HP Business Service Management

for the Windows operating system

Software Version: 9.00

Content Pack Version: 6.00

Discovery and Integration Content Permissions

Document Release Date: June 2010
Software Release Date: June 2010

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Intel®, Pentium®, and Intel® Xeon™ are trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

Microsoft®, Windows®, Windows NT®, and Windows® XP are U.S registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

Unix® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Application - Active Directory

Active Directory Connection by LDAP

The job discover the existence of Active Directory Domain Controlers via LDAP.

Protocol: LDAP

Operation	Usage description	Objects and parameters
get	Connect to an AD DC	context = InitialDirContext(environment): InitialDirContext env
get	Get AD attribute information	context.getAttributes('): getAttributes

Active Directory Topology by LDAP

The job discovers Active Directory via LDAP.

Protocol: LDAP

Operation	Usage description	Objects and parameters
get	Connect to an AD DC	context = InitialDirContext(environment): InitialDirContext env
get	Get AD attribute information	context.getAttributes('): getAttributes

Application - Microsoft Exchange

Microsoft Exchange Connection by NTCMD

The job this pattern discovers Microsoft Exchange 2007 by NTCMD protocol. It is based on executing PowerShell scenario on the remote machine.

Protocol: PowerShell

Operation	Usage description	Objects and parameters
Exchange View-Only Administrator	Get Exchange server properties	Get-ExchangeServer

Protocol: Shell

Operation	Usage description	Objects and parameters
copy	Copy file to a remote machine	Exchange_Server_2007_Discovery.ps1 - PowerShell script for Exchange Server discovery

Microsoft Exchange Connection by WMI

The job connects to remote host by WMI and discovers Exchange Server CI.

Protocol: WMI

Operation	Usage description	Objects and parameters
select	Get Microsoft Exchange Server 2003 FQDN, GUID, Type, ExchangeVersion and other properties	root\MicrosoftExchangeV2 Exchange_Server
select	Get Hostname of Exchange server	root\cimv2 Win32_ComputerSystem

Microsoft Exchange Topology by LDAP

The job pattern discovers Microsoft Exchange topology using information stored in Active Directory.

Protocol: LDAP

Operation	Usage description	Objects and parameters
query	Get Exchange Organizations	CN=Microsoft Exchange,CN=Services (objectClass=msExchOrganizationContainer)
query	Get Administrative Groups	CN=Administrative Groups (objectClass=msExchAdminGroup)
query	Get Routing Groups	CN=Routing Groups (objectClass=msExchRoutingGroup)
query	Get Exchange Servers	CN=Servers (objectClass=msExchExchangeServer)
query	Get Server MTAs	Administrative Groups (objectClass=mTA)
query	Get SMTP Connectors	CN=Connections (objectClass=msExchRoutingSMTPConnector)

query	Get Routing Group Connectors	CN=Connections (objectClass=msExchRoutingGroupConnector)
query	Get Receive Connectors	CN=SMTP Receive Connectors,CN=Protocols (objectClass=msExchSmtpReceiveConnector)

Protocol: probe's shell

Operation	Usage description	Objects and parameters
nslookup	resolve server's FQDN using remote DNS	

Microsoft Exchange Topology by NTCMD

The job this pattern discovers Microsoft Exchange 2007 topology by NTCMD protocol. It is based on executing PowerShell scenario on the remote machine.

Protocol: PowerShell

Operation	Usage description	Objects and parameters
Exchange View-Only Administrator	Get Exchange server properties	Get-ExchangeServer

Protocol: Shell

Operation	Usage description	Objects and parameters
copy	Copy file to remote machine	Exchange_Server_2007_Discovery.ps1 - PowerShell script for Exchange Server discovery

Microsoft Exchange Topology by WMI

The job connects to the remote host and brings topology for Microsoft Exchange Server 2003.

Protocol: WMI

Operation	Usage description	Objects and parameters
select	Get Hostname of Exchange server	root\cimv2 Win32_ComputerSystem
select	Get Administrative and routing groups information	root\MicrosoftExchangeV2 Exchange_Server
select	Get Folder trees	root\MicrosoftExchangeV2 Exchange_FolderTree
select	Get Public folders	root\MicrosoftExchangeV2 Exchange_PublicFolder

Application - Oracle E-Business Suite

Oracle Applications by SQL

The job this pattern discovers Oracle E-Business Suite components.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	General system status info	FND_OAM_APP_SYS_STATUS
select	Fetch applications info	FND_PRODUCT_INSTALLATIONS FND_APPLICATION_VL FND_PRODUCT_DEPENDENCIES
select	Fetch applications services info	FND_CONCURRENT_QUEUES_VL FND_CP_SERVICES_VL

Application - SAP

SAP ABAP Connection by SAP JCO

The job discover SAP Systems based on SAP JCO.

Protocol: Sap ABAP

Operation	Usage description	Objects and parameters
connect	Create Connection	Connection: S_RFC RFC1, SALX, SBDC, SDIF, SDIFRUNTIME,SDTX, SLST,SRFC,STUB,SUTL,SXMB,SXMI,SYST,SYSU, SEU_COMPONENT Create XMI Session: S_XMI_PROD EXTCOMPANY=MERCURY;EXTPRODUCT=DARM;INTERFACE=XAL
select	Querying SAP System	Table Maintenance: S_TABU_DIS DICBERCLS=SS;DICBERCLS=SC;DICBERCLS=&NC&

SAP ABAP Topology by SAP JCO

The job discover SAP environment based on Computer Center Management System (CCMS).

Protocol: Sap ABAP

Operation	Usage description	Objects and parameters
connect	Create Connection	Connection: S_RFC RFC1, SALX, SBDC, SDIF, SDIFRUNTIME,SDTX, SLST,SRFC,STUB,SUTL,SXMB,SXMI,SYST,SYSU, SEU_COMPONENT Create XMI Session: S_XMI_PROD EXTCOMPANY=MERCURY;EXTPRODUCT=DARM;INTERFACE=XAL
select	Querying SAP System	Table Maintenance: S_TABU_DIS DICBERCLS=SS;DICBERCLS=SC;DICBERCLS=&NC&

SAP Applications by SAP JCO

The job discovers a SAP environment based on Computer Center Management System (CCMS). If a long period of time is defined for transaction changes (the 'from' date to the 'to' date), a pattern will take a long time to complete (maybe several hours).

Protocol: Sap ABAP

Operation	Usage description	Objects and parameters
connect	Create Connection	Connection: S_RFC RFC1, SALX, SBDC, SDIF, SDIFRUNTIME,SDTX, SLST,SRFC,STUB,SUTL,SXMB,SXMI,SYST,SYSU, SEU_COMPONENT Create XMI Session: S_XMI_PROD EXTCOMPANY=MERCURY;EXTPRODUCT=DARM;INTERFACE=XAL
select	Querying SAP System	Table Maintenance: S_TABU_DIS DICBERCLS=SS;DICBERCLS=SC;DICBERCLS=&NC&

SAP ITS by NTCMD

The job discover SAP environment based on Computer Center Management System (CCMS).

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Fetch file content	type {FILE_NAME} cat {FILE_NAME}

SAP Java Topology by SAP JMX

The job discover SAP environment based on Computer Center Management System (CCMS).

Protocol: JMX

Operation	Usage description	Objects and parameters
select	Get all SAP Instances	Discover All Instances: Type=SAP_J2EEClusterNode Discover J2EE Clusters: Type=SAP_J2EECluster Discover Central Instances: Type=SAP_J2EEInstance
select	Get Applications Info	Type=SAP_J2EEServiceRuntimePerNode Type=SAP_J2EEClusterNode
select	Get Database Configuration Info	Type=SAP_J2EEKernelPerNode Type=SAP_J2EEServicePerNode Type=SAP_J2EEClusterNode

SAP Profiles by Shell

The job discovers profile files for SAP Application Servers.

Protocol: Shell

Operation	Usage description	Objects and parameters
select	Basic Login	uname ver
select	Discover files	UNIX: cat {FILE_PATH} Windows: type {FILE_PATH}

SAP Solution Manager Topology by SAP JCO

The job discover SAP Topology based on Solution Manager.

