



# **Configuration Management System (CMS)**

Software Version: Content Pack 28.00 (CP28)

## **Discovery and Integration Content Permissions**

Document Release Date: August 2018  
Software Release Date: August 2018



## Commands that Require Elevated Privileges

The following commands require elevated privileges to properly discover environments on UNIX systems:

- ifconfig (to discover details about network configuration)
- dmidecode
- machinfo
- ps
- lsof
- pfiles

# Application - Active Directory

## Active Directory Connection by LDAP

The job discover the existence of Active Directory Domain Controllers 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
select	Get domain controllers (<baseDn_job_parameter>,<domain_dn>)	computer dNSHostName serverReferenceBL
select	Get controller version (CN=Schema,<configurationNamingContext>)	object objectVersion

## 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
select	Get sites (CN=Sites,<configurationNamingContext>)	site name siteObjectBL
select	Get servers per site (CN=Servers,CN=<site_name>,CN=Sites,<configurationNamingContext>)	applicationSettings dNSHostName name objectClass options server dNSHostName distinguishedName name objectClass options
select	Get subnets (CN=Subnets,CN=Sites,<configurationNamingContext>)	subnet description name siteObject
select	Get inter-site transports (CN=Inter-Site Transports,CN=Sites,<configurationNamingContext>)	interSiteTransport name

select	Get site-links (CN=<site_link_name>),CN=Inter-Site Transports,CN=Sites,<configurationNamingContext>)	siteLink cost name replInterval siteList
select	Find out whether controller serves as RID manager (CN=RID Manager\$,CN=System,<domain_dn>)	object fsmoroleowner
select	Find out whether controller serves as schema master (<schemaNamingContext>)	object fsmoroleowner
select	Find out whether controller serves as infrastructure master (CN=Infrastructure,<defaultNamingContext>)	object fsmoroleowner
select	Find out whether controller serves as PDC Emulator (<defaultNamingContext>)	object fsmoroleowner
select	Find out whether controller serves as domainname master (CN=Partitions,<configurationNamingContext>)	object fsmoroleowner
select	Get domain	domain description name
select	Get domain controllers (<baseDn_job_parameter>,<domain_dn>)	computer dNSHostName serverReferenceBL
select	Get controller version (CN=Schema,<configurationNamingContext>)	object objectVersion
select	Get organizational units (OU)	organizationalUnit description ou

# Application - Cisco

## Cisco Prime by Web Services

The job this adapter discovers nodes, interfaces, net devices, and layer2 connections on a Cisco Prime.

Protocol: HTTP

Operation	Usage description	Objects and parameters
GET	It provides an aggregated view of all the available inventory information for the device.	InventoryDetails

## Application - Microsoft Exchange

### Microsoft Exchange Connection by NTCMD or UDA

The job this adapter discovers Microsoft Exchange by NTCMD or UDA protocol. It is based on executing of 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
exec	Windows version	ver
exec	Execute command	cmd /c "<command>" powershell
exec	Code page and language information	wmic OS Get CodeSet OS Get OSLanguage
exec	File manipulation	rd <folder_path> cd <folder_path> dir <folder_path> /O:-D

### Microsoft Exchange Connection by WMI

The job connects to the 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 adapter discovers Microsoft Exchange topology using information stored in Active Directory.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Set code page	chcp <code_page>

Protocol: LDAP

Operation	Usage description	Objects and parameters
query	Get Exchange Organizations	CN=Microsoft Exchange,CN=Services (objectClass=msExchOrganizationContainer) (objectClass=msExchMDB) (objectClass=msExchMDBCopY)
query	Get Exchange Site configuration	CN=Sites,CN=Configuration (objectClass=site)
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
exec	resolve server's FQDN using remote DNS	nslookup <Server FQDN> <Remote DNS>

## Microsoft Exchange Topology by NTCMD or UDA

The job this adapter discovers Microsoft Exchange topology by NTCMD or UDA protocol. It is based on executing of PowerShell scenario on the remote machine.

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
exec	Discover basic information about the host	ver wmic OS Get CodeSet wmic OS Get OSLanguage
exec	Execute command	cmd /c "<command>" powershell
exec	List specific folder	dir <folder> /O:-D

Protocol: PowerShell

Operation	Usage description	Objects and parameters
Exchange View-Only Administrator	Get Exchange server properties	Get-ExchangeServer
Exchange View-Only Administrator	Get Clustered Mailbox properties	Get-ClusteredMailboxServerStatus
PowerShell Usage	Load Exchange PowerShell Snap-In	Add-PSSnapin

## Microsoft Exchange Topology by PowerShell

The job this adapter discovers Microsoft Exchange by PowerShell protocol. It is based on executing Exchange native cmdlets.

Protocol: shell

Operation	Usage description	Objects and parameters
exec	General commands execution	ver hostname wmic OS Get CodeSet OS Get OSLanguage
exec	Exchange parameters	Get-ExchangeServer



exec	Import commandlets Exchange 2007	Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin
exec	Import commandlets Exchange 2010	Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010
exec	Get server name for clustered deployment	Get-ClusteredMailboxServerStatus.ClusteredMailboxServerName
exec	Exchange 2010 DAG configuration	Get-DatabaseAvailabilityGroup
exec	AD additional information	Get-ADServerSettings

## 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 - Microsoft MQ

## Active Directory Connection by LDAP

The job discover the existence of Active Directory Domain Controllers 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
select	Get domain controllers (<baseDn_job_parameter>,<domain_dn>)	computer dNSHostName serverReferenceBL
select	Get controller version (CN=Schema,<configurationNamingContext>)	object objectVersion

## Microsoft Message Queue Topology by LDAP

The job discovery adapter for Microsoft MQ server. Used to retrieve Active Directory side information of MS MQ topology.

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
select	Get servers per site (CN=Servers,CN=<site_name>,CN=Sites,<configurationNamingContext>)	server name distinguishedName
select	Get sites (CN=Sites,<configurationNamingContext>)	site name siteObjectBL distinguishedName
select	Get MQ name (CN=<host_name>,CN=Servers,CN=<site_name>,CN=Sites,<configurationNamingContext>)	mSMQSettings name

## Microsoft Message Queue Topology by NTCMD or UDA or PowerCmd

The job discovery adapter for Microsoft MQ server side. Uses NTCMD or UDA or PowerCmd protocol in order to retrieve queues, triggers and rules related data.

Protocol: SHELL

Operation	Usage description	Objects and parameters
exec	Registry access	Read MQ Triggers and Parameters Information: reg.exe HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters /v StoreReliablePath HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Triggers\Data\Rules\ /S HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Triggers\Data\Triggers\ /S
exec	Get the locale/codeset information	wmic OS
exec	Windows version	ver
exec	File system access	dir /B /A:-D <MSMQ Queue config Folder>  type <Path to MSMQ Queue config file>
exec	Job can execute nslookup for resolving host IP address	nslookup <hostname   FQDN>

# Application - Microsoft SharePoint

## Microsoft SharePoint Topology

The job adapter contains mechanism of MS SharePoint topology discovery.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Script execution policy should be at least 'RemoteSigned'	powershell script Sharepoint_xml.ps1
exec	Execute command	cmd /c "<command>"  powershell
copy	Copy file to remote machine	PowerShell script for SharePoint discovery: Sharepoint_xml.ps1

Protocol: PowerShell

Operation	Usage description	Objects and parameters
Import-Module	Load SharePoint library	Microsoft.SharePoint.dll
Instantiate	used SharePoint lib requires connection to config database	[Microsoft.SharePoint.Administration.SPFarm]::Local

# Application - Oracle E-Business Suite

## Oracle Applications by SQL

The job this adapter 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_DEPENDENCIES FND_APPLICATION_VL FND_PRODUCT_INSTALLATIONS
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,SY SU, SEU_COMPONENT  Create XMI Session: S_XMI_PROD EXTCOMPANY=MERCURY;EXTPRODUCT=D ARM;INTERFACE=XAL
select	Querying SAP System	Table Maintenance: S_TABU_DIS DICBERCLS=SS;DICBERCLS=SC;DICBERCLS =&NC&
select	Querying TMS manager	TSMCONF DOMNAM, DOMTXT, SYSNAM, SYSTXT, DOMCTL, CTLTXT
select	Query to determine Solution Manager	SMSY_SYSTEM_SAP SYSTEMNAME

## 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,SY SU, SEU_COMPONENT, DB6_DIAG_GET_SYSTEM_BASICS  Create XMI Session: S_XMI_PROD EXTCOMPANY=MERCURY;EXTPRODUCT=D ARM;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 SAP environment based on Computer Center Management System (CCMS).  
Discovery process can take up to several hours in case long period of time is defined for transaction changes (the 'from' date to the 'to' date).

