintext. It does this by using two independent 56-bit keys. Because the key size is so large, there are more possible keys than for any other cipher – approximately 3.7×10^{50} .

This cipher suite is appropriate for banks and other institutions that handle highly sensitive data.

AUTHENTICATION

Depending on the WebLogic server configuration, BMC ADDM uses RSA or DSS authentication.

- DEFINITIONS**
- » **RSA** (Rivest-Shamir-Adleman) is a widely used public key cryptography algorithm, which is named after its originators: Ronald Rivest, Adi Shamir, and Leonard Adleman. RSA is the most popular public key encryption algorithm in use today. RSA can be used for encryption and decryption of information and for the generation and verification of digital signatures.
 - » **DSS** (Digital Signature Standard) is the digital signature algorithm (DSA) developed by the U.S. National Security Agency (NSA) to generate a digital signature for the authentication of electronic documents.

DISCOVERY DETAILS

There is a WebLogic Administrator interface on port 7001 that allows for administration of WebLogic configuration and is accessed at `http://hostname:7001/wladmin`

If you have configured a domainwide administration port, use that port number. If you configured the administration server to use Secure Socket Layer (SSL) you must add "s" after http as follows:

`https://hostname:7002/console`

To access administrative functionality within WebLogic, a user account with administrative privileges must be used. The default username and password are admin/admin.

THE OUTCOME

BMC ADDM discovers WebLogic Domains, Applications, Application Servers, Clusters, Computer Systems that host Weblogic servers, Web Servers that forwards requests to a Weblogic server; Database Server and Database referenced by JDBC resource, Mail Server referenced by JavaMail resource, Application cluster and associated relationships.

WEBSPHERE DISCOVERY

WHAT IS WEBSPHERE

IBM WebSphere Application Server is an application server that runs on a middle tier, between thin clients and back-end databases. An application server is a server that is designed for or dedicated to running specific applications. It provides the business logic for a Web application.

WebSphere server is based on Java 2 Platform, Enterprise Edition (J2EE), the standard platform used to create Java-based, multi-tier enterprise applications.

HOW WEBSPHERE DISCOVERY IS DONE

COMMUNICATION

In 1997 IBM and Sun Microsystems launched a joint initiative to promote Java as an enterprise-development technology. What they lacked was a mature remote transport technology. The initiative resulted in creation of RMI-IIOP (Java Remote Method Invocation over Common Object Request Broker Architecture)

DEFINITIONS

- » **Java RMI** is a set of APIs (Applications Programming Interfaces) and a model for remote objects that allows developers to build distributed applications very easily in Java using the same programming model as for local Java applications.
- » **IIOP** is a message protocol that makes it possible for distributed programs written in different programming languages to communicate with each other. IIOP is used on a TCP/IP network (Internet, intranet, etc.). IIOP is a critical part of a strategic industry standard, the Common Object Request Broker Architecture (CORBA)
- » **CORBA**, is a language-independent industry standard specified by the Object Management Group. CORBA allows communication between software written in any programming language running on any operating system on any hardware architecture. Using CORBA's IIOP and related protocols, a company can write programs that will be able to communicate with their own or other company's existing or future programs wherever they are located and without having to understand anything about the program other than its service and a name.

Java RMI over IIOP combines the best features of Java RMI technology with the best features of CORBA technology. BMC ADDM uses Java RMI technology run over Internet IIOP for Web sphere discovery.

To provide open and extensible management services, WebSphere implements the Sun Microsystems, Inc. Java Management Extensions (JMX) specification.

DEFINITION

- » **JMX** (Java Management Extensions) is a set of specifications for managing and monitoring applications and services. It defines a management architecture, design patterns, APIs, and services for building Web-based, distributed, dynamic, and modular solutions to manage Java-enabled resources.

JMX is native to the Java programming language and offers efficient, lightweight management extensions to Java technology-based functions.

JMX is the only data source for WebSphere discovery. JMX provides management information for Java technology-based resources, such as a business application, a device, or the software implementation of a service or policy. BMC ADDM uses JMX technology for WebSphere discovery.

SECURITY

If WebSphere server is configured for security, BMC ADDM automatically uses SSL (Secure Sockets Layer) technology with no configuration of the discovery.

DEFINITION

- » **SSL** (Secure Sockets Layer) is a standard security technology for establishing an encrypted connection between a server and a client. This connection ensures that all data passed between the server and the client remains private and integral. By default, secure connections start with “https” instead of “http” in Web browsers. SSL is an industry standard and is used by millions of Web sites in the protection of their online transactions with their customers.

DISCOVERY DETAILS

IBM WebSphere discovery requires the IBM WebSphere Application Server Client to be installed on the discovery server.

WebSphere discovery requires the SOAP JMX connector port of the WebSphere administration server. The default SOAP JMX connector port numbers are as follows:

- » Application Server: 8880
- » Deployment Manager (Network Deployment): 8879

The WebSphere administration server is server1 when the WebSphere Application Server is installed in a stand-alone configuration. In a Network Deployment cell, the deployment manager is the WebSphere administration server for all of the managed nodes in the cell. Use the WebSphere Administrative console to obtain the SOAP JMX connector port number for the WebSphere administration server.

The default username and password is “admin.” If security is not enabled on the WebSphere Application Server any value can be used for the logon ID and password.

THE OUTCOME

BMC ADDM discovers WebSphere Domains, Applications, Application Servers, Clusters and Computer Systems that host Weblogic servers, Web Servers that forwards requests to a Weblogic server; Database Server and Database referenced by JDBC resource, Mail Server referenced by JavaMail resource, Application cluster and associated relationships.

SAP ENTERPRISE APPLICATIONS DISCOVERY

WHAT IS SAP ENTERPRISE APPLICATION

SAP Enterprise Application is the part of ERP software solution based on SAP R/3 or SAP R/3 Enterprise from SAP AG.

DEFINITION » ERP (Enterprise Resource Planning) is a set of programs that integrate the data and processes of an organization into one single system, like human resources, supply chain management, customer relations management, financials, manufacturing functions and warehouse management, etc.

SAP R/3 system consists of at least one application server and a database server. The applications include materials management, sales and distribution, financial accounting, and human resources.

HOW SAP DISCOVERY IS DONE

The only way to get the full information from SAP servers is to use native SAP connection methods: SAP Remote Function Call protocol (RFC) and SAP Java Connector (Jco).