Protocol: Sap ABAP

Operation	Usage description	Objects and parameters
connect	Create Connection	Connection: S_RFC RFC1, SALX, SBDC, SDIF, SDIFRUNTIME,SDTX, SLST,SRFC,STUB,SUTL,SXMB,SXMI,SYST,SYSU, SEU_COMPONENT Create XMI Session: S_XMI_PROD EXTCOMPANY=MERCURY;EXTPRODUCT=DARM;INTERFACE=XAL
select	Querying SAP Solution Manager	Table Maintenance: S_TABU_DIS DICBERCLS=SS;DICBERCLS=SC;DICBERCLS=&NC&

SAP Solution Manager by SAP JCO

The job discover SAP environment based on Computer Center Management System (CCMS).

Protocol: Sap ABAP

Operation	Usage description	Objects and parameters
connect	Create Connection	Connection: S_RFC RFC1, SALX, SBDC, SDIF, SDIFRUNTIME,SDTX, SLST,SRFC,STUB,SUTL,SXMB,SXMI,SYST,SYSU, SEU_COMPONENT Create XMI Session: S_XMI_PROD EXTCOMPANY=MERCURY;EXTPRODUCT=DARM;INTERFACE=XAL
select	Querying SAP System	Table Maintenance: S_TABU_DIS DICBERCLS=SS;DICBERCLS=SC;DICBERCLS=&NC&

SAP System By Shell

The job parses config files and discovers SAP Systems.

Protocol: Shell

Operation	Usage description	Objects and parameters
select	Basic Login	ver uname
select	Discover files	Windows: type {FILE_PATH} UNIX: cat {FILE_PATH}

SAP TCP Ports

The job discover open tcp\udp ports on a host of known server ports.

There are no permissions required for this job.

Application - Siebel

Siebel Application Server Configuration

The job discover configuration file of Siebel application server.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Fetching configuration file content	Windows: type {SIEBEL_INSTALL_DIR}\bin\ENU\siebel.cfg UNIX: cat {SIEBEL_INSTALL_DIR}/bin/ENU/siebel.cfg

Siebel Application Servers

The job discover Siebel topology using srvrmgr client.

Protocol: Siebel

Operation	Usage description	Objects and parameters
exec	Basic connect to the Siebel system	srvrmgr.exe /e {SIEBEL_SITE_NAME} /g {IP} /u {USER} /p {PASSWORD} /k
exec	Fetch application servers info	srvrmgr.exe list servers show SBLSRVR_NAME, HOST_NAME, INSTALL_DIR, SBLMGR_PID, SV_DISP_STATE, SBLSRVR_STATE, START_TIME, END_TIME, SBLSRVR_STATUS, SV_SRVRID srvrmgr.exe set server {SIBELSERVERNAME} Fetching server components info: srvrmgr.exe list compgrps list comps list params for component {COMPONENT_NAME} srvrmgr.exe list parameter DSConnectString for named subsystem ServerDataSrc list parameters DSSQLStyle for named subsystem ServerDataSrc list param connect srvrmgr.exe unset server

Siebel DB by TTY

The job discover DB of odbc connection.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Gathering Oracle database info	env UNIX: cat {SIEBEL_INSTALL_DIR}/sys/.odbc.ini /var/opt/oracle/oraInst.loc {TNSNAMES.ORA_PATH} {SQLNET.ORA_PATH}
exec	Gathering DB2 database info	UNIX: cat {SIEBEL_INSTALL_DIR}/sys/.odbc.ini cat /etc/services | grep {SERVICENAME} UNIX: db2 list database directory|grep -ip {DATABASE_NAME}|grep -i {NODE_NAME} list node directory|grep -ip {NODE_NAME}

Siebel DB by WMI and NTCMD

The job discover DB of odbc connection.

Protocol: WMI

Operation	Usage description	Objects and parameters
exec	Gathering database info	Windows: root\DEFAULT StdRegProv:EnumKey() StdRegProv:EnumValues()

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Fetching files content	Windows: type {TNSNAMES.ORA_PATH} {SQLNET.ORA_PATH}
exec	Gathering DB2 database info	Windows: db2 /c /w /i db2 list database directory /c /w /i db2 list node directory

Siebel Gateway Connection

The job this pattern discovers Siebel Gateway Naming Server and related components by Siebel-Web protocol.

Protocol: Siebel

Operation	Usage description	Objects and parameters
exec	Basic connect to the Siebel system	srvrmgr.exe /e {SIEBEL_SITE_NAME} /g {IP} /u {USER} /p {PASSWORD} /k
exec	Gather database related info	srvrmgr.exe list parameter DSConnectString for named subsystem GatewayDataSrc list parameters DSSQLStyle for named subsystem GatewayDataSrc list parameters DSSQLStyle for named subsystem ServerDataSrc list advanced params DSSQLStyle for named subsystem ServerDataSrc

Siebel Web Applications by NTCMD

The job this pattern discovers Siebel Webserver Extension and all web applications by NTCMD protocol.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Getting Siebel software configuration	Windows: reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall /S Windows: type {SOFTWARE_INSTALL_PATH}\BIN\eapps.cfg *

Siebel Web Applications by TTY

The job discover Siebel Webserver Extension and all web applications.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Getting Siebel software configuration	Windows: ps -ef | grep ns-http -ef | grep httpd UNIX: cat /opt/sadmin/sweapp/bin/obj.conf {SOFTWARE_INSTALL_PATH}/eapps.cfg *

Application - UDDI Registry

WebServices by URL

The job discovers the Webservice topology by reading WSDL content from a given URL.

There are no permissions required for this job.

Webservice Connections by UDDI Registry

The job this pattern discovers the UDDI registry using a given URL.

There are no permissions required for this job.

Webservices by UDDI Registry

The job discovers a UDDI Registry and published services using a given URL.

Protocol: HTTP

Operation	Usage description	Objects and parameters
get	Get UDDI registry	GET $url

Application - WebSphere MQ

MQ by Shell

The job discover MQ topology by using SSH, TELNET or NTCMD.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic login	ver uname
exec	Discover MQ Version and Queue Managers Info	mqver dspmqver dspmq
exec	Discover Queue Manager Listen Ports	ps efw | grep runmqlsr ef | grep runmqlsr cat /etc/inetd.conf | grep amqcrsta
exec	Discover Queue Managers Info	runmqsc {QUEUEMANAGER} \nDISPLAY QMGR DESCR DEADQ DEFXMITQ REPOS CCSID\nend {QUEUEMANAGER} \nDISPLAY QMGR\nend {QUEUEMANAGER} \nDISPLAY QUEUE(*) TYPE, DESCR, CLUSTER, CLUSNL, USAGE, RNAME, RQMNAME, XMITQ, TARGQ\nend {QUEUEMANAGER} \nDISPLAY CHANNEL(*) CHLTYPE,TRPTYPE,DESCR,CLUSTER,CLUSNL,CONNAME,XMITQ\nend
exec	Discover MQ Cluster Info	runmqsc {QUEUEMANAGER} \ndisplay clusqmgr(*) all\nend

Protocol: WMI

Operation	Usage description	Objects and parameters
exec	Discover Queue Manager Listen Ports	Windows: root\DEFAULT StdRegProv:EnumKey() StdRegProv:EnumValues()

Cluster - Microsoft Cluster

MS Cluster by NTCMD

The job this pattern discovers Microsoft Cluster architecture by NTCMD.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic login	ver
exec	Discover MS Cluster Topology	CLUSTER /VER /PROP:DefaultNetworkRole,EnableEventLogReplication,QuorumArbitrationTimeMin,QuorumArbitrationTimeMax,EnableResourceDllDeadlockDetection,ResourceDllDeadlockTimeout,ResourceDllDeadlockThreshold,ResourceDllDeadlockPeriod,ClusSvcHeartbeatTimeout,HangRecoveryAction NODE NODE {THENODENAME} /prop:NodeHighestVersion,NodeLowestVersion,BuildNumber,CSDVersion,Description,EnableEventLogReplication 'cluster netint /node:{THENODENAME} /net:Public /prop:Address GROUP GROUP {THEGROUPNAME} /prop GROUP RESOURCE | find {THEGROUPNAME} GROUP RESOURCE {RESOURCENAME} /PROP GROUP RESOURCE {RESOURCENAME} /PRIV GROUP RESOURCE {RESOURCENAME} /LISTDEP

Cluster - ServiceGuard

Service Guard Cluster Topology by TTY

The job discover ServiceGuard cluster server architecture by TTY.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic Login	ver uname
exec	Connecting to cluster software	/usr/sbin/cmviewcl -v
exec	Fetching configuration file content	UNIX: cat {FILE_PATH}

Cluster - Veritas

Veritas Cluster by Shell

The job discover Veritas cluster server architecture by Shell.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic Login	ver uname
exec	Checking for existing of configuration file	ls /etc/rc3.d/S*vcs
exec	Fetching configuration file content	cat {FILE_PATH}

Database - DB2

DB2 Connection by SQL

The job dB2 database connection pattern.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Check DB2 dadabase version	sysibm.sysversions SYSIBMADM.ENV_INST_INFO

DB2 Topology by SQL

The job discover the physical elements within DB2 database.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Getting tablespaces info	sysproc.SNAPSHOT_CONTAINER
select	Getting opened db sessions info	sysproc.SNAPSHOT_APPL_INFO
select	Getting existing schema names	SYSCAT.SCHEMATA

Databases TCP Ports

The job discover open tcp\udp ports on a host of known server ports.