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, SY SU, SEU_COMPONENT  Create XMI Session: S_XMI_PROD EXTCOMPANY=MERCURY;EXTPRODUCT=D ARM;INTERFACE=XAL
select	Querying SAP System	Table Maintenance: S_TABU_DIS DICBERCLS=SS;DICBERCLS=SC;DICBERCLS =&NC&

## SAP FRUN Topology by CIM

The job discover SAP Topology based on FRUN with CIM protocol.

Protocol: CIM

Operation	Usage description	Objects and parameters
-----------	-------------------	------------------------

get	classes	SAP_CustomerNetwork SAP_BCSystem SAP_ComputerSystem SAP_BCApplicationServer SAP_BCApplicationServerHost SAP_BCSystemApplicationServer SAP_DatabaseSystem SAP_BCSystemSystemDB SAP_DatabaseInstance SAP_DBSystemInstance SAP_DBInstanceHost SAP_BCClient SAP_BCSystemClient SAP_InstalledSoftwareComponent SAP_InstalledSWComponentOnApplicationSystem SAP_SoftwareComponent SAP_SoftwareComponentType SAP_BCCentralServiceInstance SAP_BCSystemServiceInstance SAP_BCCentralServiceInstanceHost SAP_J2EEEngineCluster SAP_J2EEEngineInstance SAP_J2EEEngineInstanceHost SAP_J2EEEngineClusterInstance SAP_J2EEEngineSystemDB SAP_J2EEEngineServiceInstance
-----	---------	---

## SAP ITS by NTCMD or UDA

The job discover SAP Internet Transaction Server based on parsing configuration files.

Protocol: Shell

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



## SAP Java Topology by HTTP

The job discover SAP J2EE environment based on XML queried by HTTP.

Permissions information is unavailable or no permissions are required.

## SAP Java Topology by SAP JMX

The job discover SAP J2EE environment based on JMX.

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_J2EEClusterNode
select	Get System Development Components	Type=SAP_J2EEServicePerNode  Type=SAP_J2EEInterfacePerNode  Type=SAP_J2EELibraryPerNode

## SAP Java Topology by WebServices

The job discover SAP J2EE environment based on JMX.

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_J2EEClusterNode
select	Get System Development Components	Type=SAP_J2EEServicePerNode Type=SAP_J2EEInterfacePerNode Type=SAP_J2EELibraryPerNode

## SAP Solution Manager Connection by CIM

The job connect to SAP Solution Manager with CIM protocol.

Protocol: CIM

Operation	Usage description	Objects and parameters
get	get always existing class to check connectivity	SAP_ComputerSystem

## SAP Solution Manager Topology by CIM

The job discover SAP Topology based on Solution Manager with CIM protocol.

Protocol: CIM

Operation	Usage description	Objects and parameters
-----------	-------------------	------------------------

get	SAP system related classes	SAP_BCSystem SAP_ComputerSystem SAP_BCApplicationServer SAP_BCApplicationServerHost SAP_BCSystemApplicationServer SAP_DatabaseSystem SAP_BCSystemSystemDB SAP_DatabaseInstance SAP_DBSystemInstance SAP_DBInstanceHost SAP_BCClient SAP_BCSystemClient SAP_InstalledSoftwareComponent SAP_InstalledSWComponentOnApplicationSystem SAP_SoftwareComponent SAP_SoftwareComponentType SAP_BCCentralServiceInstance SAP_BCSystemServiceInstance SAP_BCCentralServiceInstanceHost SAP_J2EEEngineCluster SAP_J2EEEngineInstance SAP_J2EEEngineInstanceHost SAP_J2EEEngineClusterInstance SAP_J2EEEngineSystemDB SAP_J2EEEngineServiceInstance
-----	----------------------------	--

## 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,SY SU, SEU_COMPONENT  Create XMI Session: S_XMI_PROD EXTCOMPANY=MERCURY;EXTPRODUCT=D ARM;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 business layer based on Solution Manager system management suite.

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,SY SU, SEU_COMPONENT  Create XMI Session: S_XMI_PROD EXTCOMPANY=MERCURY;EXTPRODUCT=D ARM;INTERFACE=XAL
select	Querying SAP System	Table Maintenance: S_TABU_DIS DICBERCLS=SS;DICBERCLS=SC;DICBERCLS =&NC&

## SAP TCP Ports

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

Protocol: TCP

Operation	Usage description	Objects and parameters
connect	The probe host must not be blocked by ACL	socket

# 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
exec	Query file last modified time	Windows: wmic datafile where "name='<file_path>' get LastModified /format:list  UNIX: ls <file_path> -lA <folder_path>

## 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	Fetching server components info: srvrmgr.exe list compgrps list comps list comps show SV_NAME, CC_ALIAS list params for component {COMPONENT_NAME}  srvrmgr.exe list param connect list parameter DSConnectionString for named subsystem ServerDataSrc list parameters DSSQLStyle for named subsystem ServerDataSrc list servers show SBLSRVR_NAME, HOST_NAME, INSTALL_DIR, SBLMGR_PID, SV_DISP_STATE, SBLSRVR_STATE, START_TIME, END_TIME, SBLSRVR_STATUS, SV_SRVRID set server {SIBELSERVERNAME} unset server

## Siebel DB by NTCMD or UDA

The job discover DB of odbc connection.

Protocol: Shell

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

## Siebel DB by TTY

The job discover DB of odbc connection.

Protocol: Shell

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

## Siebel Gateway Connection

The job this adapter 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	svrmgr.exe /e {SIEBEL_SITE_NAME} /g {IP} /u {USER} /p {PASSWORD} /k
exec	Gather database related info	svrmgr.exe list advanced params DSSQLStyle for named subsystem ServerDataSrc list parameter DSConnectionString for named subsystem GatewayDataSrc list parameters DSSQLStyle for named subsystem GatewayDataSrc list parameters DSSQLStyle for named subsystem ServerDataSrc

## Siebel Web Applications by NTCMD or UDA

The job this adapter discovers Siebel Webserver Extension and all web applications by NTCMD or UDA 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 - UCS

## Cisco UCS Connection

The job find Cisco UCS.

Protocol: READ

Operation	Usage description	Objects and parameters
READ	Read access of UCS	UCS READ

## Cisco UCS Manual

The job cisco UCS Manual.

Protocol: READ

Operation	Usage description	Objects and parameters
READ	Read access of UCS	UCS READ

## Cisco UCS Topology

The job pull data from Cisco UCS.

Protocol: READ

Operation	Usage description	Objects and parameters
READ	Read access of UCS	UCS READ



## Application - UDDI Registry

### Web Services by URL

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

Permissions information is unavailable or no permissions are required.

### Web Service Connections by UDDI Registry

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

Permissions information is unavailable or no permissions are required.

### Web Services 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 Websphere MQ topology by using SSH, TELNET, NTCMD or UDA.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic login	nslookup <host_name>  type "%SystemRoot%\system32\drivers\etc\hosts"  uname  ver
exec	Get language information	wmic OS Get CodeSet  wmic OS Get OSLanguage
exec	Discover MQ Version and Queue Managers Info	mqver  dspmq  dspmqver
exec	Discover Queue Manager Listen Ports	cat /etc/inetd.conf   grep amqcrsta  ps ef   grep runmqslr efw   grep runmqslr
exec	Discover Queue Managers Info	runmqsc (or runmqadm -f) DISPLAY CHANNEL(*) CHLTYPE,TRPTYPE,DESCR,CLUSTER,CLUSNL,CONNNAME,XMITQ {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  echo DISPLAY NAMELIST(*) NAMES NAMCOUNT DESCR   runmqadm -r <QUEUEMANAGER>  echo DISPLAY NAMELIST(*) NAMES NAMCOUNT DESCR   runmqsc <QUEUEMANAGER>
exec	Discover MQ Cluster Info	runmqsc (or runmqadm -f) {QUEUEMANAGER} \ndisplay clusqmgr(*) all\nend

## **Atrium to UCMDB**

### **Import data from Atrium**

The job import CIs and Relationships from BMC Atrium into UCMDB.

Permissions information is unavailable or no permissions are required.