DEFINITIONS » **Remote Function Call (RFC)** is SAP's primary real-time communications protocol that allows function modules to be invoked locally or remotely. It was originally released with R/3 in the early 1990s and has since been regularly updated. Using the RFC interface, BMC ADDM can act as both the client and the server to an SAP system. The only activity that can be performed by RFC is the execution of a function module. Calling an RFC function that resides in an SAP system from BMC ADDM is similar in principle to calling an RFC function from another SAP system.

» **SAP Java Connector**, also referred to as SAP JCo, enables communication between Java applications and the SAP system. SAP provides SAP Java Connector as a standalone software component that can be installed independently of the SAP system. JCo supports both inbound (Java calls ABAP) and outbound (ABAP calls Java) calls in desktop and server applications. The SAP Java Connector (JCo) package provides an API which enables communication with SAP systems.

BMC ADDM server calls into the SAP central application server via SAP Remote Function Call protocol using SAP Java Connector. To access data on the SAP server, the client process must present authentication information (username and password) entered at a correspondent step of Discovery Wizard. If no credentials are provided, only basic SAP system infrastructure can be discovered. The call without credentials works on SAP releases that have a kernel versions 46C, 46D, and 620.

The BMC ADDM server uses a port from the port range 3300-3396 to connect to SAP central application server. The number of the port depends on the instance number which was set in Discovery Wizard. So if instance number is 56, the port which will be used is 3356.

DISCOVERY DETAILS

To run a discovery task on a SAP central application server, specify its central instance number and its client number in the discovery task. If you do not provide an instance number, the discovery task will try all instance numbers (00-96). If you do not provide a client number, the default client number 000 will be used.

To access data on the SAP central application server, specify the logon credentials for the SAP Java Connector. With no credentials, the basic SAP system infrastructure can still be discovered on SAP releases that use kernel versions 46C, 46D, and 620. Some of the advanced aspects require appropriate access rights.

THE OUTCOME

The SAP discovery task discovers the logical and physical configuration items that belong to an SAP system and the relationships among those configuration items. The configuration items and relationships are stored in the

discovery datastore. The BMC Discovery is able to classify the discovered items into the following configuration items: SAP System, SAP System Client, SAP Application, SAP Application Server, SAP Software Component, SAP Printer, SAP Services: Gateway, Background, Dialog, Enqueue, Message, Spool and Update services. For more information, refer to the "SAP configuration items" section in the "BMC Atrium Discovery and Dependency Mapping: Discovering and Managing Configuration Data" guide.

SIEBEL ENTERPRISE APPLICATIONS DISCOVERY

WHAT IS SIEBEL ENTERPRISE APPLICATIONS

Siebel Enterprise Applications is a family of e-business software that includes Customer Relationship Management (CRM), Enterprise Resource Management (ERM), and Partner Relationship Management (PRM) applications. They are designed to automate those aspects of business and allow an enterprise to perform and coordinate associated tasks over the Internet and through other channels, such as retail or call-center networks.

DEFINITION

- » **Siebel Enterprise Servers (SES)** are a logical grouping of Siebel Servers (SS) that connect to one Siebel database. SES is not a physical server, it is just a logical grouping on several Siebel Servers. In other terms, the SES is composed of one or more Siebel Servers. Siebel Servers function as application servers and are composed of server components.
- » **Siebel Server (SS)** is the system on which Siebel Server Components are installed and it functions as application server. Each server component performs a defined function. Server components or groups of components determine what applications and services a Siebel Server supports. The Siebel Server runs as a system service under Windows and a process under UNIX. This system service or process monitors and controls the state of all server components on that Siebel Server. Each Siebel Server is one instantiation of the Siebel Server system service or process within the current Siebel Enterprise Server.
- » **Siebel Webserver Extensions (SWSE)** The responsibility of this component is to identify if the request that has arrived on Webserver is a Siebel request or not, and also helps to format server HTML pages requested by Siebel Web Clients.
- » **Siebel Gateway Name Server (SGNS)** can be considered a Siebel Server contact information storehouse for all the Siebel servers. It serves as the dynamic address registry for Siebel Servers and components.
- » **Application Object Manager (AOM)** processes user requests and is application- or service-specific. For example a sales application will have sales AOM and call center application will have a call-center AOM. This Application Object Manager provides the session environment in which this application runs.
- » **Data Manager** is another component that is a part of AOM. Its primary function is to receive user requests and then create corresponding SQL and forward it to the database server. It also receives results from the database server and forwards it to Siebel Business Object Layer for additional processing.

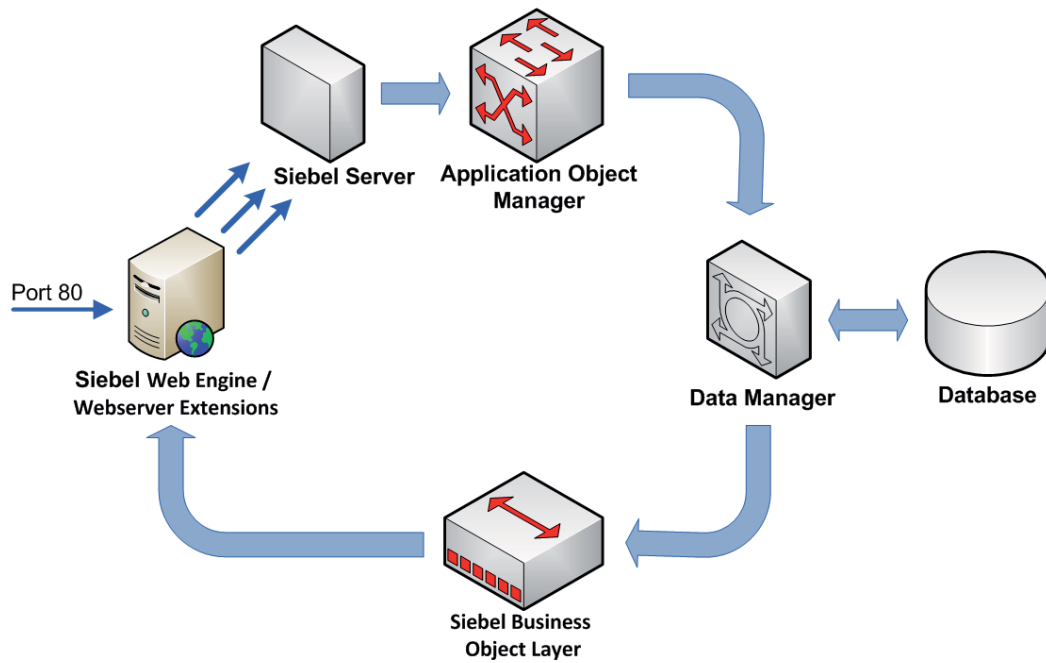
HOW SIEBEL DISCOVERY IS DONE

After running the Discovery Task, the BMC ADDM server connects to the SIEBEL Enterprise Instance using the SIEBEL Application Login Page method. The connection is made via port 80 by HTTP protocol.