There are no permissions required for this job.

Database - MS-SQL

Databases TCP Ports

The job discover open tcp\udp ports on a host of known server ports.

There are no permissions required for this job.

MSSQL Connection by SQL

The job this pattern discovers databases using SQL protocol.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Check Oracle/MS SQL database version	v$version @@version SERVERPROPERTY ProductVersion

MSSQL Server Credentials by SQL

The job this pattern discovers the credentials of SQL Server database discovered by patterns which do not use SQL credentials.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Check MSSQL Server version	@@version

MSSQL Topology by SQL

The job the job discovers MS SQL Server topology.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Get server properties	SERVERPROPERTY ProductVersion Collation IsClustered LicenseType IsFulltextInstalled InstanceName Edition ProductLevel
select	Gather users info	master..syslogins
select	Gather schemas info	master..sysdatabases
exec	Server configutation	master..xp_instance_regread HKEY_LOCAL_MACHINE SOFTWARE\Microsoft\MSSQLServer\MSSQLServer MailAccountName HKEY_LOCAL_MACHINE SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\SuperSocketNetLib ProtocolList HKEY_LOCAL_MACHINE SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\SuperSocketNetLib\Tcp TcpHideFlag HKEY_LOCAL_MACHINE SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\SuperSocketNetLib\Tcp TcpPort

select	Server configutation	master.dbo.spt_values master.dbo.sysconfigures master..sysobjects
select	Server startup info	master..sysobjects
exec	Server startup info	master..xp_instance_regread HKEY_LOCAL_MACHINE SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\Parameters SQLArg??
select	SQL Server Plans	msdb..sysjobs msdb.dbo.sysdtspackages90 msdb.dbo.sysdtspackagefolders90 msdb.dbo.sysmaintplan_subplans msdb.dbo.sysmaintplan_plans msdb.dbo.sysdbmaintplans msdb.dbo.sysdbmaintplan_databases
select	Gather process information	master..sysprocesses master..sysdatabases
exec	Cluster information information	master..xp_instance_regread HKEY_LOCAL_MACHINE SOFTWARE\Microsoft\MSSQLServer\Replication IsInstalled sp_helpdistributor sp_helpdistpublisher
select	Database configuration	master..sysfiles master..sysfilegroups master..sysusers

Database - MySQL

MySQL by Shell

The job discovers MySQL instances and replication topology.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec		{MYSQL_HOME}/bin/mysqld --verbose --help
exec		WIN: type {MYSQL_HOME}/my.cnf UNIX: cat {MYSQL_HOME}/my.cnf

Database - Oracle

Databases TCP Ports

The job discover open tcp\udp ports on a host of known server ports.

There are no permissions required for this job.

Oracle Config Files by SQL

The job this pattern discovers Oracle database configuration based on its v$parameter table.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Get server properties	v$parameter

Oracle Connection by SQL

The job this pattern discovers databases using SQL protocol.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Check Oracle/MS SQL database version	v$version @@version SERVERPROPERTY ProductVersion

Oracle Listeners by Shell

The job discovers Oracle TNS Listener by Shell.

Protocol: shell

Operation	Usage description	Objects and parameters
file read	Read of Listener configuration	cat $ORACLE_HOME/network/admin/listener.ora
exec	Listener curent status	$ORACLE_HOME/bin/lsnrctl status

Oracle RAC Topology by Shell

The job discovers Oracle RAC Topology by Shell.

Protocol: shell

Operation	Usage description	Objects and parameters
file read	Parsing of listener and tnsnames configuration files	cat $ORACLE_HOME\network\listener.ora cat $ORACLE_HOME\network\admin\tnsnames.ora

Oracle Topology by SQL

The job this pattern discovers Oracle database topology by SQL.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Check Oracle database version	v$version
select	Gather database info	v$CONTROLFILE v$parameter DBA_TEMP_FILES Discover objects of requested types: DBA_OBJECTS V$BACKUP DBA_SNAPSHOTS DBA_TABLESPACES V$DATAFILE DBA_USERS V$SESSION V$LOG v$database V$LOGFILE DBA_DB_LINKS dba_scheduler_jobs V$RECOVER_FILE DBA_JOBS
select	Oracle RAC related info	V$SPPARAMETER Discover all the rac nodes: GV$INSTANCE

Database - Oracle TNS

Oracle Config Files by SQL

The job this pattern discovers Oracle database configuration based on its v$parameter table.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Get server properties	v$parameter

Oracle Credentials by SQL

The job this pattern discovers the credentials of Oracle database discovered by TNS parser using an Oracle protocol.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Check Oracle database version	v$version

Oracle TNSName by Shell

The job discovers and parses Oracle configuration documents.

Protocol: Shell

Operation	Usage description	Objects and parameters
select	Basic Login	ver uname
select	Discover files	Windows: dir {FOLDER_PATH} /Q /-C UNIX: ls -lA {FOLDER_PATH} Windows: attrib {FILE_PATH} Windows: type {FILE_PATH} UNIX: cat {FILE_PATH}

Database - Sybase

Databases TCP Ports

The job discover open tcp\udp ports on a host of known server ports.

There are no permissions required for this job.

Sybase Connection by SQL

The job this pattern discovers Sybase database by SQL.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Check sybase dadabase version	@@version

Sybase Topology by SQL

The job this pattern discovers Sybase database topology by SQL.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Getting existing schema names	master.dbo.sysusages master..spt_values master..sysdatabases
select	Getting opened db sessions info	master..sysprocesses master..syslogins master..sysdatabases
select	Getting tablespaces info	sybsystemprocs..sp_helpdevice

Discovery Samples

Dynamic Credential Sample

The job this Discovery Pattern serves as a sample how to dynamically create and use credentials for connecting to remote machines.

There are no permissions required for this job.

Import from CSV sample

The job imports data from a CSV file into CMDB, using mapping of the CSV file columns to CIT attributes
This mapping is usually defined by the setting pattern parameters:
ciType: to define the CIT name which you want to create, mappingString: to define the mapping of the CIT attributes to the CSV file columns
In cases you need more complex mapping abilities, such as conversion of the strings contained in CSV file to the appropriate type of CMDB object's attribute,
you should use the mapping XML configuration file specified by the mappingFile parameter.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic Login	ver uname
exec	Fetching file content	Windows: type UNIX: cat

Discovery Tools

File Monitor by Shell

The job discovers Document files and Directories.

There are no permissions required for this job.

Import from CSV file

The job imports data from a CSV file into CMDB, using mapping of the CSV file columns to CIT attributes
This mapping is usually defined by the setting pattern parameters:
ciType: to define the CIT name which you want to create, mappingString: to define the mapping of the CIT attributes to the CSV file columns
In cases you need more complex mapping abilities, such as conversion of the strings contained in CSV file to the appropriate type of CMDB object's attribute,
you should use the mapping XML configuration file specified by the mappingFile parameter.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic Login	ver uname
exec	Fetching file content	Windows: type UNIX: cat

Import from Database

The job imports data from a an external database into CMDB, using mapping of table columns to CIT attributes
This mapping is usually defined by the setting pattern parameters:
ciType: to define the CIT name which you want to create, mappingString: to define the mapping of the CIT attributes to the table columns
In cases you need more complex mapping abilities, such as conversion of types you should use the mapping XML configuration file specified by the mappingFile parameter.
A SQL 'select' query is generated automatically and selects all columns in specified table, which defined by parameter: tableName
In advanced cases you can specify SQL query itself, which allows complex selects from more then one table.

There are no permissions required for this job.