# Auditing - Oracle LMS

## Oracle LMS CPU Data Collection by Shell

The job this adapter collects data related to CPU, which can then be sent to Oracle LMS organization for Oracle License Review or Audit.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic login	AIX,FreeBSD,HP-UX,Linux,SunOS: locale -a AIX: uname -M AIX,FreeBSD,HP-UX,Linux,SunOS: uname -a Unix: /usr/ios/cli/ioscli uname -L ver Windows: wmic OS Get Caption OS Get CodeSet OS Get OSLanguage path Win32_ComputerSystem get Name /value
exec	Plugins can read file content	Unix: cat <file_name> Windows: type <file_name>
exec	run Oracle LMS CPU scripts	Windows: full administrative permissions Unix: root permissions
upload files	upload file to temp folder	
write file	write permissions	

## Oracle LMS Data Collection by SQL

The job this adapter collects data related to Oracle software usage, which can then be sent to Oracle LMS organization for Oracle License Review or Audit.

Protocol: SQL

Operation	Usage description	Objects and parameters
-----------	-------------------	------------------------

select	You must have full read access rights to the target Oracle database server.	V\$OPTION DBA_USERS DBA_TABLES V\$INSTANCE v\$VERSION V\$DATABASE V\$LICENSE V\$SESSION MGMT_LICENSE_DEFINITIONS MGMT_LICENSES DBA_FEATURE_USAGE_STATISTICS DBA_REGISTRY TMP_FEATURE_INFO DBA_OBJECTS DBA_AWS GV\$INSTANCE DBA_RECYCLEBIN LBACSYS.LBAC\$POLT SMP_REP_VERSION DUAL MDSYS.SDO_GEOM_METADATA_TABLE SYS.DBA_MINING_MODELS SYS.AUDIT_DBA_USERS DVSYS.DBA_DV_REALM ODM_DOCUMENT ODM_RECORD DBA_ENCRYPTED_COLUMNS DBA_TABLESPACES GV\$PARAMETER CMPINSTALLATION_V SYS.REGISTRY\$HISTORY USER_SYS_PRIVS USER_ROLE_PRIVS ROLE_SYS_PRIVS DBA_FLASHBACK_ARCHIVE DBA_FLASHBACK_ARCHIVE_TS DBA_FLASHBACK_ARCHIVE_TABLES DBA_LOBS DBA_LOB_PARTITIONS
--------	---	--

		<p>DBA_LOB_SUBPARTITIONS</p> <p>V\$BLOCK_CHANGE_TRACKING</p> <p>OLAPSYS.DBA\$OLAP_CUBES</p> <p>Oracle 9: ODM.ODM_MINING_MODEL</p> <p>Oracle 10 and later: MGMT_ADMIN_LICENSES</p> <p>Oracle 10 and later: MGMT_TARGETS</p> <p>Oracle 10 and later: MGMT_LICENSE_CONFIRMATION</p> <p>Oracle 10 and later: DBA_SQL_PROFILES</p> <p>Oracle 10 and later: MGMT_TARGET_TYPES</p> <p>Oracle 10 and later: MGMT_LICENSED_TARGETS</p> <p>Oracle 10.1: DBA_ADVISOR_TASKS</p> <p>Oracle 10.1: DBA_SQLSET</p> <p>Oracle 10.1 and later: DBA_SQLSET_REFERENCES</p> <p>Oracle 10.1 and later: SYSMAN.MGMT_VERSIONS</p> <p>Oracle 10.1 and later: SYSMAN.MGMT_INV</p> <p>Oracle 10.1 and later: MGMT\$TARGET</p> <p>Oracle 10.2: DMSYS.DM\$P_MODEL</p> <p>Oracle 10.2 and later: DBA_CPU_USAGE_STATISTICS</p> <p>Oracle 11 and later: SYS.MODEL\$</p> <p>Oracle 11.1 and later: V\$ARCHIVE_DEST_STATUS</p> <p>Oracle 11.1 and later: V\$DATABASE</p> <p>Oracle 11.1 and later: DBA_TAB_PARTITIONS</p> <p>Oracle 11.1 and later: DBA_TAB_SUBPARTITIONS</p> <p>Oracle 11.1 and later: DBA_CUBES</p> <p>Oracle 12.1 and later: V\$CONTAINERS</p> <p>Oracle 12.1 and later: SYSMAN.MGMT_FU_REGISTRATIONS</p> <p>Oracle 12.1 and later: SYSMAN.MGMT_FU_STATISTICS</p> <p>Oracle 12.1 and later: SYSMAN.MGMT_TARGETS</p> <p>Oracle 12.1 and later: SYSMAN.MGMT_FU_LICENSE_MAP</p>
--	--	---

# Basic Applications

## Host Applications by PowerShell

The job discovers host resources, process connectivity and software elements on Windows machines using PowerShell protocol.

Protocol: PowerShell

Operation	Usage description	Objects and parameters
exec	Basic login	ver  hostname
exec	Shared resources	wmic path Win32_Share get Description, Name, Path
exec	CPU	For Windows 2008: wmic path Win32_Processor get DeviceId,MaxClockSpeed,Manufacturer,LoadPercentage,Name,NumberOfCores  wmic path Win32_Processor get DeviceId,MaxClockSpeed,Manufacturer,LoadPercentage,Name,SocketDesignation
exec	Windows information	Language: wmic OS Get OSLanguage  Codepage: wmic OS Get CodeSet  wmic path Win32_OperatingSystem get BuildNumber, Caption, Version, csdversion, lastBootUpTime, organization, otherTypeDescription, registeredUser, totalVisibleMemorySize  wmic path Win32_ComputerSystem get Domain, Manufacturer, Model, Name, NumberOfProcessors
exec	File system	wmic logicaldisk get ProviderName, deviceId, driveType, freespace, size  dir %SystemRoot% /O:-D   find /I "system32"   Out-String -width 80
exec	Memory	Physical memory: wmic path Win32_PhysicalMemory get Capacity  Swap memory: wmic PAGEFILESET GET MaximumSize
exec	Processes	wmic Win32_Process get ParentProcessId, commandLine, creationdate, executablepath, name, processId
exec	User	wmic path Win32_UserAccount get Description, Disabled, Domain, FullName, Lockout, Name, SID

exec	Installed Software	wmic path Win32_Product get identifyingNumber, installDate, installLocation, name, vendor, version  For 32bit: reg query HKEY_LOCAL_MACHINE\SOFTWARE\Micros oft\Windows\CurrentVersion\Uninstall /S  For 64bit: reg query HKEY_LOCAL_MACHINE\SOFTWARE\Wow6 432Node\Microsoft\Windows\CurrentVersion\ Uninstall /S
exec	Windows Services	reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentC ontrolSet\Services /S  wmic service get AcceptPause, Description, DisplayName, Name, PathName, ServiceType, StartMode, State
exec	TCP Connections Info	Windows (XP Onwards), Includes process to port info: netstat -noa  Windows (before XP): netstat -na
exec	Code Page Info	chcp

## Host 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.lanmanag er.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 Applications by Shell

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

Protocol: Registry

Operation	Usage description	Objects and parameters
read	Microsoft MQ Plugin	Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters\setup  Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters\MachineCache  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Setup
read	Microsoft Operations Manager Management Server Plugin	HKLM\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Agent Management Groups  HKLM\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Setup  HKLM\SOFTWARE\Microsoft\Microsoft Operations Manager\2.0\Setup  HKLM\SOFTWARE\Mission Critical Software\OnePoint\Configurations  HKLM\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Server Management Groups  HKLM\Software\Microsoft\Microsoft Operations Manager  HKLM\SOFTWARE\Mission Critical Software\DASServer

Protocol: Shell

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

exec	Environment variables query and setup, data parsing and processing	<p>Windows: set PATH=%PATH%;%WINDIR%\system32\wbem\</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: echo \$SHELL</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: echo \$?</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: grep .*</p> <p>AIX: egrep .*</p> <p>AIX: ioscli .*</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: awk .*</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: nice .*</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: export .*</p>
exec	Basic login	<p>AIX,FreeBSD,HP-UX,Linux,SunOS: uname -a</p> <p>AIX: uname -M</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: uname</p> <p>Unix: /usr/ios/cli/ioscli uname -L</p> <p>ver</p> <p>Windows: wmic OS Get Caption OS Get CodeSet OS Get OSLanguage path Win32_ComputerSystem get Name /value</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: locale -a</p>
exec	Fibre Channel info	<p>VIO AIX: command -v lsdev fcstat</p> <p>AIX: command -v lsdev lscfg /usr/sbin/lscfg fcstat</p> <p>VIO AIX: lsdev --help -type adapter -field name -vpd -dev fcsx</p> <p>AIX: lsdev --help -C -c adapter -r name</p> <p>AIX: lscfg usage lscfg -v -p -l fcsx</p> <p>AIX: lslpp -l '*&lt;driverid&gt;.rte'</p> <p>VIO AIX: lslpp -l '*&lt;driverid&gt;.rte'</p> <p>AIX: fcstat fcsx</p> <p>VIO AIX: fcstat fcsx</p> <p>HP_UX: ioscan -f -n -C fc</p> <p>HP_UX: fcmsutil &lt;port_name&gt; &lt;port_name&gt; vpd &lt;port_name&gt; get remote all</p> <p>SunOS: fcinfo -? hba-port remote-port -p &lt;port_name&gt;</p> <p>Windows: wmic /namespace:\\root\WMI path MSFC_FCAdapterHBAAttributes get Active, DriverVersion, FirmwareVersion, InstanceName, Manufacturer, Model, ModelDescription, NodeWWN, SerialNumber, UniqueAdapterId /value /namespace:\\root\WMI path MSFC_FibrePortHBAAttributes get Active, Attributes, HBASatus, InstanceName, UniquePortId /value</p>