The request is received by Siebel Webserver Extensions (SWSE) component. It forwards the request to the Siebel Server on round-robin basis due to its load balancing feature. Once the request is received by Siebel server, it is passed to the Application Object Manager (AOM) component.

When an AOM receives a BMC ADDM request, it starts a user session and processes any required business logic, and sends a data request to the data manager. The data manager forwards requests to the database server then receives it back and forwards it to Siebel Business Object Layer for additional processing.

Siebel Business Object Layer forwards the results to Siebel Web Engine (SWE). SWE forwards the data to the SWSE Component, which resides on the Web server. The Web server then sends back the results to the BMC ADDM server.



The following HTTP commands are used during discovery:

- » **GET** - Retrieves the document specified in the URL property
- » **HEAD** - Gets the header information
- » **POST** - Sends data to the server
- » **PUT** - Replaces the page specified in the URL property with the specified data

Of the four commands available in the Internet Transfer control for HTTP transfers, the **GET** command is the most used. This command is used to retrieve a document based on the supplied URL. The **HEAD** command is used to retrieve only the document's header information. Both commands need to use the **GetHeader** method to retrieve header information, and the **GET** command uses the **GetChunk** method to retrieve the body of the document.

The **POST** command is used to send data back to the server. This is most often used with HTML forms that need to transmit data to the server for processing. The **PUT** method is used to add a new document or file to the Web server or update an existing document. This command may not work with all Web servers, and it will most likely require information in the headers for authorization information.

DISCOVERY DETAILS

To run the discovery task against Siebel enterprise, specify the application Uniform Resource Identifier (URI) for the Siebel application that you want to log on to and the Siebel application Web server port number. The default port number is 80. For the discovery task to access the Siebel enterprise, you must provide a login account with system administrator privileges, such as **SADMIN**. The login account must have access to the Siebel Server Manager Graphic User Interface (GUI) screens and the views in the Siebel application that you want to discover.

Include the Siebel application Web server host in the discovery domain. The Siebel application URL contains the Web server host name and application URI. For example, if the URL is **http://sb77-vm1/callcenter_enu/**, add the host **sb77-vm1** to the discovery domain (or include it in the IP address range or subnet).

TIPS

- » To customize dependency relationships of Siebel applications, edit the `TD_HOME\etc\action_util\siebel\1.00\siebel_dependent.xml` file using the following guidelines:
 - **Application Name:** Specify the name of an object manager.
 - **AppDependentComponentGroup Name:** Specify the name of the component groups on which the object manager depends.

- » Firewall proxies and reverse proxies implemented in conjunction with Siebel applications are supported with HTTP 1.0 or 1.1 protocol. Special deployment considerations should be made when using proxies that support HTTP 1.0. Oracle strongly recommends using HTTP 1.1 to avoid known errors in HTTP 1.0.

THE OUTCOME

BMC ADDM can discover the components of Siebel server versions 7.7 or 7.5.2. These components are represented as configuration items (CIs) with relationships between them. BMC ADDM recognizes the following components of Siebel Enterprise Applications: Siebel Enterprise, Siebel Application, Siebel Application Server, Siebel Component and Siebel Component Group, Siebel Resource, Siebel DB Resource, Siebel File System Resource, Siebel Servers: Chart Server, Configurator Remote Server, Gateway Server, Report Server, Remote Search Server, Web eCollaboration Server and Servers: LDAP, Mail, Web servers.

DATABASE DISCOVERY

WHAT IS A DATABASE

A database is an organized collection of data. The data can be textual, like order or inventory data, or it can be pictures, programs or anything else that can be stored on a computer in binary form.

A relational database stores the data in the form of tables and columns. A table is the category of data, such as "employee," and the columns are information about the category, such as "name" or "address."

Some databases have minimal feature sets and only store data, while others include programming languages, facilities and utilities to support enterprise-level applications, such as ERP and data warehousing.

HOW DATABASE DISCOVERY IS DONE

BMC ADDM leverages the following discovery methods: LDAP, Oracle Instances from TNS Listener, and Database Scan using Nmap.

- DEFINITIONS**
- » **LDAP** (Lightweight Directory Access Protocol) is an Internet standard protocol used by applications to access information in a directory. It runs directly over TCP. LDAP was created as a way to minimize the implementation requirements on directory clients, and to simplify and encourage the use of directories among applications.
 - » **TNS** (Transparent Network Substrate) **Listener** is a process that listens for TNS connections and then routes them to the appropriate service. The TNS Listener listens for connections and then sends them in the right direction.
 - » **Nmap** (Network Mapper) is a free and open source utility for network exploration. Nmap supports dozens of scanning techniques and offers a number of advanced scan features.

LDAP DISCOVERY METHOD DETAILS

The LDAP method uses the LDAP Protocol for accessing and obtaining a list of database servers from enterprise discovery server. This method works with Microsoft SQL Server, IBM DB2 and Sybase databases.

LDAP method requires user account and password to access the port 389 on a server that hosts LDAP catalog in order to obtain a list of all database servers listed on the LDAP directory server.

The discovery uses DIGEST-MD5 authentication if required by the LDAP server. Sometimes a security policy may require to avoid passwords being sent in clear text over the wire. One common method to avoid clear text passwords is deploying Transport Layer Security (TLS) for LDAP connections.

- DEFINITIONS**
- » Digest-MD5 is authentication mechanism based on the HTTP Digest Authentication. DIGEST-MD5 is a challenge-response mechanism with which the user's password is not transmitted as plaintext. In cryptography, MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value. As an Internet standard (RFC 1321), MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files.
 - » TLS (Transport Layer Security), is a protocol for establishing a secure connection between a client and a server. TLS is capable of authenticating both the client and the server and creating an encrypted connection between the two.

To perform any LDAP operation, an LDAP client needs to establish a connection with an LDAP server. The LDAP protocol specifies the use of TCP/IP port number 389, although servers may run on other ports.

The LDAP protocol also defines a simple method for authentication. LDAP servers can be set up to restrict permissions to the application directory they host. Before an LDAP client can perform an operation on an LDAP server, the client must authenticate itself to the server by supplying a distinguished name and password. If the

user identified by the distinguished name does not have permission to perform the operation, the server does not execute the operation.