Import from Properties file

The job imports data from a Properties file into CMDB, using mapping of the CSV file columns to CIT attributes
This mapping is usually defined by the setting pattern parameters:
ciType: to define the CIT name which you want to create, mappingString: to define the mapping of the Properties attributes to the CSV file columns
In cases you need more complex mapping abilities, such as conversion of the strings contained in Properties file to the appropriate type of CMDB object's attribute,
you should use the mapping XML configuration file specified by the mappingFile parameter.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic Login	ver uname
exec	Fetching file content	Windows: type UNIX: cat

Integration - EMC Control Center

ECC Integration by SQL

The job this pattern discovers storage devices and SAN infrastructure from the EMC control Center SRM database.

Protocol: sqlprotocol

Operation	Usage description	Objects and parameters
select	Discover Fiber Channel Switch details	Fiber Channel Port: stssys.sts_switch_port Fiber Channel Switch: stssys.sts_switch_list
select	Discover Storage Array details	Storage Array: stssys.sts_array_list Logical Volume: stssys.sts_array_device Fiber Channel Port and HBA: stssys.sts_array_port
select	Discover Host details	Logical Volume dependencies: stssys.sts_host_shareddevice General Host info: stssys.sts_host_list Fiber Channel Port and HBA: stssys.sts_host_hba Logical Volume: stssys.sts_host_device
select	Discovery Fiber Channel Connect links	FCConnect between Array and Switch: stssys.sts_array_port_connection FCConnect between Switch and Host: stssys.sts_switch_port

Integration - NNM Layer2

Layer2 by NNM

The job this pattern connects to the NNMi web service and pulls NNMi discovered nodes, IPs, networks, interfaces and layer two connection information to create a Layer 2 topology in UCMDB. Note that it is recommended NOT to run the UCMDB Layer 2 discoveries if using NNMi Layer 2 integration discovery.

Protocol: NNM

Operation	Usage description	Objects and parameters
Web Service calls	Permission to access web services. Requires Integration License	http://<nnm_server>:<port>/IPv4AddressBeanService/IPv4AddressBean: getIPv4Addresses() offset, maxObjects http://<nnm_server>:<port>/InterfaceBeanService/InterfaceBean: getInterfaces() offset, maxObjects http://<nnm_server>:<port>/L2ConnectionBeanService/L2ConnectionBean: getL2Connections() offset, maxObjects http://<nnm_server>:<port>/IPv4SubnetBeanService/IPv4SubnetBean: getIPv4Subnets() offset, maxObjects http://<nnm_server>:<port>/NodeBeanService/NodeBean: getNodes() offset, maxObjects

Update Ids in NNM

The job this pattern updates the nodes in the NNM topology with the UCMDB IDs of the corresponding nodes in UCMDB.

Protocol: NNM

Operation	Usage description	Objects and parameters
Web Service calls	Permission to access web services. Requires Integration License	http://<nnm_server>:<port>/NodeBeanService/NodeBean: updateCustomAttributes() NNM ID, custom attribute

Integration - Storage Essentials

SE Integration by SQL

The job this discovery job retrieves Storage and SAN information from the HP Storage Essentials SRM database.

Protocol: sqlprotocol

Operation	Usage description	Objects and parameters
select	Checking if materialized views are being refreshed	appiq_system.mview_status
select	Discover Fiber Channel Switch details	Fiber Channel Switch: appiq_system.mvc_switchsummaryvw Get additional FC Switch data: appiq_system.mvc_swtichconfigvw Fiber Channel Port: appiq_system.mvc_portsummaryvw
select	Discover Storage Array details	Storage Array: appiq_system.mvc_storagesystemsummaryvw Fiber Channel Port: appiq_system.mvc_portsummaryvw HBA: appiq_system.mvc_cardsummaryvw STORAGE PROCESSOR: appiq_system.mvc_storageprocessorsummaryvw STORAGE POOL: appiq_system.mvc_storagepoolconfigvw appiq_system.mvc_storagevolumesummaryvw: appiq_system.mvc_storagepoolconfigvw
select	FC Host information	General Host info: appiq_system.mvc_hostsummaryvw General Host info: appiq_system.mvc_assetsummaryvw
select	Share links between Logical Disks and Logical Volums	appiq_system.mvc_hostsummaryvw appiq_system.mvc_pathvw appiq_system.mvc_subpathvw appiq_system.mvc_diskdrivesummaryvw appiq_system.mvc_hostvolumesummaryvw appiq_system.mvc_storgaepoolsummaryvw appiq_system.mvc_storagevolumesummaryvw appiq_system.mvc_storagevolumeports appiq_system.mvc_protocolcontrollervw
select	FC connect links between FC Ports	appiq_system.mvc_portsummaryvw

J2EE - JBoss

J2EE JBoss by Shell

The job this pattern discovers JBoss J2EE environment and components using shell.

Protocol: Shell

Operation	Usage description	Objects and parameters
select	Basic Login	uname ver
select	Discover files	Windows: dir {FOLDER_PATH} /Q /-C UNIX: ls -lA {FOLDER_PATH} Windows: attrib {FILE_PATH} UNIX: cat {FILE_PATH} Windows: type {FILE_PATH}

J2EE TCP Ports

The job discover open tcp\udp ports on a host of known server ports.

There are no permissions required for this job.

JBoss Connections by JMX

The job this pattern discovers JBoss servers instances based on the JMX protocol.

Protocol: JMX

Operation	Usage description	Objects and parameters
select	Get Server Name	jboss.system:type=ServerConfig,*
select	Get Server Address	jboss.system:type=ServerInfo,*
select	Get Server Version	jboss.system:type=Server,*

JBoss by JMX

The job this pattern discovers JBoss J2EE environment and components based on the JMX protocol.

Protocol: JMX

Operation	Usage description	Objects and parameters
select	Get JMS info	jboss.mq.destination:service=Topic,* jboss.mq.destination:service=Queue,*
select	Get JVM info	jboss.management.local:j2eeType=JVM,*

select	Get EJBs info	jboss.management.local:j2eeType=StatefullSessionBean,* jboss.management.local:j2eeType=MessageDrivenBean,* jboss.management.local:j2eeType=EJBModule,* jboss.management.local:j2eeType=StatelessSessionBean,* jboss.management.local:j2eeType=EntityBean,*
select	Get Web Modules info	jboss.management.local:j2eeType=Servlet,* jboss.management.local:j2eeType=WebModule,*
select	Get JDBC DataSource info	jboss.jca:service=ManagedConnectionPool,* jboss.management.local:j2eeType=WebModule,*

J2EE - Oracle Application Server

Oracle Application Server

The job discovers Oracle Application Server.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Fetch file content	Windows: type {FILE_FULLPATH} Windows: dir {DIR}*.wsdl /s |find "server-wsdl"

WebServices by URL

The job discovers the Webservice topology by reading WSDL content from a given URL.

There are no permissions required for this job.

J2EE - WebLogic

J2EE TCP Ports

The job discover open tcp\udp ports on a host of known server ports.

There are no permissions required for this job.

J2EE Weblogic Connections by JMX

The job discovers WebLogic Server based on JMX protocol. Supported versions: 6.0, 6.1, 7.0, 8.1, 9.0, 9.1, 9.2, 10.

Protocol: JMX

Operation	Usage description	Objects and parameters
select	Get Server Name, Listen Address and Version	Type=ServerRuntime

J2EE Weblogic by JMX

The job this pattern discovers WebLogic j2ee environment and components.Supported WL versions:6.0, 6.1, 7.0, 8.1, 9.0, 9.1, 9.2,10.

Protocol: JMX

Operation	Usage description	Objects and parameters
select	Get all node names and SSL ports	Type=SSL Type=Server
select	Get Server info	Type=ServerRuntime
select	Get J2EE Domain info	Type=DomainRuntime
select	Get Clusters info	Type=Cluster
select	Get Applications info	Type=WebAppComponent Type=Servlets Type=Application Type=ApplicationRuntime Type=WebAppComponentRuntime Type=EJBComponentRuntime Type=EJBComponent
select	Get Web Services info	Type=ServletRuntime Type=WebServiceRuntime
select	Get JDBC info	Type=JDBCConnectionPool Type=JDBCDataSourceConfig Type=JDBCTxDataSource Type=JDBCDataSource

select	Get JMS info	Type=JDBCDataSourceConfig Type=JMSServer Type=JDBCTxDataSource Type=JDBCDataSource
select	Get Deployment info	Type=DeploymentTaskRuntime
select	Get Execute Queue info	Type=ExecuteQueue

J2EE Weblogic by Shell

The job discovers WebLogic J2EE environment and components by shell. Supported versions: 8.1, 9.0, 9.1, 9.2, 10.