exec	iSCSI Info	<p>Windows: wmic /namespace:\\root\\Microsoft\\Windows\\Storage path MSFT_iSCSI Session get InitiatorNodeAddress, SessionIdentifier, TargetNodeAddress /value</p> <p>/namespace:\\root\\Microsoft\\Windows\\Storage path MSFT_iSCSI SessionToDisk get Disk, iSCSI Session /value</p> <p>/namespace:\\root\\Microsoft\\Windows\\Storage path MSFT_Disk get FriendlyName, Number, ObjectId, Path, SerialNumber, Size /value</p> <p>/namespace:\\root\\Microsoft\\Windows\\Storage path MSFT_Partition get AccessPaths, DiskId, DiskNumber, DriveLetter, Size /value</p>
exec	CPU Info	<p>AIX: lsattr -El &lt;procId&gt;</p> <p>Windows: wmic cpu get * /translate:basicxml /format:rawxml.xml cpu get DeviceId,MaxClockSpeed,Manufacturer,LoadPercentage,Name,NumberOfCores /translate:basicxml /format:rawxml.xml cpu get DeviceId,MaxClockSpeed,Manufacturer,LoadPercentage,Name,SocketDesignation /translate:basicxml /format:rawxml.xml path Win32_Processor get DeviceId, LoadPercentage, Manufacturer, MaxClockSpeed, Name, SocketDesignation /value</p> <p>HP-UX: echo itick_per_usec/D   /usr/bin/adb -k /stand/vmunix /dev/kmem   /usr/bin/tail -n 1</p> <p>HP-UX: echo "sc product cpu;il"   /usr/sbin/cstm   grep 'CPU Module'</p> <p>FreeBSD: dmesg   grep "cpu\\ Multiprocessor"   grep -A 1 "CPU:"</p> <p>Linux: cat /proc/cpuinfo</p> <p>Windows: reg query HKEY_LOCAL_MACHINE\\HARDWARE\\DESCRIPTION\\System\\CentralProcessor /S</p> <p>FreeBSD: sysctl hw.model hw.ncpu hw.clockrate</p> <p>SunOS: /usr/sbin/psrinfo -v</p> <p>HP-UX: model</p> <p>SunOS: prtconf</p> <p>AIX: prtconf   grep "proc"</p> <p>AIX: lscfg -vpl sysplanar0   grep PROC</p> <p>HP-UX,SunOS: kstat -p cpu_info</p>

exec	Memory Info	<p>Linux: free -m</p> <p>Windows: wmic path Win32_PhysicalMemory get Capacity /format:csv MEMORYCHIP get Capacity /format:csv &lt; %SystemRoot%\win.ini PAGEFILESET GET MaximumSize /format:list &lt; %SystemRoot%\win.ini wmic path Win32_OperatingSystem get BuildNumber, Caption, Version, csdversion, lastBootUpTime, organization, otherTypeDescription, registeredUser, totalVisibleMemorySize /value</p> <p>HP-UX: swapinfo -tm   grep total</p> <p>HP-UX: echo "selclass qualifier memory;info;wait;info;log"   cstm   grep "Total Configured Memory"</p> <p>AIX: swap -s</p> <p>HP-UX: grep Physical /var/adm/syslog/syslog.log</p> <p>HP-UX: print_manifest   grep Memory</p> <p>SunOS: prtconf</p> <p>HP-UX: ls /usr/contrib/bin/machinfo</p> <p>HP-UX: /usr/contrib/bin/machinfo -v</p> <p>Windows: meminfo.exe</p> <p>FreeBSD: dmesg   grep \'real memory\'</p> <p>FreeBSD: swapinfo -m</p> <p>FreeBSD: sysctl hw.physmem</p> <p>AIX: prtconf   grep \'^Memory\'   awk \'{print \$1,\$3,\$4}\'</p> <p>VMKernel: esxcfg-info -F xml   sed -n \'/&lt;memory-info&gt;/,&lt;/memory-info&gt;/p\'</p> <p>SunOS: swap -l</p>
exec	Disks info	<p>Windows: wmic path win32_logicaldisk get ProviderName, deviceId, driveType, freespace, size /value</p> <p>Windows: diskinfo.exe</p> <p>AIX,HP-UX,Linux,SunOS: df -P -k -k   awk \'{print \$1,\$2,\$3,\$4,\$5,\$6}\'</p>
exec	Users info	<p>AIX,FreeBSD,HP-UX,Linux,SunOS: cat /etc/passwd</p> <p>Windows: wmic path Win32_UserAccount where "Domain = '&lt;host_name&gt;'" get Description, Disabled, Domain, FullName, Lockout, Name, SID /value</p>

exec	Processes info	<p>Windows: wmic path Win32_Process get commandLine, creationdate, executablepath, name, processId /value</p> <p>Windows: processlist.exe</p> <p>SunOS: zonename</p> <p>AIX, Linux, SunOS: uname -r</p> <p>SunOS: ps -agxwwu -e -o pid -o zone</p> <p>HP-UX: ps -ef</p> <p>AIX, FreeBSD, HP-UX, Linux: ps -ax -o pid,uid,user,cputime,command -e -o 'user,pid,time,args' -ef -eo user,pid,lstart,command --cols 4000 --no-headers</p> <p>Linux: date +%z</p> <p>SunOS: pkgchk -l -p</p> <p>VMKernel: esxcfg-info -F xml   sed -n \'/&lt;vmfs-fileSystems&gt;/,&lt;\/vmfs-fileSystems&gt;/p\'</p>
exec	Installed Software info	<p>AIX: lspp -Lc -q</p> <p>HP-UX: swlist -a name -a revision -a title -a install_date -a vendor_tag</p> <p>UNIX: pkg_info -a -I</p> <p>Windows: reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall /S</p> <p>Windows: wmic path Win32_QuickFixEngineering where "InstalledBy != "" get HotFixID, InstallDate /value</p> <p>UNIX: rpm -qa --qf '%{NAME}~%{VERSION}~%{RELEASE}~%{ARCH}~%{GROUP}~%{VENDOR}~%{installtime:date}~%{INSTALLTID}\n'</p> <p>SunOS: pkginfo -l</p>
exec	Windows Services	<p>Windows: reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services /S</p> <p>Windows: wmic path Win32_Service get AcceptPause, Description, DisplayName, Name, PathName, ServiceType, StartMode, State /value</p>
exec	Discover TCP Connections Info	<p>Windows (XP Onwards), Includes process to port info: netstat -noa</p> <p>HP-UX: nestat -num -routinfo</p> <p>AIX, HP-UX, SunOS, Includes process to port info: lsof -i -P -n</p> <p>Windows, AIX, FreeBSD, HP-UX, Linux, SunOS: netstat -na</p> <p>SunOS, HP-UX, only process to port info: pfiles for i in `ps -e   awk '{print \$1}'`; do echo __[\$i]; pfiles \$i   grep 'sockname: AF_INET'; done</p> <p>Linux, Includes process to port info: netstat -nap</p>
exec	Shared resources	<p>Windows: wmic share where "Path &lt;&gt; "" get description, name, path /value</p>