In Digest-MD5, the LDAP server sends data that includes various authentication options that it is willing to support plus a special token to the LDAP client. The client responds by sending an encrypted response that indicates the authentication options that it has selected. The response is encrypted in such a way that proves that the client knows its password. The LDAP server then decrypts and verifies the client's response.

TLS is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with 3DES encryption method. The TLS Handshake Protocol allows the server and client to authenticate with each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged.

ORACLE TNS LISTENER METHOD DETAILS

Oracle Instances from TNS Listener method uses the Oracle Transparent Network Substrate (TNS) Listener application to find and receive information from Oracle servers. This method supports Oracle 8i Database, Oracle 9i Database, and Oracle Database 10g database servers

The Oracle TNS allows clients and servers to communicate over the network using a common API, regardless of which transport protocol is being used on either end. Here's how:

1. Oracle receives a connection request with username, password and System ID (SID) or service name on a specific port.
2. Oracle checks the SID or service name and if configured to listen to that SID or service name forwards the login information to that instance.
3. Oracle authenticates login information, the listener process redirects the client to any new available port, and a session is created between the client and the server on that new port.
4. Once this flow is completed, TNS Listener starts to listen on original port leaving server process and client process to do their own work.

In its default configuration, no password is required to access the TNS Listener. If the TNS Listener has a password, it is encrypted by an Oracle specific API during the communication.

Oracle discovery requires entering the Oracle TNS Listener port number, which is 1521 by default. TNS Listener method requires unfiltered access to port 1521 of target Oracle server. The discovery also requires specifying a TNS Listener password when you want to discover an Oracle Database 10g database server or when a TNS Listener password has been set for Oracle 8i Database or Oracle 9i Database.

DATABASE SCAN METHOD DETAILS

Database Scan method uses Nmap (Network Mapper) third-party utility to scan ports of target hosts in order to determine if a physical servers hosts a database.

Nmap queries TCP/IP ports and records the target's response. Nmap gains information about the target host by determining what services are currently running, who owns those services, whether anonymous logins are supported, and whether certain network services require authentication.

Nmap can only match port numbers to services listed in its database and it can receive some "footprint" of several services, such as HTTP for example, when you connect to port 80 of Apache, you will receive "Apache 2.2 listen:DATA:808>" This will allow Nmap to report that Apache version 2.2 was found.

However this mechanism is unavailable for databases, because a response from database's port 1533, for example, is "dumb," such as "RTLS:77, 56, 445.OK." Thus Nmap cannot retrieve database instance information.

THE OUTCOME

The BMC ADDM methods allow detecting and recognizing a wide range of databases and their elements. Using just one Database Scan method a customer can discover the following database types and versions:

- » Oracle Database v.8.1.7.0, 9.2.0.4, 10g
- » IBM DB2 Universal Database v.8.1, 8.2
- » Microsoft SQL Server 2000 and 2005
- » IBM Informix Dynamic Server v.7.3, 9.4
- » Sybase Adaptive Server Enterprise (ASE) v.12.5.0
- » MySQL v.3.23.49, 4.0.11
- » PostgreSQL v.7.2.2, 8.0.1

The following CIs are being discovered during database inventory discovery task: Database, Software Server, Database Server, Database System and Computer System.

DNS SERVER AND WEB SERVER DISCOVERY

WHAT IS A DNS SERVER

Network resources are identified by numeric IP addresses, but these IP addresses are difficult to remember. For example, on the Web, it's much easier to remember the name `www.amazon.com` than it is to remember its corresponding IP address `207.171.166.48`. The DNS (Domain Name System) database contains records that map user-friendly alphanumeric names for network resources to the IP address used by those resources for communication. In this way, DNS acts as a mnemonic device, making network resources easier to remember for network users. It allows your computer to register and resolve domain names.

Each organization that maintains a computer network has at least one server handling DNS queries. That server, called a DNS server, will hold a list of all the IP addresses within its network, plus a cache of IP addresses for recently accessed computers outside the network. Each computer on each network needs to know the location of only one DNS server.

WHAT IS A WEB SERVER

A Web server is a program that, using the client/server model and the World Wide Web's Hypertext Transfer Protocol (HTTP), serves the files that form Web pages to Web users (whose computers contain HTTP clients that forward their requests). Every computer on the Internet that contains a Web site must have a Web server program. Two leading Web servers are Apache, the most widely-installed Web server, and Microsoft's Internet Information Server (IIS).

Web servers often come as part of a larger package of Internet- and intranet-related programs for serving e-mail, downloading requests for File Transfer Protocol (FTP) files, and building and publishing Web pages.

HOW DNS SERVER DISCOVERY IS DONE

The discovery uses the **DNS Scan** method. DNS Scan relies on the Nmap utility.

DEFINITION » **Nmap** (Network Mapper) is a free and open source utility for network exploration. Nmap supports dozens of scanning techniques and offers a number of advanced scan features.

The DNS Server inventory discovery type uses the DNS Scan method to access a host computer and determine if a DNS server is present. No credentials are required to access the server host and perform the scan.

HOW WEB SERVER DISCOVERY IS DONE

The discovery uses the HTTP protocol, with no encryption. BMC ADDM simply tries to connect to ports you have specified on a machine using HTTP and determines if a Web server is present. No credentials are required to access the server host and perform the scan.

DISCOVERY DETAILS

DNS Scan method requires at least one port number where the DNS servers on your network can be accessed. The default DNS port number is 53.

Web Server discovery requires the HTTP port number of the Web servers that you want to discover. You must provide at least one Web server port. The default port is 80; other common HTTP ports are 8080 and 8001.

THE OUTCOME

BMC ADDM can discover DNS Servers, Web Servers and their IPs as well as their relationship with other CIs.

WEB SERVICES DISCOVERY

WHAT IS WEB SERVICE

Web services are application components that communicate using open protocols such as HTTP. Usually web services are self-contained and self-describing. Having XML protocol as a basis they consist from the following elements: SOAP (Simple Object Access Protocol), UDDI (Universal Description, Discovery and Integration) and WSDL (Web Services Description Language).

- DEFINITIONS**
- » **SOAP** (Simple Object Access Protocol) is a protocol that allows applications to communicate using HTTP and XML messages. SOAP specifies exactly how to encode an HTTP header and an XML file so that an application in one computer can call an application in another computer and pass it information. It also specifies how the called program can return a response.
 - » **WSDL** (Web Services Description Language) is a XML-based language, that primary used for locating and describing Web Services.
 - » **UDDI** (Universal Description, Discovery and Integration) is a directory service where companies can register and search for Web services. UDDI communicates with over directories and hosts via SOAP.

HOW WEB SERVICES DISCOVERY IS DONE

The web services discovery uses two methods to discover web services: **WSDL URL** method and **UDDI Server** method.