Protocol: Shell

Operation	Usage description	Objects and parameters
select	Basic Login	uname ver
select	Discover files	Windows: dir {FOLDER_PATH} /Q /-C UNIX: ls -lA {FOLDER_PATH} Windows: attrib {FILE_PATH} UNIX: cat {FILE_PATH} Windows: type {FILE_PATH}

WebServices by URL

The job discovers the Webservice topology by reading WSDL content from a given URL.

There are no permissions required for this job.

J2EE - WebSphere

J2EE TCP Ports

The job discover open tcp\udp ports on a host of known server ports.

There are no permissions required for this job.

J2EE WebSphere Connections by JMX

The job this pattern discovers WebSphere servers based on either SOAP or RMI authentication.

Protocol: JMX

Operation	Usage description	Objects and parameters
select	Get Server Name and Version	*:type=Server,*

J2EE WebSphere by Shell

The job this pattern discovers WebSphere J2EE environment and components by shell.

Protocol: Shell

Operation	Usage description	Objects and parameters
select	Basic Login	uname ver
select	Discover files	Windows: dir {FOLDER_PATH} /Q /-C UNIX: ls -lA {FOLDER_PATH} Windows: attrib {FILE_PATH} UNIX: cat {FILE_PATH} Windows: type {FILE_PATH}

J2EE WebSphere by Shell or JMX

The job this pattern discovers WebSphere J2EE environment and components.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Fetch file content	cat {FILE_NAME} type {FILE_NAME}

Protocol: JMX

Operation	Usage description	Objects and parameters
select	Get Server info	*:type=Server,*

select	Get Cluster info	*:type=Server,*
select	Get Applications info	*:type=Application,cell=<CELL_NAME>,node=<NODE_NAMEgt;,Server=<SERVER_NAMEgt;,*
select	Get JMS Server info	*:type=JMSServer,cell=<CELL_NAME>,node=<NODE_NAMEgt;,Server=<SERVER_NAMEgt;,*
select	Get JDBC Provider info	*:type=JDBCProvider,cell=<CELL_NAME>,node=<NODE_NAMEgt;,Server=<SERVER_NAMEgt;,*

Network - Advanced

Arp Table by SNMP

The job this pattern discovers the ARP table of a router using the SNMP protocol. This discovery reveals IP addresses by querying the protocol that translates IPs into the Ethernet addresses used by local area networks, as well as the host and network it belongs to.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	Discover ipAddrEntry	iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable.ipAddrEntry: 1.3.6.1.2.1.4.20.1
get	Discover ARP table	iso.org.dod.internet.mgmt.mib-2.ip.ipNetToMediaTable.ipNetToMediaEntry.ipNetToMediaPhysAddress: 1.3.6.1.2.1.4.22.1.2
get	Discover ARP physical address	iso.org.dod.internet.mgmt.mib-2.at.atTable.atEntry.atPhysAddress: 1.3.6.1.2.1.3.1.1.2

Cisco HSRP by SNMP

The job discovers Cisco HSRP routers using SNMP protocol.

There are no permissions required for this job.

Class B IPs by ICMP

The job performs an IP ping sweep on class B networks.

There are no permissions required for this job.

DNS Zone by Nslookup

The job discovers the DNS Zone topology by a querying all available DNS servers.

Protocol: WMI

Operation	Usage description	Objects and parameters
select	Obtains Zone names	Windows: root\DEFAULT StdRegProv:EnumKey() StdRegProv:EnumValues() uname

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Zones discovery	nslookup ls -d {ZONE_NAME} | nslookup {IP_ADDRESS}

Host Networking by SNMP

The job discovers host networking topology using SNMP route and system tables.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	System table info	iso.org.dod.internet.mgmt.mib-2.system: 1.3.6.1.2.1.1 sysname,sysDescription,sysObjectID,sysContact,sysLocation sysClass,sysVendor,sysOs,sysModel
get	IP addresses info	iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable.ipAddrEntry: 1.3.6.1.2.1.4.20.1
get	Interfaces info	iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry: 1.3.6.1.2.1.2.2.1
get	Routes info	iso.org.dod.internet.mgmt.mib-2.ip.ipRouteTable.ipRouteEntry: 1.3.6.1.2.1.4.21.1
get	Bridges info	iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dBase.dot1dBaseBridgeAddress: 1.3.6.1.2.1.17.1.1

Hosts by Shell using NSLOOKUP on DNS Server

The job discovers hosts by querying all available DNS servers.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Getting server and domain info	nslookup - echo exit
exec	Getting DNS info	nslookup {DNSServerName} ls -d {DNSServerName}

TCP Ports

The job discover open tcp\udp ports on a host of known server ports.

There are no permissions required for this job.

Network - Basic

Class C IPs by ICMP

The job performs an IP ping sweep on class C networks.

There are no permissions required for this job.

DNS Resolver

The job discover DNS names on IPs and hosts.

There are no permissions required for this job.

Host Connection by SNMP

The job discovers SNMP agents by trying to connect to a machine using the SNMP protocol, updates the correct host class (Windows, UNIX, router, and so on) according to the relevant OID.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	IP addresses and Networks info	iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable.ipAddrEntry: 1.3.6.1.2.1.4.20.1
get	Interfaces info	iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry: 1.3.6.1.2.1.2.2.1
get	System table info	iso.org.dod.internet.mgmt.mib-2.system: 1.3.6.1.2.1.1 sysname,sysDescription,sysObjectID,sysContact,sysLocation sysClass,sysVendor,sysOs,sysModel

Host Connection by Shell

The job establishes a Shell connection to remote machines. Discovery tries to connect to remote machines through the SSH, Telnet, and NTCmd protocols until the first valid connection is found.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Discover Basic Host Info	hostname UNIX: domainname
exec	Discover OS version info	Windows: ver AIX: oslevel -r UNIX: uname *

exec	Discover Host boot time info	Windows: wmic OS Get LastBootUpTime /format:list < %SystemRoot%\win.ini Windows: net stats srv Windows: reg query "HKCU\Control Panel\International" /v sShortDate UNIX: uptime UNIX: date '+%Y-%m-%d'
exec	Discover network interfaces and IPs info	UNIX: ifconfig -a Windows: ipconfig /all AIX: lscfg | grep ent AIX: lsdev -Cc adapter -S | egrep ^ent AIX: entstat * HPUX: lanscan HPUX: netstat -i SunOS: netstat -np
exec	Discover Virtualization Info	AIX LPARS: lparstat -i | grep "Partition Number" AIX LPARS: prtconf | grep "LPAR Info" IBM HMC: lshmc -V -n Solaris Zones: ps -o zone
exec	Discover Host Serial Number info	AIX: lsattr -El sys0 -a systemid SunOS and Linux: hostid
exec	Discover Host Manufacture Info	SunOS: showrev
exec	Discover Host HW Architecture Info	SunOS: prtdiag
exec	Discover system locale and code page info	Windows: chcp UNIX: locale
exec	DiscoverHost Bios UUID	UNIX: dmidecode

Host Connection by WMI

The job this pattern discovers WMI agents by trying to connect to a Windows machine using the WMI protocol as well as updating the correct host class (Windows, UNIX, router, and so on).

Protocol: WMI

Operation	Usage description	Objects and parameters
select	Obtains basic host information	root\cimv2 Win32_ComputerSystem Win32_NetworkAdapterConfiguration Win32_OperatingSystem Win32_SystemEnclosure

Range IPs by ICMP

The job this pattern performs an IP ping sweep on probe range(s).

There are no permissions required for this job.

Network - Credentialess Discovery

Host Fingerprint using nmap

The job this pattern discovers hosts, IPs, open TCP and UDP ports, and host operating systems using nmap.exe.

There are no permissions required for this job.

Hosts using NSLookup on Probe

The job discover hosts using NSLOOKUP command on probe machine's shell.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Getting server and domain info	nslookup echo exit
exec	Getting DNS info	nslookup {DNSServerName} ls -d {DNSServerName}

MS Domains

The job discovers Microsoft Domains, same as: My Network Places->Entire Network.

There are no permissions required for this job.

MS Domains Topology

The job discovers hosts on Microsoft Domain.

There are no permissions required for this job.