exec	File version and modification date information	<p>Windows: wmic datafile where "name = '&lt;file_path&gt;'" get LastModified /format:list datafile where "name = '&lt;formattedPath&gt;'" get version</p> <p>Linux: rpm -qa --qf '%{NAME}~%{VERSION}\n'   grep -i</p> <p>SunOS: /usr/sbin/pkgchk -l -p \"" + file_path + ""\</p> <p>Unix: perl -e 'print ((stat(\$ARGV[0]))[9],\"\\n\\n\");' &lt;file_path&gt;</p> <p>Linux: rpm -qf "&lt;file_path&gt;" --qf '%{NAME}\\n' -qf "&lt;file_path&gt;" --qf '%{VERSION}\\n'</p> <p>Windows: Cscript.exe /nologo filever.vbs '+file_path+'</p>
exec	File location information	<p>Unix: which "&lt;file_name&gt;"</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: whereis -b "&lt;file_name&gt;"</p> <p>Unix: export "PATH=\$PATH:/opt/csw/bin:/opt/csw/sbin"</p>
exec	Postgres SQL plugin	postmaster --version
exec	Windows Registry read	<p>Windows: reg_mam &lt;path to key&gt; /S</p> <p>Windows: reg &lt;path to key&gt; /S</p>
exec	Plugins can execute nslookup for resolving host,	nslookup <hostname>
exec	HP-UX specific commands	<p>HP-UX: lstcpip -hostname</p> <p>HP-UX: cat /etc/hostname</p> <p>HP-UX: cat /etc/nodename</p> <p>HP-UX: lstcpip -interfaces</p> <p>HP-UX: netstat -num -routinfo</p> <p>HP-UX: lsmap -all -net</p> <p>HP-UX: lsdev -dev &lt;entry&gt; -attr</p>
exec	Service Guard by Shell plugin	<p>Unix: swlist   grep Serviceguard</p> <p>Unix: /usr/sbin/swlist   grep Serviceguard</p>
exec	Plugins can check if file exist	Unix: ls <file_name>
exec	Plugins can read file content	type <file_name>
exec	Set environment variable	<p>Windows: set &lt;variableName&gt;=&lt;variableValue&gt;</p> <p>Unix: export &lt;variableName&gt;=&lt;variableValue&gt;</p>
exec	DB version plugin	<p>Unix: type /etc/oratab</p> <p>sqlplus -v</p> <p>lsnrctl status</p>

exec	DB2 plugin	<p>Windows. Getting DB2 instance name by process pid: reg query "HKEY_LOCAL_MACHINE\SOFTWARE\IBM"</p> <p>Windows. Resetting ERRORLEVEL environment variable to 0: cmd.exe /c "exit /b 0"</p> <p>Unix. Setting DB2INSTANCE environment variable: export DB2INSTANCE="&lt;db2_instance_name&gt;"</p> <p>Getting version information: db2level</p> <p>Windows: db2cmd -c -w -i</p> <p>Getting Db2Instance, Db2Database and Db2Alias details: db2 list db directory list dcs directory list node directory show detail get dbm cfg</p> <p>Windows: find</p> <p>Windows: findstr</p> <p>Unix: grep</p> <p>Unix: echo ~&lt;db2_instance_name&gt;</p>
------	------------	--

## Host Applications by WMI

The job this adapter 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 Win32_PhysicalMemory
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
select	Fibre Channel info	root\WMI MSFC_FCAdapterHBAAttributes MSFC_FibrePortHBAAttributes

select	Windows Storage info	root\Microsoft\Windows\Storage MSFT_iSCSI Session MSFT_Partition MSFT_Disk MSFT_iSCSI SessionToDisk
--------	----------------------	---



# Citrix NetScaler

## Citrix NetScaler by SNMP

The job citrix NetScaler by SNMP.

Permissions information is unavailable or no permissions are required.

# Cloud - AWS

## AWS by Web Services

The job discovers AWS topologies of the Auto Scaling Group, CloudFormation, EC2, ECR, ECS, ELB, S3 Bucket, RDS, and VPC services using Web Services.

Protocol: RDS

Operation	Usage description	Objects and parameters
webservice call	Get DB instances	AmazonRDSClient.describeDBInstances
webservice call	Get available DB engines	AmazonRDSClient.describeDBEngineVersions
webservice call	Get DB parameter groups	AmazonRDSClient.describeDBParameterGroups
webservice call	Get DB security groups	AmazonRDSClient.describeDBSecurityGroups
webservice call	Get DB snapshots	AmazonRDSClient.describeDBSnapshots

Protocol: S3

Operation	Usage description	Objects and parameters
webservice call	Get S3 Buckets	AmazonS3Client.listBuckets()
webservice call	Get S3 Bucket Region	AmazonS3Client.getBucketLocation(bucketName)
webservice call	Get S3 Bucket Versioning Status	AmazonS3Client.getBucketVersioningConfiguration(bucketName)
webservice call	Get S3 Bucket Replication Status	AmazonS3Client.getBucketReplicationConfiguration(bucketName)

Protocol: ASG

Operation	Usage description	Objects and parameters
webservice call	Get Auto Scaling Group	AmazonAutoScalingClient.describeAutoScalingGroups()

Protocol: ECS

Operation	Usage description	Objects and parameters
webservice call	Get Task Definition	AmazonECSClient.describeTaskDefinition
webservice call	List Clusters	AmazonECSClient.listClusters
webservice call	Get Clusters	AmazonECSClient.describeClusters

webservice call	List Container Instances	AmazonECSClient.listContainerInstances
webservice call	Get Container Instances	AmazonECSClient.describeContainerInstances
webservice call	List Tasks	AmazonECSClient.listTasks
webservice call	Get Tasks	AmazonECSClient.describeTasks
webservice call	List Services	AmazonECSClient.listServices
webservice call	Get Services	AmazonECSClient.describeServices
webservice call	Get Images	AmazonECSClient.describeImages
webservice call	Get Repositories	AmazonECSClient.describeRepositories

Protocol: AIM

Operation	Usage description	Objects and parameters
webservice call	Get account ID using ARN saved in user information	AmazonIdentityManagementClient.getUser

Protocol: EC2

Operation	Usage description	Objects and parameters
webservice call	Get regions	AmazonEC2Client.describeRegions
webservice call	Get availability zones	AmazonEC2Client.describeAvailabilityZones
webservice call	Get running instances	AmazonEC2Client.getInstanceByStatus running
webservice call	Get instance EBS volumes by IDs	AmazonEC2Client.describeVolumes DescribeVolumesRequest(volume_id)
webservice call	Get snapshots of EBS volumes by IDs	AmazonEC2Client.describeSnapshots DescribeSnapshotsRequest(snapshot_id)
webservice call	Get AMI by ID	AmazonEC2Client.describeImages DescribeImagesRequest(ami_id)
webservice call	Get elastic IPs	AmazonEC2Client.describeAddresses

# Cloud - Cloud Foundry

## CloudFoundry by WebServices

The job this adapter discovers applications and services on a CloudFoundry.

Protocol: HTTP/HTTPS

Operation	Usage description	Objects and parameters
GET	List all Organizations	/v2/organizations
GET	List all Organization Quota Definitions	/v2/quota_definitions
GET	List all Spaces	/v2/spaces
GET	List all Space Quota Definitions	/v2/space_quota_definitions
GET	List all Private Domains	/v2/private_domains
GET	List all Shared Domains	/v2/shared_domains
GET	List all Routes	/v2/routes
GET	List all Apps	/v2/apps
GET	List all Services	/v2/services
GET	List all Service Plans	/v2/service_plans
GET	List all Service Instances	/v2/service_instances
GET	List all Service Bindings	/v2/service_bindings
GET	List all Route Mappings	/v2/route_mappings

# Cloud - Microsoft Azure

## Azure by WebServices

The job this adapter discovers subscriptions, resource groups, virtual machines, networks and storage accounts on an Azure tenant.

Protocol: HTTPS

Operation	Usage description	Objects and parameters
GET	List all tenants	<a href="https://management.azure.com/tenants?api-version=2015-01-01">https://management.azure.com/tenants?api-version=2015-01-01</a>
GET	List all subscriptions	<a href="https://management.azure.com/subscriptions?api-version=2015-01-01">https://management.azure.com/subscriptions?api-version=2015-01-01</a>
GET	List all resource groups	<a href="https://management.azure.com/subscriptions/{subscription-id}/resourcegroups?api-version=2015-01-01">https://management.azure.com/subscriptions/{subscription-id}/resourcegroups?api-version=2015-01-01</a>
GET	List all resources in a subscriptions	<a href="https://management.azure.com/subscriptions/{subscription-id}/providers/.....">https://management.azure.com/subscriptions/{subscription-id}/providers/.....</a>

# Cloud - OpenStack

## OpenStack by Web Services

The job this adapter discovers projects, compute resources, networks, storage and other details on an OpenStack.

Protocol: HTTP

Operation	Usage description	Objects and parameters
API Access	Keystone	openstack-keystone
API Access	Compute	openstack-nova
API Access	Volume	openstack-cinder
API Access	Image	openstack-glance
API Access	Network	openstack-neutron

## **Cloud - OpenStackEvent**

### **Manual AMQP for OpenStack**

The job report AMQP server with its message consumer.