Using **WSDL URL** method ADDM connects to a server which hosts web services and reads a content of the WSDL file that provides a detailed description of each web service and what operation it can perform.

UDDI Server method allows discovering web services by using a connection to the UDDI server. In most cases a user does not need to provide credentials to access the UDDI service.

One can benefit using both WSDL URL and UDDI Server methods together because UDDI uses WSDL to describe interfaces to web services. It allows obtaining most complete information about web services.

DISCOVERY DETAILS

WSDL URL method requires a correct URL to the WSDL file. This file resides on a server which hosts web services, for example: `http://localhost/wsdl?config.file`

WSDL files consist of several main sections. By reading them ADDM can create CIs related to servers that host web services and their relationships.

The UDDI Server method is also the simple way to obtain comprehensive information about web services. In this case ADDM connects to the UDDI directory service. A user can specify the entity type (business entity, web or business service) to refine the list of web services discovered on UDDI server. The discover server polls the UDDI directory service using HTTP GET requests, gathers information and creates CIs and their relationship.

THE OUTCOME

BMC ADDM discovers UDDI Server, Web Services server, Web Service, Web Service Endpoint, Web Service Interface, Web Service operation, Web Service Operation Interface and others.

EXCHANGE MESSAGING SYSTEMS DISCOVERY

WHAT IS EXCHANGE SERVER

Microsoft Exchange Server is a messaging and collaborative software product. It was developed by Microsoft and released in 1993. Since then it is part of the Microsoft Servers line of server products and is widely used by enterprises. Exchange provides the following main features: electronic mail, calendaring, contacts and tasks; support for mobile and web-based access to information; support for data storage.

HOW EXCHANGE SERVER DISCOVERY IS DONE

The discovery uses the LDAP Server method to obtain information from Microsoft Active Directory. An Active Directory service stores full information about any Exchange servers that are registered in the Active Directory service.

A discovery host performs series of LDAP queries against a server that is Active Directory domain controller. As a result it receives necessary Exchange-specific information.

DISCOVERY DETAILS

Exchange Server Inventory discovery requires unfiltered access to LDAP port of the Active Directory domain controller that may hold information about Exchange servers. Also a user must provide a login account with administrative privileges to Active Directory server or an account with view-only privileges to Exchange Server database.

It is important to know that a discovery host and Active Directory server should be in one Active Directory domain/forest or have trust relationships between them.

Exchange Server Inventory discovery may fail if a firewall prevents access to LDAP port of Active Directory server, which number is 389 by default. In this case an exception should be made for discovery host IP address.

THE OUTCOME

BMC ADDM discovers Microsoft Exchange Server version 2003 and 2007.

As a result of discovery task a user receives a list of discovered configuration items, which may contain: Computer System, Communication Endpoint, IP address and Exchange-specific CIs: Exchange Organization, Exchange Administrative Group, Exchange Server, LDAP Server, Information Store, Message Transfer Agent (MTA), System Attendant, Routing Group, Routing Group Connector and EdgeSync.

VIRTUAL SYSTEMS DISCOVERY

WHAT IS VIRTUAL SYSTEM

A Virtual System (or Hypervisor) is a program that allows multiple operating systems to share a single hardware host. Virtual Systems are becoming very popular on the modern IT market because they help organizations to reduce costs, increase return of investments and simplify a management of enterprise application infrastructure.

BMC ADDM supports discovery of the following Virtual Systems: VMware Virtual Center/ESX, Microsoft Hyper-V, Solaris Zones and LPar for AIX.

SOLARIS ZONES

Solaris Zones is a part of Solaris Containers framework solution, which allows creating logical partitions where Solaris operation systems can act independently of each other and from host OS. Solaris Zones made a long way growing from "sandbox" feature of UNIX operation systems to well-scaled element of enterprise-class solution.

VMWARE ESX/GSX

An ESX/GSX server is lightweight virtualization software. ESX/GSX server allows creating virtual computers (usually called "virtual machines") by emulating their hardware components (such as network cards, hard drives, and so on).

When running, a virtual machine uses CPU, memory, and other resources of a physical server on which ESX/GSX is installed. ESX/GSX allows managing virtual machines – create, delete, power them on or off, and so on.

ESX/GSX allows running several virtual machines on a single physical server. Since virtual machines are independent, they can run different operating systems and can be turned on or off without influencing each other.

The difference between ESX and GSX is that an ESX server runs on its own Linux kernel and is installed directly on a "bare metal," while GSX can be installed only on top of Windows or Linux operating systems.

VMWARE VIRTUAL CENTER

VMware VirtualCenter is software for managing ESX and ESXi servers and virtual machines on those servers. The product delivers centralized management, operational automation, resource optimization and high availability to IT environments. Virtualization-based distributed services equip the data center with a high level of responsiveness, service ability, efficiency and reliability. VirtualCenter delivers simplicity, efficiency, security, and reliability required to manage virtualized IT environment of any size.

VirtualCenter consists of:

- » **VirtualCenter Management Server** is the central control node for configuring, provisioning and managing virtualized IT environments. The Management Server runs as a service on Microsoft® Windows 2000, Microsoft® Windows XP Professional and Microsoft® Windows Server 2003.
- » **VirtualCenter Database** is used to store persistent information about the physical servers, resource pools and virtual machines managed by the VirtualCenter Management Server. The database resides on standard versions of Oracle, Microsoft® SQL Server, or Microsoft® MSDE.
- » **Virtual Infrastructure Client** allows administrators and users to connect remotely to the VirtualCenter Management Server or individual ESX Servers from any Windows PC.
- » **VirtualCenter Agent** connects VMware ESX Servers with VirtualCenter Management Server.

MICROSOFT HYPER-V

Microsoft Hyper-V is a role of Windows 2008 Server. This role enables the operating system to act as a Hypervisor and host multiple operating systems in their own environment, separated from each other. Hyper-V is a free feature and it works only on 64bit versions of Windows 2008.

Hyper-V provides a user with Management Console where he/she can perform basic management of virtual machines. More advanced management capabilities are being provided with Microsoft System Center Virtual Machine Manager 2008 (MSCVMM 2008). The MSCVMM 2008 allows management of Hyper-V servers and virtual machines, physical to virtual conversion, self-provisioning and self-servicing.

HOW VIRTUAL SYSTEMS DISCOVERY IS DONE

SSH/TELNET METHOD

Using SSH/Telnet method ADDM collects information from UNIX servers. The SSH/Telnet method uses Telnet and SSH protocols to connect to the target UNIX hosts. To make discovery task successful, SSH and Telnet services must be installed and enabled on the hosts which are being discovered. SSH protocol is more secure than Telnet and should be considered as more preferable.