Network - Host Resources and Applications

Host Resources and Applications by SNMP

The job discovers host resources and software elements.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	Process info	iso. org. dod. internet. mgmt. mib-2. host. hrSWRun. hrSWRunTable. hrSWRunEntry: 1.3.6.1.2.1.25.4.2.1
get	Network Services Info	iso.org.dod.internet.private.enterprises.lanmanager.lanmgr-2.server.svSvcTable.svSvcEntry: 1.3.6.1.4.1.77.1.2.3.1
get	Installed Software Info	iso. org. dod. internet. mgmt. mib-2. host. hrSWInstalled. hrSWInstalledTable. hrSWInstalledEntry. hrSWInstalledIndex: 1.3.6.1.2.1.25.6.3.1.1
get	Users Info	iso. org. dod. internet. private. enterprises. lanmanager. lanmgr-2. server. svUserTable. svUserEntry: 1.3.6.1.4.1.77.1.2.25.1
get	Disks Info	iso. org. dod. internet. mgmt. mib-2. host. hrStorage. hrStorageTable. hrStorageEntry: 1.3.6.1.2.1.25.2.3.1
get	Discover TCP Connections Info	1.3.6.1.2.1.6.13.1.1,.1.3.6.1.2.1.6.13.1.2

Host Resources and Applications by Shell

The job discovers host resources, process connectivity and software elements on UNIX and Windows machines using SSH, Telnet and NTCMD protocols.

Protocol: Shell

Operation	Usage description	Objects and parameters
copy	Copy file to remote machine	diskinfo.exe - Gathers information about hard disk getfilever.vbs - Visual Basic script for file version discovery meminfo.exe - Information about random access memory processlist.exe - Prints list of current running processes reg_mam.exe - Console registry tool for Windows
exec	Basic login	ver uname

exec	CPU Info	AIX: prtconf | grep "proc" AIX: lsattr | grep "proc" FreeBSD: sysctl hw.model hw.ncpu hw.clockrate FreeBSD: dmesg | grep -A 1 "CPU:" | grep "cpu|Multiprocessor" HPUX: model HPUX: echo itick_per_usec/D | /usr/bin/adb -k /stand/vmunix /dev/kmem | /usr/bin/tail -n 1 SunOS: /usr/sbin/psrinfo -v SunOS: prtconf Linux: cat /proc/cpuinfo Windows: reg query HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor /S
exec	Memory Info	AIX: prtconf | grep \'^Memory\' | awk \'{print $1,$3,$4}\' AIX: swap -s FreeBSD: sysctl hw.physmem FreeBSD: dmesg | grep \'real memory\' FreeBSD: swapinfo -m HPUX: echo "selclass qualifier memory;info;wait;infolog" | cstm | grep "Total Configured Memory" HPUX: grep Physical /var/adm/syslog/syslog.log HPUX: swapinfo -tm | grep total SunOS: prtconf SunOS: swap -m Linux: free -l Windows: meminfo.exe Windows: wmic MEMORYCHIP get Capacity /format:csv < %SystemRoot%\win.ini PAGEFILESET GET MaximumSize /format:list < %SystemRoot%\win.ini
exec	Disks info	UNIX: df -P -k -k | awk \'{print $1,$2,$3,$4,$5,$6}\' Windows: diskinfo.exe Windows: wmic wmic logicaldisk get deviceId,size,freespace,driveType /format:csv < %SystemRoot%\win.ini
exec	Users info	UNIX: cat /etc/passwd
exec	Processes info	UNIX (not SunOS): ps -e -o 'user,pid,time,args' -ef -ax -o pid,uid,user,cputime,command -eo user,pid,lstart,command --cols 2048 --no-headers SunOS: uname -r SunOS: zonename SunOS: ps -e -o pid -o zone -agxwwu Windows: processlist.exe Windows: wmic process get commandLine,creationdate,executablepath,name,processId /format:csv < %SystemRoot%\win.ini SunOs: pkgchk -l -p

exec	Installed Software info	UNIX: lslpp -Lc -q UNIX: pkg_info -a -I UNIX: swlist UNIX: rpm -qa --qf '%{NAME}~%{VERSION}~%{GROUP}~%{VENDOR}\\n' UNIX: pkginfo -l Windows: reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall /S
exec	Windows Services	Windows: reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services /S
exec	Discover TCP Connections Info	Windows (before XP) and UNIX: netstat -na Windows (XP Onwards), Includes process to port info: netstat -noa Linux, Includes process to port info: netstat -nap AIX, HPUX, SunOS, Includes process to port info: lsof -i -P -n SunOS, only process to port info: pfiles for i in `ps -e|awk '{print $1}'`; do echo __[$i]; pfiles $i | grep 'sockname: AF_INET'; done

Host Resources and Applications by WMI

The job this pattern discovers host resources and software elements on Windows machines using WMI protocol.

Protocol: WMI

Operation	Usage description	Objects and parameters
select	CPU Info	root\cimv2 Win32_Processor
select	Disks Info	root\cimv2 Win32_LogicalDisk
select	Memory Info	root\cimv2 Win32_OperatingSystem Win32_PageFileSetting
select	Processes Info	root\cimv2 Win32_Process
select	Windows Services	root\cimv2 Win32_Service
select	Shared Folders	root\cimv2 Win32_ShareToDirectory
select	Users info	root\cimv2 Win32_ComputerSystem Win32_UserAccount
exec	Installed Software info	Windows: root\DEFAULT StdRegProv:EnumKey() StdRegProv:EnumValues()
select	Installed Software info	root\cimv2 Win32_Product

Software Element CF by Shell

The job application configuration files.

There are no permissions required for this job.

Network - Layer2

Host Networking by SNMP

The job discovers host networking topology using SNMP route and system tables.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	System table info	iso.org.dod.internet.mgmt.mib-2.system: 1.3.6.1.2.1.1 sysname,sysDescription,sysObjectID,sysContact,sysLocation sysClass,sysVendor,sysOs,sysModel
get	IP addresses info	iso.org.dod.internet.mgmt.mib-2.ip.ipAddrTable.ipAddrEntry: 1.3.6.1.2.1.4.20.1
get	Interfaces info	iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry: 1.3.6.1.2.1.2.2.1
get	Routes info	iso.org.dod.internet.mgmt.mib-2.ip.ipRouteTable.ipRouteEntry: 1.3.6.1.2.1.4.21.1
get	Bridges info	iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dBase.dot1dBaseBridgeAddress: 1.3.6.1.2.1.17.1.1

Layer2 Enrichment

The job this pattern removes layer 2 links between Physical Port and Interface with inappropriate mac address.

There are no permissions required for this job.

Layer2 Topology Bridge based by SNMP

The job this pattern discovers the Layer 2 topology of a switch by SNMP.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	Interfaces info	iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry: 1.3.6.1.2.1.2.2.1
get	STP Port info	iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dStp.dot1dStpPortTable.dot1dStpPortEntry: 1.3.6.1.2.1.17.2.15.1
get	Bridges info	iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dBase: 1.3.6.1.2.1.17.1
get	Bribge unicast MAC address info	iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dTp.dot1dTpFdbTable.dot1dTpFdbEntry: 1.3.6.1.2.1.17.4.3.1
get	Additional interface info	iso.org.dod.internet.mgmt.mib-2.ifMIB.ifMIBObjects.ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1

Layer2 Topology VLAN based by SNMP

The job this pattern discovers the Layer 2 topology of a specific VLAN by SNMP.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	Interface info	iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry: 1.3.6.1.2.1.2.2.1
get	STP Port info	iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dStp.dot1dStpPortTable.dot1dStpPortEntry: 1.3.6.1.2.1.17.2.15.1
get	Bridges info	iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dBase: 1.3.6.1.2.1.17.1
get	Bribge unicast MAC address info	iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dTp.dot1dTpFdbTable.dot1dTpFdbEntry: 1.3.6.1.2.1.17.4.3.1
get	Additional interface info	iso.org.dod.internet.mgmt.mib-2.ifMIB.ifMIBObjects.ifXTable.ifXEntry: 1.3.6.1.2.1.31.1.1.1

VLAN ports by SNMP

The job discovers the physical ports on a VLAN.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	Bridges, Physical ports, Bridging type	iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dBase: 1.3.6.1.2.1.17.1

VLANs by SNMP

The job this pattern discovers VLANs on a switch by SNMP.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	VLAN info	iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoVtpMIB.vtpMIBObjects.vlanInfo.vtpVlanTable.vtpVlanEntry: 1.3.6.1.4.1.9.9.46.1.3.1.1
get	Correlation between a LAN Emulation client and the VLAN that it extends.	iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoLecExtMIB.ciscoLecExtMIBObjects.cLecExtVlan.cLecToVlanTable.cLecToVlanEntry: 1.3.6.1.4.1.9.9.77.1.1.1.1
get	LAN Emulation Client info	iso.org.dod.internet.private.enterprises.atmForum.atmForumNetworkManagement.leClientMIB.leClientMIBObjects.lecStatusTable.lecStatusEntry: 1.3.6.1.4.1.353.5.3.1.1.2.1