Permissions information is unavailable or no permissions are required.

### **OpenStack Event Monitor**

The job openStack Event Monitor.

Permissions information is unavailable or no permissions are required.

## Cloud - vCloudEvent

### vCloud Event Monitor

The job vCloud Event Monitor.

Permissions information is unavailable or no permissions are required.



# CloudFoundry Event Monitor

## CloudFoundry Event Monitor

The job cloudFoundry Event Monitor.

Protocol: HTTP/HTTPS

Operation	Usage description	Objects and parameters
GET	Get events	/v2/events
GET	List all Organizations	/v2/events
GET	List all Spaces	/v2/spaces
GET	List all Private Domains	/v2/private_domains
GET	List all Shared Domains	/v2/shared_domains
GET	List all Routes	/v2/routes
GET	List all Apps	/v2/apps
GET	List all Services	/v2/services
GET	List all Service Plans	/v2/service_plans
GET	List all Service Instances	/v2/service_instances
GET	List all Service Bindings	/v2/service_bindings
GET	List all Route Mappings	/v2/route_mappings

## Cluster - A10 vThunder

### A10 vThunder by SNMP

The job this adapter discovers A10 vThunder Load Balancer using SNMP protocol.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	General information about A10 vThunder	iso.org.dod.internet.private.enterprises.a10.a10Mgmt.axMgmt.axSystem.axSysVersion: 1.3.6.1.4.1.22610.2.4.1.1
get	Virtual servers	iso.org.dod.internet.private.enterprises.a10.a10Mgmt.axMgmt.axApp.axServers.axServerPort.axServerPortTable.axServerPortEntry: 1.3.6.1.4.1.22610.2.4.3.4.3.1.1
get	Virtual Groups	a10Mgmt.axMgmt.axApp.axServiceGroups.axServiceGroupMember.axServiceGroupMemberTable.axServiceGroupMemberEntry: 1.3.6.1.4.1.22610.2.4.3.3.3.1.1
get	Real Servers	a10Mgmt.axMgmt.axApp.axServers.axServerPort.axServerPortTable.axServerPortEntry: 1.3.6.1.4.1.22610.2.4.3.2.3.1.1

## Cluster - Alteon LB

### Alteon application switch by SNMP

The job discovers Nortel Application Switches using the SNMP protocol.

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

## Cluster - Cisco ACE

### Cisco ACE by SNMP

The job this adapter discovers Cisco ACE Load Balancer using SNMP protocol.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	Farm	iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoSlbMIB.ciscoSlbMIBObjects.slbServerFarms: 1.3.6.1.4.1.9.9.161.1.2.1.1
get	Real Server	iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoSlbMIB.ciscoSlbMIBObjects.slbRealServers.slbRealTable.slbRealTableEntry: 1.3.6.1.4.1.9.9.161.1.3.1.1
get	Virtual Server	iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoSlbMIB.ciscoSlbMIBObjects.slbVirtualServers.slbVirtualServerTable.slbVirtualServerTableEntry: 1.3.6.1.4.1.9.9.161.1.4.1.1

## Cluster - Cisco CSS

### Cisco CSS by SNMP

The job discovers Cisco CSS (Content Services Switch) using the SNMP protocol.

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

# Cluster - EMC AutoStart

## EMC AutoStart by Shell

The job discover EMC AutoStart cluster by shell.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic login	uname ver
exec	Get cluster version	ftcli -version
exec	Verify domain name	cat {full_path}/{domain}-sites type {full_path}/{domain}-sites
exec	Get cluster configuration	ftcli -cmd 'listManagedIPs' -cmd 'listManagedNics' -cmd 'listNodes' -cmd 'listResourceGroups' -cmd 'listDataSources' -cmd 'listProcs' -cmd 'getIP {ipName}' -cmd 'getNic {nodeName} {nicName}' -cmd 'getNode {nodeName}' -cmd 'getResourceGroup {groupName}' -cmd 'getDataSource {dataSourceName}' -cmd 'getProc {processName}'

## Cluster - F5 BIG-IP

### F5 BIG-IP LTM by SNMP

The job this adapter 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

### F5 BIG-IP LTM by Shell

The job this adapter discovers F5 BIG-IP LTM by shell.

Protocol: Shell

Operation	Usage description	Objects and parameters
-----------	-------------------	------------------------

exec	Basic Login	UNIX: date +%z UNIX: echo \$? \$SHELL UNIX: uname -a -r UNIX: locale -a
exec	Discover files and F5 details	UNIX: ps -eo user,pid,lstart,command --cols 2530 --no-headers UNIX: readlink UNIX: ls -lA <folder_path> UNIX: cat <file_path> UNIX: perl -e java -version UNIX: find <folder_path>



# Cluster - IBM HACMP

## HACMP Application Discovery

The job discovers IBM HACMP virtual applications.

Protocol: shell

Operation	Usage description	Objects and parameters
exec	Basic login	AIX: cat etc/hosts
exec	Get volume information	AIX: lspv
exec	Cluster configuration information	AIX: cldisp
exec	Network configuration information	AIX: cllsif -c

## HACMP Topology Discovery

The job discovers IBM HACMP node Topology on servers via SSH, Telnet or UDA.

Protocol: shell

Operation	Usage description	Objects and parameters
exec	Basic Login	uname locale -a
exec	Cluster configuration	AIX: cluster.license
exec	cluster configuration	AIX: cldisp
lslpp -l	Cluster license information	AIX: lslpp -l
lspv	Get Physical volume and volume groups	AIX: lspv
lsvg -l	Get logical volumes	AIX: lsvg -l
lsdev -Cc adapter	Get the adapters on the host	AIX: lsdev -Cc adapter
entstat	Get details about an adapter	AIX: entstat

## Cluster - Microsoft Cluster

### MS Cluster by NTCMD or UDA or PowerCmd

The job this adapter discovers Microsoft Cluster architecture by NTCMD.

Protocol: Shell

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

# Cluster - Microsoft NLB

## MS NLB by NTCMD or UDA

The job discovers MS Network Load Balancing topology by NTCMD or UDA.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Generic commands execution	ver wmic OS Get CodeSet OS Get OSLanguage
exec	Read nlb params	wlbs params nlb params

# 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	uname ver
exec	Connecting to cluster software	/usr/sbin/cmviewcl -v
exec	Find configuration files	UNIX: find {FILE_PATH}
exec	Fetching configuration file content	UNIX: cat {FILE_PATH} -type f
exec	Lookup for existing locales on the destination	UNIX: locale -a
exec	Domain name and ip resolving	UNIX: nslookup {FQDN or IP}
exec	List running processes	UNIX: ps -ef
exec	Gather packages info	UNIX: cmgetconf -K -c <clustername> -p <packagename>
exec	Gather process to port info	UNIX: nice pfiles <pid> 2> &1   awk "/S_IFSOCK SOCK_STREAM SOCK_DGRAM port/ { print }"
exec	Gather process to port info	UNIX: nice lsof -i 4 -a -P -n -p <pid>

# Cluster - Solaris

## Sun Cluster by Shell

The job adapter discovers Sun Cluster topology via shell including cluster nodes, resource groups and resources, quorum configuration, cluster interconnect.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic login	uname ver
exec	Get Networking information	Interfaces: netstat -np IP information, IPMP Groups: /usr/sbin/ifconfig -a Resolve IP to MAC: /usr/sbin/arp [ip] Resolve hostname to IP: /usr/sbin/nslookup [hostname] Get hostname of connected host: hostname
exec	Get cluster version	/usr/cluster/bin/scinstall -p
exec	Get cluster configuration	/usr/cluster/bin/scconf -pv
exec	Get cluster statistics	Quorum stats: /usr/cluster/bin/scstat -q Nodes stats: /usr/cluster/bin/scstat -n Resource Groups stats: /usr/cluster/bin/scstat -g Transport paths stats: /usr/cluster/bin/scstat -W
exec	Get resources and resource groups	/usr/cluster/bin/scrgadm -pvv

# 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	uname ver
exec	Checking for existing of configuration file	ls /etc/rc3.d/S*vcs
exec	Fetching configuration file content	cat {FILE_PATH}
exec	Fetching group node running state	hagrp state
exec	Hostname resolution	nslookup <host_name>
exec	Windows language & codepage	Codepage: wmic OS Get CodeSet Language: wmic Get OSLanguage
exec	Windows configuration file monitoring	Check configuration existence: type <file_path>\main.cf  Configuration last modification: wmic datafile where "name = "<file_path>\main.cf" get LastModified /format

# Config Parser

## Config Parser by Shell

The job sample adapter - Get and parse the configuration file of a running software and report an IP address.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Any command	Windows/UNIX: Any command -l

## Config Parser by Shell - Manual

The job sample adapter - Get and parse the configuration file of a running software and report an IP address.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Any command	Windows/UNIX: Any command -l

# Database - Connections using Host credentials

## DB Connections by Shell

The job database existence discovery by Shell.