After connecting to the server, ADDM executes several UNIX commands, parses the results and, if necessary, creates Cls.

VMWARE DIRECT API METHOD

The BMC ADDM server uses **VMware Direct API** method for obtaining information from GSX/ESX hosts. The VMware Direct API method uses the VmPerl Scripting API. By using the VMware Scripting APIs, the BMC ADDM server can access virtual machines without using a local or remote console. VMware Scripting APIs version 2.3 comprises two components: VmCOM and VmPerl.

- DEFINITIONS**
- » **VmCOM** is a Component Object Model (COM) interface for languages such as Microsoft® Visual Basic®, Microsoft® Visual Basic® Scripting Edition (also known as VBScript), Microsoft® Visual C++® and JScript®. You may install the VmCOM Scripting API on machines with the Microsoft® Windows® operating system.
 - » **VmPerl** is an application programming interface (API) that utilizes the Perl scripting language. You may install the VmPerl Scripting API on machines with the Microsoft Windows or Linux operating system.

BMC Discovery uses VmPerl component for VMware discovery. This component requires:

- » The TCP/IP port for connecting to the VMware server remote console. The default port number is 902
- » Any user account and password with access to the VMware server

The PERL scripts of the VMware Direct API connect to server by SSL using RSA or DSS authentication with 3DES encryption.

VMWARE VIRTUAL CENTER/ESX METHOD

BMC ADDM's VMware VirtualCenter/ESX method uses the VMware VirtualCenter Web Service.

- DEFINITION**
- » **VMware VirtualCenter Web service** is a programming interface that exposes the functionality of VMware VirtualCenter to customer-written or third-party applications, such as BMC ADDM. The VirtualCenter Web service is optionally installed with a VirtualCenter server; it must be installed to use this method in BMC ADDM.

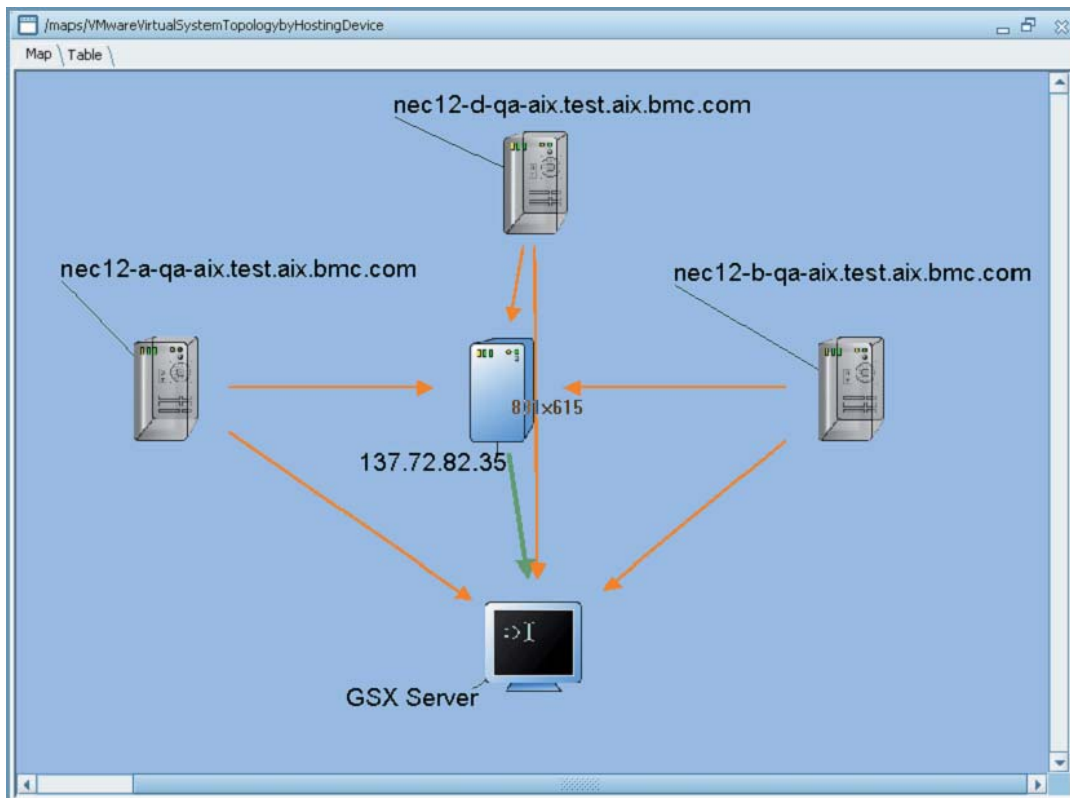
The VirtualCenter Web Service uses SSL protocol to encrypt the traffic between the VirtualCenter client and server. BMC ADDM automatically installs the SSL certificate for the VirtualCenter Web Service on the discovery application server.

During Discovery Task the BMC ADDM connects to 8443 or 443 ports of target Virtual Center server. For VirtualCenter 1.x, the default port number is 8443 and for Virtual Center 2.x and ESX Server 3.x, the default port number is 443.

The access the VMware VirtualCenter Web Service on the VMware server requires a user account which must

belong to the administrator group at VMware VirtualCenter server.

Upon Discovery Task completion, you receive a list of discovered configuration items, which may contain: host names and IP addresses of virtual machines hosted at the target VMware VirtualCenter server.



MSCVMM 2008 METHOD

The BMC ADDM server uses **MSCVMM 2008** method to obtain information from MSCVMM 2008 server. Discovery host uploads a Windows Powershell script to a target server that runs MSCVMM 2008 and executes the script. As a result of script work, discovery host receives a list of Hyper-V servers and virtual machines that are managed by the MSCVMM 2008. The script is being deleted upon completion.

DISCOVERY DETAILS

SOLARIS ZONES

The SSH/Telnet method requires a user account with superuser privileges, such as root. The root account is required for retrieving most complete information about Zones from the Solaris host. In case of none-root account, discovery results may vary, depending on the access rights of the account.

VMWARE GSX/ESX

SSL is used to establish a secure connection between BMC ADDM and ESX/GSX server. RSA, DSS, or 3DES encryption algorithms can be used.

DEFINITIONS

- » **SSL** (Secure Sockets Layer) is a standard security technology for establishing an encrypted connection between a server and a client. This connection ensures that all data passed between the server and the client remains private and integral. By default, secure connections start with "https" instead of "http" in Web browsers. SSL is an industry standard and is used by millions of Web sites in the protection of their online transactions with their customers.