Network - Load Balancer

Alteon application switch by SNMP

The job this pattern discovers Nortel Application Switches via SNMP.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	Virtual Servers	iso.org.dod.internet.private.enterprises.alteon.private-mibs.aws-switch.layer4.layer4Configs.slbCfg.virtualServerCfg.slbCurCfgVirtServerTable.slbCurCfgVirtualServerEntry: 1.3.6.1.4.1.1872.2.5.4.1.1.4.2.1
get	Virtual Services	iso.org.dod.internet.private.enterprises.alteon.private-mibs.aws-switch.layer4.layer4Configs.slbCfg.virtualServerCfg.slbCurCfgVirtServicesTable.slbCurCfgVirtServicesEntry: 1.3.6.1.4.1.1872.2.5.4.1.1.4.5.1
get	Real Server Groups	iso.org.dod.internet.private.enterprises.alteon.private-mibs.aws-switch.layer4.layer4Configs.slbCfg.realServerGroupCfg.slbCurCfgGroupTable.slbCurCfgGroupEntry: 1.3.6.1.4.1.1872.2.5.4.1.1.3.3.1
get	Real Servers	iso.org.dod.internet.private.enterprises.alteon.private-mibs.aws-switch.layer4.layer4Configs.slbCfg.realServerCfg.slbCurCfgRealServerTable.slbCurCfgRealServerEntry: 1.3.6.1.4.1.1872.2.5.4.1.1.2.2.1
get	Real Server Port	iso.org.dod.internet.private.enterprises.alteon.private-mibs.aws-switch.layer4.layer4Configs.slbCfg.realServerCfg.slbCurCfgRealServPortTable.slbCurCfgRealServPortEntry: 1.3.6.1.4.1.1872.2.5.4.1.1.2.5.1
get	Ports	iso.org.dod.internet.private.enterprises.alteon.private-mibs.aws-switch.layer4.layer4Configs.slbCfg.portCfg.slbCurCfgPortTable.slbCurCfgPortEntry: 1.3.6.1.4.1.1872.2.5.4.1.1.5.2.1

Cisco CSS by SNMP

The job cisco CSS (Content Services Switch) by SNMP.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	Content rules	iso.org.dod.internet.private.enterprises.arrowPoint.apMgmt.cntExt.apCntTable.apCntEntry: 1.3.6.1.4.1.2467.1.16.4.1 iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.arrowPoint.apMgmt.cntExt: 1.3.6.1.4.1.9.9.368.1.16.4.1
get	Content providing service	iso.org.dod.internet.private.enterprises.arrowPoint.apMgmt.svcExt.apSvcTable.apSvcEntry: 1.3.6.1.4.1.2467.1.15.2.1 iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.arrowPoint.apMgmt.svcExt: 1.3.6.1.4.1.9.9.368.1.15.2.1

get	Connection between content rules and content providing service	iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.arrowPoint.apMgmt.cntsvcExt: 1.3.6.1.4.1.9.9.368.1.18.2.1 iso.org.dod.internet.private.enterprises.arrowPoint.apMgmt.cntsvcExt.apCntsvcTable.apCntsvcEntry: 1.3.6.1.4.1.2467.1.18.2.1

F5 BIG-IP LTM by SNMP

The job this pattern discovers F5 BIG-IP Local Traffic Manager using SNMP protocol.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	General information about F5 LTM	iso.org.dod.internet.private.enterprises.f5.bigipTrafficMgmt.bigipSystem.sysProduct: 1.3.6.1.4.1.3375.2.1.4
get	Virtual servers	iso.org.dod.internet.private.enterprises.f5.bigipTrafficMgmt.bigipLocalTM.ltmVirtualServers.ltmVirtualServ.ltmVirtualServTable.ltmVirtualServEntry: 1.3.6.1.4.1.3375.2.2.10.1.2.1
get	Pools	iso.org.dod.internet.private.enterprises.f5.bigipTrafficMgmt.bigipLocalTM.ltmPools.ltmPool.ltmPoolTable.ltmPoolEntry: 1.3.6.1.4.1.3375.2.2.5.1.2.1
get	Virtual server to Pool connection	iso.org.dod.internet.private.enterprises.f5.bigipTrafficMgmt.bigipLocalTM.ltmVirtualServers.ltmVirtualServPool.ltmVirtualServPoolTable.ltmVirtualServPoolEntry: 1.3.6.1.4.1.3375.2.2.10.6.2.1
get	Pool members	iso.org.dod.internet.private.enterprises.f5.bigipTrafficMgmt.bigipLocalTM.ltmPools.ltmPoolMember.ltmPoolMemberTable.ltmPoolMemberEntry: 1.3.6.1.4.1.3375.2.2.5.3.2.1
get	Connection between Rules and Virtual servers	iso.org.dod.internet.private.enterprises.f5.bigipTrafficMgmt.bigipLocalTM.ltmVirtualServers.ltmVirtualServRule.ltmVirtualServRuleTable.ltmVirtualServRuleEntry: 1.3.6.1.4.1.3375.2.2.10.8.2.1
get	Rules	iso.org.dod.internet.private.enterprises.f5.bigipTrafficMgmt.bigipLocalTM.ltmRules.ltmRule.ltmRuleTable.ltmRuleEntry: 1.3.6.1.4.1.3375.2.2.8.1.2.1

Network - Mainframe

Mainframe TCP by SNMP

The job this pattern discovers IBM mainframe.

There are no permissions required for this job.

Mainframe topology by SNMP

The job this pattern discovers IBM mainframe topology.

There are no permissions required for this job.

Network - Obsolete

Collect Network Data by Shell or SNMP

The job this job is obsolete. Activate Host Resources By Shell/SNMP/WMI instead.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic login	ver uname
exec	Discover TCP Connections Info	Windows (before XP) and UNIX: netstat -na Windows (XP Onwards), Includes process to port info: netstat -noa Linux, Includes process to port info: netstat -nap AIX, HPUX, SunOS, Includes process to port info: lsof -i -P -n SunOS, only process to port info: pfiles for i in `ps -e|awk '{print $1}'`; do echo __[$i]; pfiles $i | grep 'sockname: AF_INET'; done

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	Discover TCP Connections Info	1.3.6.1.2.1.6.13.1.1,.1.3.6.1.2.1.6.13.1.2

Network - SolarisZone

Solaris Zones by TTY

The job this pattern discovers Solaris Zones architecture by SSH and Telnet protocols. This pattern also discovers the global zone and all its related zones (treated as hosts) and their related shared resources such as disks and network interfaces.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic login	ver uname
exec	Find all predefined zones	uname -r zoneadm list -c
exec	Get zones resources	zonecfg -z {ZONE_NAME} info Resolve macaddresses: ifconfig

Network Connections - Active Discovery

IP Traffic by Network Data

The job discovers the IP Communication patterns - which IPs communicte and the top interesting ports for these communication channels.
Brings data from DDM database.

There are no permissions required for this job.

Server Ports by Network Data

The job discover listening ports on network according to portNumberToPortName.xml configuration file.
Brings data from DDM database.

There are no permissions required for this job.

Network Connections - Passive Discovery

Collect Network Data by NetFlow

The job this pattern listens to NetFlow data broadcasts and writes the data to the Probe database, where the data is aggregated and made available for the following patterns:
Potential Services by TCP DB, Services Connections by TCP DB, and Services by TCP DB.

There are no permissions required for this job.

IP Traffic by Network Data

The job discovers the IP Communication patterns - which IPs communicte and the top interesting ports for these communication channels.
Brings data from DDM database.

There are no permissions required for this job.

Potential Servers by Network Data

The job the job tries to identify servers by network trafic data or number of clients.
Brings data from DDM database.

There are no permissions required for this job.

Servers by Network Data

The job discover key services on the network according to portNumberToPortName.xml configuration file.
Brings data from DDM database.

There are no permissions required for this job.

Virtualization - VMware

Manual VMware VIM Connection

The job pattern discovers the VMware Server connection using Virtual Infrastructure Management protocol. It is activated manually and it uses the URL string parameter for connection.

Protocol: VMWare

Operation	Usage description	Objects and parameters
exec	Get properties of VMware server (VirtualCenter or ESX) we connected to.	ServiceContent: AboutInfo
exec	Get UUID of ESX server (requires System.Read permission)	HostSystem: summary.hardware.uuid

VMware ESX Connection by VIM

The job pattern discovers VMware ESX Servers running on Unix hosts.