Protocol: Shell

Operation	Usage description	Objects and parameters
copy	Copy file to remote machine	reg_mam.exe - Console registry tool for Windows
exec	Basic login	Windows: ver Windows: wmic OS Get CodeSet Windows: wmic OS Get OSLanguage UNIX: uname UNIX: echo\$ UNIX: locale -a
exec	File operations	Windows: dir /s/b (file or path) Windows: type (file) UNIX: ls -lA (file or path) UNIX: cat (file)
exec	Processes info	Windows: wmic process get commandLine,creationdate,executablepath,name,processId /format:csv < %SystemRoot%\win.ini Windows: processlist.exe SunOS: zonename SunOS: uname -r SunOS: ps -agxwwu -e -o pid -o zone UNIX (not SunOS): ps -ax -o pid,uid,user,cputime,command -e -o 'user,pid,time,args' -ef -eo user,pid,lstart,command --cols 2048 --no-headers SunOs: pkgchk -l -p
exec	Installed Software info	UNIX: lspp -Lc -q UNIX: swlist UNIX: pkg_info -a -I Windows: reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall /S UNIX: rpm -qa --qf '%{NAME}~%{VERSION}~%{GROUP}~%{VENDOR}\\n' UNIX: pkginfo -l



exec	Windows Services	<p>Windows: reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services /S</p> <p>Windows: wmic service get displayname, pathname, processid, started /format:csv</p>
exec	Discover TCP Connections Info	<p>Windows (XP Onwards), Includes process to port info: netstat -noa</p> <p>AIX, HPUX, SunOS, Includes process to port info: lsof -i -P -n</p> <p>Windows (before XP) and UNIX: netstat -na</p> <p>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</p> <p>Linux, Includes process to port info: netstat -nap</p>
exec	Discover TCP Connections Info	<p>Windows (XP and later), Includes process to port info: netstat -noa</p> <p>AIX, HPUX, SunOS, Includes process to port info: lsof -i -P -n</p> <p>Windows (before XP) and UNIX: netstat -na</p> <p>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</p> <p>Linux, Includes process to port info: netstat -nap</p>
exec	SQL Server details	<p>Listener Port: reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\instanceName\MSSQLServer\SuperSocketNetLib\Tcp\TcpPort /S</p> <p>SQL Server Installed Instances: reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server /s</p> <p>Install Path: reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\instanceName\Setup\SQLPath /S</p> <p>Software Version: reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\instanceName\MSSQLServer\CurrentVersion\CurrentVersion /S</p> <p>Cluster IP Address: reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\instanceName\MSSQLServer\Cluster\ClusterIpAddr /S</p> <p>Cluster Name: reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\instanceName\MSSQLServer\Cluster\ClusterName /S</p>

## DB Connections by WMI

The job database existence discovery by WMI.

Protocol: WMI

Operation	Usage description	Objects and parameters
select	System Name Info	root\cimv2 Win32_ComputerSystem
select	Process Info	root\cimv2 Win32_Process
select	Service Info	root\cimv2 Win32_Service
exec	Installed Software info	Windows: root\DEFAULT StdRegProv:EnumKey() StdRegProv:EnumValues()
select	Installed Software info	root\cimv2 Win32_Product

# Database - DB2

## DB2 Topology by SQL

The job discover the physical elements within DB2 database.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Probe local shell initialization	ver wmic OS Get CodeSet OS Get OSLanguage echo chcp if exist %SystemRoot%\SysWOW64 (echo SysWOW64) ELSE (echo FALSE)
exec	Ip or hostname resolution	nslookup

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Getting version	TABLE(sysproc.env_get_inst_info())
select	Getting tablespaces info	SYSCAT.TABLESPACES
select	Getting tablespace containers info	SYSIBMADM.CONTAINER_UTILIZATION
select	Getting opened db sessions info	TABLE(SNAP_GET_APPL_INFO(", -1))
select	Getting partition groups info	SYSCAT.DBPARTITIONGROUPS
select	Getting partitions info	TABLE(DB_PARTITIONS())
select	Getting custom partitions info	SYSCAT.DBPARTITIONGROUPDEF
select	Getting buffer pools info	SYSCAT.BUFFERPOOLS
select	Getting buffer pools to partitions relation info	SYSCAT.BUFFERPOOLDBPARTITIONS
select	Getting tables info	SYSCAT.TABLES
select	Getting existing schemas info	SYSCAT.SCHEMATA

## DB2 Universal Database Connection by SQL

The job this adapter discovers databases using SQL protocol.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Getting instance name and version	TABLE(sysproc.env_get_inst_info()) as x
select	Getting database name	SYSIBM.SYSDUMMY1
select	Getting network service name(svcename)	SYSIBMADM.DBMCFG
select	Getting instance address	TABLE(SYSPROC.ENV_GET_SYS_INFO()) as T

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Probe local shell initialization	echo chcp ver if exist %SystemRoot%\SysWOW64 (echo SysWOW64) ELSE (echo FALSE) wmic OS Get CodeSet OS Get OSLanguage
exec	Ip or hostname resolution	nslookup

## Databases TCP Ports

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

Protocol: TCP

Operation	Usage description	Objects and parameters
connect	The probe host must not be blocked by ACL	socket

# Database - MS-SQL

## Databases TCP Ports

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

Protocol: TCP

Operation	Usage description	Objects and parameters
connect	The probe host must not be blocked by ACL	socket

## MSSQL Server Connection by SQL

The job this adapter discovers databases using SQL protocol.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Check MS SQL database version	@@version  @@servername  SERVERPROPERTY ProductVersion ProductLevel
select	check listen ports for MS SQL	sys.dm_exec_connections

## 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 Collation Edition InstanceName IsClustered IsFulltextInstalled LicenseType ProductLevel ProductVersion
select	Gather users info	master..syslogins
select	Gather schemas info	master..sysdatabases

exec	Server configuration	master..xp_instance_regread N'HKEY_LOCAL_MACHINE',N'SOFTWARE\Microsoft\MSSQLServer\MSSQLServer',N'MailAccountName' N'HKEY_LOCAL_MACHINE',N'SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\SuperSocketNetLib',N'ProtocolList' N'HKEY_LOCAL_MACHINE',N'SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\SuperSocketNetLib\Tcp',N'TcpHideFlag' N'HKEY_LOCAL_MACHINE',N'SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\SuperSocketNetLib\Tcp',N'TcpPort'
select	Server configuration	master.dbo.sysconfigures  master..sysobjects  sysobjects  master.dbo.spt_values
select	Server startup info	master..sysobjects
exec	Server startup info	master..xp_instance_regread N'HKEY_LOCAL_MACHINE',N'SOFTWARE\Microsoft\MSSQLServer\MSSQLServer\Parameters',N'SQLArg??'
select	SQL Server Plans	msdb.dbo.sysdtspackages90  msdb.dbo.sysmaintplan_subplans  msdb.dbo.sysmaintplan_plans  msdb.dbo.sysdbmaintplans  msdb.dbo.sysdtspackagefolders90  msdb..sysjobs  msdb.dbo.sysdbmaintplan_databases
select	Gather process information	master..sysdatabases  master..sysprocesses
exec	Cluster information	sp_helpdistpublisher  sp_helpdistributor  master..xp_instance_regread N'HKEY_LOCAL_MACHINE',N'SOFTWARE\Microsoft\MSSQLServer\Replication',N'IsInstalled'
select	Database configuration	master..sysfilegroups  master..sysfiles  master..sysusers  sysusers
select	Getting SQL File. To discover SQL files each user priviledges have to be assigned	each database: sysfiles each database: sysfilegroups
select	Getting Backup Information. To discover SQL files each user priviledges have to be assigned	msdb..backupset msdb..backupmediafamily

select	Getting Storage Procedure information.	<database name>.information_schema.routines
select	Getting Always On Cluster information	sys.availability_databases_cluster sys.availability_groups_cluster sys.availability_group_listeners sys.availability_group_listener_ip_addresses

# Database - MySQL

## Databases TCP Ports

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

Protocol: TCP

Operation	Usage description	Objects and parameters
connect	The probe host must not be blocked by ACL	socket

## MySQL Connection by SQL

The job connects to MySQL databases.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Check MySql database version	version()

## MySQL Topology by SQL

The job discovers MySQL instances topology by SQL.