- » **RSA** (Rivest-Shamir-Adleman) is a widely used public key cryptography algorithm, which is named after its originators: Ronald Rivest, Adi Shamir, and Leonard Adleman. RSA is the most popular public key encryption algorithm in use today. RSA can be used for encryption and decryption of information and for the generation and verification of digital signatures.
- » **DSS** (Digital Signature Standard) is the digital signature algorithm (DSA) developed by the U.S. National Security Agency (NSA) to generate a digital signature for the authentication of electronic documents.
- » **3DES** also called Triple DES or EDE (encrypt, decrypt, encrypt), a secret key encryption algorithm based on repeated application of the Data Encryption Standard (DES). 3DES works by applying the DES algorithm three times in succession to 64-bit blocks of plaintext. It does this by using two independent 56-bit keys.

Make sure that firewall on your ESX host is not blocking incoming packets to the ports 443 and 902. When discovery task is running, BMC ADDM connects to the target ESX host and polls the ESX server via API for specific information

VMWARE VIRTUALCENTER

Requires the Virtual Machine Agent port number for the VirtualCenter Web Service. For Virtual Center 1.x, the default port number is 8443 and for Virtual Center 2.x and ESX Server 3.x the default port number is 443.

Requires a user account with access to the VMware VirtualCenter Web Service on the VMware server. The VMware VirtualCenter user account must belong to the administrator group.

TIPS

- » To discover a virtual machine, the virtual machine must be active and VMware Tools must be installed in the guest operating system.
- » To discover a virtual machine using the VirtualCenter method, the VMware server must be connected to the Virtual Center.
- » If ESX Server is a part of a cluster, the discovery task creates a relationship between the ESX Server and the cluster. Virtual inventory discovery creates complete cluster topology but a user must discover all ESX servers that belong to a cluster.

MICROSOFT HYPER-V

For successful discovery of virtual machines on Hyper-V servers, a MSCVMM 2008 server must be running the Windows Management Instrumentation (WMI) service and has Windows Powershell installed.

A discovery host connects to \$ADMIN share of MSCVMM 2008 server via NetBIOS protocol. The credentials for this connection require user domain account that is a member of Local Administrators group. A Windows Powershell script is being uploaded to a \$ADMIN share and executed. It gathers a data using Windows Management Instrumentation interface and sends back results upon completion.

THE OUTCOME

BMC ADDM discovers virtual machines running at the following standalone VMware server hypervisors using VMware Direct API method:

- » VMware ESX Server 2.x releases
- » VMware GSX Server 2.x releases
- » VMware GSX Server 3.x releases
- » VMware Server 1.0 releases

VMware VirtualCenter/ESX method works for the ESX servers connected to the following versions of VMware Virtual Center:

- » Virtual Center 1.2
- » Virtual Center 1.3
- » Virtual Center 2.0
- » VMware ESX Server 3.x releases

The MSCVMM2008 method allows discovering virtual machines that hosted at Hyper-V servers which are connected to Microsoft System Center Virtual Machines Manager 2008.

After discovery task completion, you receive a list of discovered configuration items, which may contain: Virtual System, Virtual System Setting Data, Virtual System Enabler, Cluster, Resource Pool, Computer System, Operating System and others.

UNIVERSAL APPLICATION DISCOVERY

WHAT IS UNIVERSAL APPLICATION DISCOVERY

Universal Application Discovery is designed for discovering non-standard, in-house applications and their relationships.

In a distributed, multi-tier, or multiple-host infrastructure the servers communicate with each other to make an enterprise application work. BMC Universal Application Discovery (UAD) provides discovery of the configuration items that represent enterprise applications. By exploring dependent target hosts the UAD creates a logical “map” of relationships between the applications by analyzing application fingerprints, host ports, and processes.

HOW UNIVERSAL APPLICATION DISCOVERY IS DONE

A running Universal Application Discovery task contacts the target server A and B, gets lists of ports opened by running applications and tries to identify the application by matching it to the records of BMC ADDM internal “applications list.” If UAD finds that an application process is in the “application list,” it marks the process as qualified (or “known”), creates the configuration item for the process and stores the configuration item in the database.

Next, UAD tries to establish a logical link between two application processes by following the list of relationship rules. If the matching is successful, UAD creates the configuration item of relationship and stores it in the database.

In case discovery results are not reliable, a user must validate application and relationship configuration items. BMC ADDM provides a great opportunity to add customer in-house applications to the application list and create custom relationship rules.

DISCOVERY DETAILS

For collection of information from target systems being discovered, UAD uses SNMP, SSH/Telnet, Remote Command, or Tuner methods.

- DEFINITIONS**
- » **SNMP** (Simple Network Management Protocol) is a widely using protocol for network management. With a help of SNMP a user can collect information from and configure a large set of network devices, such as servers, switches, printers and routers. BMC ADDM uses SNMP method to discover additional information from SNMP-enabled devices.
 - » **SSH** (Secure Shell) is a network protocol that allows data to be transmitted and received via secure channel between two network devices. The SSH has been used on Linux and Unix servers for many years. There are other types of SSH-capable devices on a market, such as routers, switches and UPSes.
 - » **Telnet** is a network protocol that allows a user to connect to remote network devices. Telnet is weak in security and does not provide an encryption for a data which is transmitted over the network.

DISCOVERY DETAILS

The SNMP method polls the SNMP agent that is installed in host operating system. If communication was successful, UAD receives information about running application processes on target host. It is important to set in task properties the correct credentials, such as SNMP read-only community name of Linux/Unix/Windows system or a port number of SNMP agent.

SSH/Telnet method executes a specific command (netstat for example) inside Linux or Unix operation systems and retrieves the information about running application processes and open ports. The root account is required for retrieving full information from the host. In case of none-root account, discovery results may vary, depending on the access rights of the account.

The Remote command method is very similar to SSH/Telnet method. The main difference is that the method is

being used in Windows systems to run a command (netstat for example). This method requires domain or local administrator-level account and password.

The Tuner method gathers information from BMC Configuration Management tuner. This application must be installed on Windows, Linux, or UNIX system before using the Tuner method. Also it is required to add a UAD channel on that tuner. The channel UAD.car can be downloaded from

`http://serverhostname:8080/discovery/installers/UAD.car`

where serverhostname is the host name of the BMC ADDM server. The tuner uses the same methods as SSH/Telnet and Remote Command to retrieve a list of processes and open ports from target hosts.