Protocol: VMWare

Operation	Usage description	Objects and parameters
exec	Get properties of VMware ESX server we connected to.	ServiceContent: AboutInfo
exec	Get UUID of ESX server (requires System.Read permission)	HostSystem: summary.hardware.uuid

VMware ESX Topology by VIM

The job this pattern discovers VMware ESX Servers using VIM protocol.

Protocol: VMWare

Operation	Usage description	Objects and parameters
exec	Get licenses availability information (requries Global.Licenses permission) for ESX server	LicenseManager: queryLicenseSourceAvailability
exec	Get licenses usage information for ESX server (requires System.Read permission)	LicenseManager: queryLicenseUsage
exec	Get ComputeResource of ESX server we conected to along with its properties (requires System.Read permission)	ComputeResource: name ComputeResource: resourcePool ComputeResource: configStatus
exec	Get all ResourcePools along with their properties (requires System.Read permission)	ResourcePool: configStatus ResourcePool: name ResourcePool: config ResourcePool: vm ResourcePool: parent

exec	Get HostSystem of this ESX servers along with its properties (requires System.Read permission)	HostSystem: config.network.dnsConfig HostSystem: vm HostSystem: configStatus HostSystem: runtime.connectionState HostSystem: name HostSystem: config.product HostSystem: summary
exec	Get all VirtualMachines along with their properties (requires System.Read permission)	VirtualMachine: configStatus VirtualMachine: name VirtualMachine: config VirtualMachine: runtime VirtualMachine: guest

VMware VMotion Monitor by VIM

The job pattern monitors migration events of Virtual Machines from one host to another.

Protocol: VMWare

Operation	Usage description	Objects and parameters
exec	Get custom HostSystems(ESX servers) along with their properties(requires System.Read permission)	HostSystem config.network.dnsConfig config.product configStatus name runtime.connectionState summary vm
exec	Get custom VirtualMachines along with their properties(requires System.Read permission)	VirtualMachine config configStatus guest name runtime

VMware VirtualCenter Connection by WMI and VIM

The job pattern discovers the VMware VirtualCenter connection using Virtual Infrastructure Management protocol. If VIM port is specified in credentials, this port will be used. Otherwise it tries to connect to host using WMI protocol and retrieves the VirtualCenter's port information from registry. The retrieved information is used to generate the connection URL.

Protocol: WMI

Operation	Usage description	Objects and parameters
select	Query for VirtualCenter port number in registry	HKLM\SOFTWARE\VMware, Inc.\VMware VirtualCenter: HttpsProxyPort HKLM\SOFTWARE\VMware, Inc.\VMware VirtualCenter: HttpProxyPort

Protocol: VMWare

Operation	Usage description	Objects and parameters
exec	Get properties of VMware VirtualCenter server we connected to.	ServiceContent: AboutInfo

VMware VirtualCenter Topology by VIM

The job pattern collects Virtual Infrastructure topology information using Virtual Center Server by VI Management protocol.

Protocol: VMWare

Operation	Usage description	Objects and parameters
exec	Get all Datacenters along with their properies (requires System.Read permission)	Datacenter: name Datacenter: hostFolder Datacenter: configStatus Datacenter: vmFolder
exec	Get licenses availability information (requries Global.Licenses permission) for VMware server (VirtualCenter or ESX)	LicenseManager: queryLicenseSourceAvailability
exec	Get licenses usage information for VMware server (VirtualCenter or ESX, requires System.Read permission)	LicenseManager: queryLicenseUsage
exec	Get all ComputeResources along with their properties (requires System.Read permission)	ComputeResource: name ClusterComputeResource: summary ComputeResource: resourcePool ClusterComputeResource (2.5): configurationEx ClusterComputeResource (2.0): configuration ComputeResource: configStatus
exec	Get all ResourcePools along with their properties (requires System.Read permission)	ResourcePool: configStatus ResourcePool: name ResourcePool: config ResourcePool: vm ResourcePool: parent
exec	Get all HostSystems (ESX servers) along with their properties (requires System.Read permission)	HostSystem: config.network.dnsConfig HostSystem: vm HostSystem: configStatus HostSystem: runtime.connectionState HostSystem: name HostSystem: config.product HostSystem: summary
exec	Get all VirtualMachines along with their properties (requires System.Read permission)	VirtualMachine: configStatus VirtualMachine: name VirtualMachine: config VirtualMachine: runtime VirtualMachine: guest

Web Servers - Apache Tomcat

Apache Tomcat by Shell

The job this pattern discovers Apache Tomcat Web Server.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic login	uname ver
exec	Discover Apache Tomcat Topology	cscript.exe adsutil.vbs ENUM "MSFTPSVC/{SITENUM}root" adsutil.vbs ENUM "W3SVC" adsutil.vbs ENUM "W3SVC/AppPools" adsutil.vbs ENUM "W3SVC/AppPools/{POOLNAME}" adsutil.vbs ENUM "W3SVC/{SITENUM}" adsutil.vbs ENUM "W3SVC/{SITENUM}/root" adsutil.vbs ENUM /p MSFTPSVC adsutil.vbs ENUM /p MSFTPSVC/{SITENUM}/Root adsutil.vbs ENUM /p W3SVC adsutil.vbs ENUM /p W3SVC/AppPools adsutil.vbs ENUM MSFTPSVC adsutil.vbs ENUM MSFTPSVC/{SITENUM} adsutil.vbs ENUM SMTPSVC adsutil.vbs GET "{PATH}/KeyType" adsutil.vbs GET MSFTPSVC/{SITENUM}/Root/{PATH}/KeyType adsutil.vbs GET MaxBandwidth adsutil.vbs GET MaxBandwidth dir /B hostname

Web Servers - Basic

WebServer Detection using TCP Ports

The job this pattern discovers Web servers using TCP ports.

There are no permissions required for this job.

Webserver by Shell

The job this pattern discovers Apache Web servers by Shell.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic Login	ver uname
exec	Checking existence of file(s) in given path	Windows: dir {FILE_PATH} /B /A-D {FOLDER_PATH} /B /AD {FOLDER_PATH} Windows: type {FILE_PATH} {APACHE_INSTALL_DIR}\version.signature | find i "ibm http server" UNIX: ls {FILE_PATH} -lA {FOLDER_PATH} UNIX: cat {FILE_PATH}
exec	Get Apache compile-time variables	{apache executable} -V
exec	Query registry in order to get Apache ServerRoot	Windows: reg query "HKLM\SOFTWARE\Apache Software Foundation\Apache" /s query "HKCU\SOFTWARE\Apache Software Foundation\Apache" /s

Web Servers - IHS

IHS Websphere Plugin by Shell

The job discovers IBM Http Server's WebSphere plugin configuration by parsing the IHS plugin configuration file.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic Login	ver uname
exec	Fetching configuration file content	Windows: type {FILE_PATH} | grep "[<=>]" UNIX: cat {FILE_PATH} | grep "[<=>]"

Web Servers - IIS

IIS Applications by NTCMD

The job this pattern discovers Microsoft Internet Information Services (IIS).

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic login	ver uname
copy	Copy file to remote machine	adsutil.vbs - Visual Basic script for IIS discovery
exec	Discover IIS Topology	cscript.exe adsutil.vbs ENUM "MSFTPSVC/{SITENUM}root" adsutil.vbs ENUM "W3SVC" adsutil.vbs ENUM "W3SVC/AppPools" adsutil.vbs ENUM "W3SVC/AppPools/{POOLNAME}" adsutil.vbs ENUM "W3SVC/{SITENUM}" adsutil.vbs ENUM "W3SVC/{SITENUM}/root" adsutil.vbs ENUM /p MSFTPSVC adsutil.vbs ENUM /p MSFTPSVC/{SITENUM}/Root adsutil.vbs ENUM /p W3SVC adsutil.vbs ENUM /p W3SVC/AppPools adsutil.vbs ENUM MSFTPSVC adsutil.vbs ENUM MSFTPSVC/{SITENUM} adsutil.vbs ENUM SMTPSVC adsutil.vbs GET "{PATH}/KeyType" adsutil.vbs GET MSFTPSVC/{SITENUM}/Root/{PATH}/KeyType adsutil.vbs GET MaxBandwidth adsutil.vbs GET KeyType dir /B hostname

WebServices by URL

The job discovers the Webservice topology by reading WSDL content from a given URL.

There are no permissions required for this job.