THE OUTCOME

The following list represents the types of configuration items discovered by UAD: Application Server, Software Server, Application Server, Database Server, DNS Server, LDAP Server, FTP Server, Mail Server, News Server, SSH Server, Telnet Server, Web Server and others.

The following applications are supported out-of-the-box by UAD:

- » Apache:
 - Apache EasyPHP Server
 - Apache Tomcat
 - Apache Web Server
 - Apache2 Web Server
- » BEA:
 - BEA Weblogic Application Server
 - BEA Weblogic Node Manager
- » BMC:
 - BMC Atrium CMDB
 - BMC CONTROL-M
 - BMC Distribution Server
 - BMC Impact Manager,
 - BMC Configuration Management Tuner
 - BMC PATROL Agent
 - BMC PATROL Central
 - BMC PATROL Console
 - BMC PATROL Console Server
 - BMC PATROL DashBoard Server
 - BMC PATROL Enterprise Manager
 - BMC PATROL Visualis Client
 - BMC PATROL Visualis Server
 - BMC Portal, BMC PRfN Selection Tools
 - BMC PSRfN Server
 - BMC RealTime Server
 - BMC Remedy Action Request System
 - BMC Remedy SLA Engine
 - BMC Remedy Windows Client
 - BMC ADDM Client
 - BMC ADDM Console
 - BMC ADDM Server
- » Borland Interbase Software
- » Business Object Broadcast Agent, Business Objects Enterprise Server
- » HP
 - HP OpenView Database
 - HP OpenView Network Node Manager

- HP OpenView VPO Agent
- HP OpenView Windows GUI
- HP OVO Management Server
- » Hummingbird Exceed
- » IBM
 - IBM DB2
 - IBM Tivoli Enterprise Console
 - IBM Tivoli Management Platform
 - IBM WebSphere Application Server Service
 - IBM Websphere Server
- » IONA Orbix
- » Microsoft
 - Microsoft AD Controller
 - Microsoft Exchange Server
 - Microsoft IIS
 - Microsoft Windows DNS
 - MSSQL Server
- » MySQL
- » Oracle:
 - Oracle Database Services
 - Oracle DB
 - Oracle Listener
- » Pointbase
- » RealVNC Server
- » SAP
 - SAP DB
 - SAP Gateway
 - SAP Server
 - SAP Service
- » Siebel
 - Siebel Application Server
 - Siebel Gateway Server
 - Siebel Server Manager
- » Solstice Backup Client, Solstice Backup Server
- » Sun One Web Server
- » Sybase
- » VMware
 - VMware Server
 - VMware Virtual Machine
 - VMware VI Client
 - VMware VirtualCenter Server
 - VMware VirtualCenter Web Service
 - VMware Workstation-Console
- » Web Server

NETWORK DISCOVERY

WHAT IS NETWORK DISCOVERY

BMC ADDM can discover a full range of network devices, presenting a precise picture of Local Area Network (LAN) and Wide Area Network (WAN) infrastructure and topology.

In a LAN/WAN network discovery task, you can choose to discover the following types of devices:

- » Network Printer discovers printers and their logical and physical network connections.
- » Network Computer discovers computer systems, such as workstations and servers, and their logical and physical network connections, including network adapters, IP addresses, IP subnets, and LAN and WAN interfaces.
- » Network Infrastructure discovers network infrastructure devices, such as routers and switches and their physical and logical network connections, including MAC addresses, IP address, IP subnets, and LAN and WAN interfaces.

HOW NETWORK DISCOVERY IS DONE

LAN/WAN network discovery uses the SNMP method to collect information from SNMP-enabled devices. The SNMP method retrieves information from SNMP MIBs about the network, running application processes, and the communications occurring among hosts. You can run the SNMP method on any operating system that has an SNMP agent installed.

- DEFINITIONS**
- » **SNMP** (Simple Network Management Protocol) is a widely using protocol for network management. With a help of SNMP a user can collect information from and configure a large set of network devices, such as servers, switches, printers and routers. BMC ADDM uses SNMP method to discover additional information from SNMP-enabled devices.
 - » **MIB** (Management Information Base) is formal description of network objects that can be managed by SNMP. MIB is basically a text file that describes SNMP network elements as a list of data objects.

DISCOVERY DETAILS

For the discovery task to access the SNMP agent, you must create an SNMP community name credential containing an SNMP community name with public access.

THE OUTCOME

LAN/WAN network discovery discovers the logical and physical configuration items of a network and the relationships between those configuration items.

- DEFINITIONS**
- » **Firewall** is a device or application designed to prevent unauthorized access to a computer network. Usually a firewall sits between a private and a public networks. An administrator configures a firewall to allow, deny, encrypt, decrypt, or proxy specific incoming and outgoing network traffic. A firewall examines each message and blocks those that do not meet the specified security criteria.
 - » **Switch** is a device that joins multiple computers together within one local area network (LAN). For example, you can plug an Internet cable to a switch, and then all computers that you plug to this switch will have access to the Internet. A switch looks at each packet or data unit it gets, determines where it should go, and switches it out toward that device.
 - » **Layer 3 Switch** is a high-performance device for network routing, which actually differs very little from routers.
 - » **Router** is a device that joins multiple networks together. This device determines the next

network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet.

- » **Wireless Access Point** (APs or WAPs) is a device that acts as a central transmitter and receiver of wireless network.
- » **Print Server** is a computer that is connected to one or more printers and workstations over a network. A print server accepts print jobs from computers and sends the jobs to the appropriate printers.
- » **Server** is a computer connected to a network that performs a certain role or roles. For example, a database server is the one that hosts a database, a file server is the one that is dedicated to store files, and so on.
- » **Workstation** is a computer intended for business or professional use. The configuration of a workstation depends on the tasks that one has to perform.
- » **Operating System** is a software that provides an environment in which programs can run. Usually operating systems come with built-in programs that allow it to work with files and folders, browse the Internet, play music, and so on.
- » **LAN** is a group of computers and network devices that are connected with each other.
- » **LAN Segment** is a section of a local area network that is used by a particular workgroup or department and separated from the rest of the LAN by a bridge, router or switch. Networks are divided into multiple segments for security and to improve traffic flow by filtering out packets that are not destined for the segment.
- » **DLCI** (Data Link Connection Identifier). is a number of a private or switched virtual circuit in a Frame Relay network that tells the Frame Relay how to route the data.
- » **VLAN** (Virtual Local Area Network) is a logical local area network that extends beyond a single traditional LAN to a group of LAN segments, given specific configurations. Because a VLAN is a logical entity, its creation and configuration is done completely in software.
- » **WAN Network** (Wide Area Network) is a geographically distributed network.