Permissions information is unavailable or no permissions are required.

## MySQL by Shell

The job discovers MySQL instances and replication topology by Shell.

Protocol: Shell

Operation	Usage description	Objects and parameters
-----------	-------------------	------------------------



exec	Basic login	echo \$  locale -a  uname  ver  wmic OS Get CodeSet OS Get OSLanguage
exec	MySQL Topology	WIN: dir /-C {MYSQL_HOME}\my.cnf /-C {MYSQL_HOME}\my.ini  WIN: {MYSQL_HOME}\mysqld.exe --version -- verbose --help  WIN: type {MYSQL_HOME}\my.cnf {MYSQL_HOME}\my.ini  UNIX: cat {MYSQL_HOME}/my.cnf  UNIX: ls -lA {MYSQL_HOME}/my.cnf  UNIX: mysqld --version --verbose --help

# Database - Oracle

## Databases TCP Ports

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

Protocol: TCP

Operation	Usage description	Objects and parameters
connect	The probe host must not be blocked by ACL	socket

## Oracle Config Files by SQL

The job discovers Oracle database configurations based on the v\$parameter table.

Protocol: SQL

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

## Oracle Connection by Shell

The job this adapter discovers Oracle database topology by Shell.

Protocol: SQLPlus

Operation	Usage description	Objects and parameters
select	Gather database info	V\$SPPARAMETER V\$BACKUP V\$DATAFILE V\$RECOVER_FILE V\$PARAMETER V\$DATABASE

Protocol: Shell

Operation	Usage description	Objects and parameters
sqlplus	Check Oracle database role	

## Oracle Database Connection by SQL

The job this adapter discovers databases using SQL protocol.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Check Oracle database version	v\$version V\$PARAMETER where name='instance_name'
select	Check oracle instance host name	UTL_INADDR.get_host_address from dual
select	Check fqdn of oracle server	HOST_NAME from V\$INSTANCE where upper(INSTANCE_NAME) = <instance name>
select	Check for clustered database	value from V\$SPPARAMETER where name = <cluster_database>
select	Check for clustered database	value from V\$PARAMETER where name = <cluster_database>
select	Gather service information	V\$SERVICES

## Oracle Database Connection by SQL - Lightweight

The job this adapter discovers databases using SQL protocol.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Check Oracle database version	v\$version V\$PARAMETER where name='instance_name'
select	Check oracle instance host name	UTL_INADDR.get_host_address from dual
select	Check fqdn of oracle server	HOST_NAME from V\$INSTANCE where upper(INSTANCE_NAME) = <instance name>

## 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 current status	\$ORACLE_HOME/bin/lsnrctl status
exec	System information	Windows,UNIX: hostname Windows,UNIX: nslookup Windows: ver UNIX: uname UNIX: echo <variable> UNIX: locale -a

## 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
exec	Enumerates configured service names on the node or in RAC including node related data and sid	srvctl status database -d <instance name> srvctl config database
exec	System identification	uname
exec	Locale identification	locale -a
exec	DNS resolving	nslookup
exec	Host name identification in FQDN format	hostname -i -f

## Oracle TNS Names by LDAP

The job this adapter discovers Oracle database information saved in LDAP storage.

Protocol: LDAP

Operation	Usage description	Objects and parameters
select	Connect to an AD DC	from root: all
get	Get AD attribute information	rootDomainNamingContext
select	Get Oracle's contexts from rootDomainNamingContext or based_dn	orclContext name distinguishedname
select	Get TNS Names from Oracle's Context object	orclNetService orclNetDescString

## Oracle Topology by SQL

The job this adapter 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 DBA_DATA_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_SEGMENTS DBA_SCHEDULER_JOBS V\$RECOVER_FILE DBA_JOBS
select	Oracle RAC related info	V\$SPPARAMETER Discover all the rac nodes: GV\$INSTANCE
select	Check valid standby count	v\$archive_dest

## Oracle Topology by SQL - Service Name

The job this adapter uses Service Name to connect Oracle and discovers Oracle 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 DBA_DATA_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_SEGMENTS DBA_SCHEDULER_JOBS V\$RECOVER_FILE DBA_JOBS
select	Oracle RAC related info	V\$SPPARAMETER Discover all the rac nodes: GV\$INSTANCE
select	Check valid standby count	v\$archive_dest

# Database - PostgreSQL

## Databases TCP Ports

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

Protocol: TCP

Operation	Usage description	Objects and parameters
connect	The probe host must not be blocked by ACL	socket

## PostgreSQL Connection by SQL

The job this adapter discovers databases using SQL protocol.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Check PostgreSQL database version	version()



# Database - Sybase

## Databases TCP Ports

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

Protocol: TCP

Operation	Usage description	Objects and parameters
connect	The probe host must not be blocked by ACL	socket

## Sybase Database Connection by SQL

The job this adapter discovers databases using SQL protocol.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Check Sybase database version	@@version
select	sid information	master..sys.servers

## Sybase Topology by SQL

The job this adapter discovers Sybase database topology by SQL.

Protocol: SQL

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

## Deprecated Jobs

### SAP Profiles by Shell

The job discover profile files for SAP Application Servers.

Permissions information is unavailable or no permissions are required.

### SAP System by Shell

The job the job discovers SAP Systems using information from the configuration files.

Permissions information is unavailable or no permissions are required.

# Discovery Samples

## Dynamic Credential Sample

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

Permissions information is unavailable or no permissions are required.

## Import from CSV sample

The job imports data from a CSV file into CMDB using mapping of the CSV file columns to CIT attributes. Mapping is defined by the following 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. Mapping file is used for more complex mapping definitions. Mapping file name is specified by 'mappingFile' parameter.

Protocol: Shell

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

# Discovery Tools

## File Monitor by Shell

The job discovers Document files and Directories.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Windows information acquaintance	Windows version: ver File monitoring: cmd /V:ON /c <script> Directory listing: dir dir /b <folder_path> Directory traversal: cd /D <folder_path> Codepage: wmic OS Get CodeSet Language: wmic OS Get OSLanguage
exec	Unix-like OS information acquaintance	OS/Kernel version in Linux and AIX: uname System variables acquaintance in Linux and AIX: echo <variable> File monitoring in Linux and AIX: perl -e <monitoring script> Locale information in Linux and AIX: locale -a   grep -E "en_US.* ^C POSIX"

## Import from CSV file

The job imports data from a CSV file into CMDB using mapping of the CSV file columns to CIT attributes. Mapping is defined by the following 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. Mapping file is used for more complex mapping definitions. Mapping file name is specified by 'mappingFile' parameter.

Protocol: Shell

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

## Import from Database

The job imports data from an external database into CMDB using mapping of table columns to CIT attributes. Mapping is defined by the following 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. Mapping file is used for more complex mapping definitions. Mapping file name is specified by `'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 custom SQL query.

Permissions information is unavailable or no permissions are required.

## Import from Excel Workbook

The job imports data from Excel Workbooks. Parses through multiple worksheet XLS files. Uses `'CIImports.xls'` (default) file to import data.

Protocol: Shell

Operation	Usage description	Objects and parameters
read	Read import file content	file_name

## 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 adapter 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	uname ver
exec	Fetching file content	UNIX: cat Windows: type

## Link DB Datafiles And Clustered FS

The job this adapter is used for linking of database datafiles with clustered file system.

Permissions information is unavailable or no permissions are required.

## Merge Clustered Software

The job adapter used by the Merging topologies of the Clustered Software Elements.

Permissions information is unavailable or no permissions are required.

## TCP Ports

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

Protocol: TCP

Operation	Usage description	Objects and parameters
connect	The probe host must not be blocked by ACL	socket

## Thin clients MAC based detection

The job adapter Description.

Permissions information is unavailable or no permissions are required.

# Docker

## Docker Discovery by Shell

The job docker runtime Discovery.

Protocol: shell

Operation	Usage description	Objects and parameters
exec	Get processes on host	ps -ef
exec	Discover Docker	docker diff docker images inspect ps

## Docker Swarm Discovery by RESTful API

The job docker Swarm runtime Discovery using RESTful API.

Protocol: HTTP

Operation	Usage description	Objects and parameters
API Access	version, info, images, containers, inspect, top	images top inspect containers version info

# Docker Swarm Event Monitor

## Docker Swarm Event Monitor

The job docker Swarm Event Monitor.

Protocol: HTTP

Operation	Usage description	Objects and parameters
API Access	events	events



# Execute Command

## Execute Command by Shell

The job execute command on a host.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Any command	Windows/UNIX: Any command -l

## Execute Command by Shell - Manual

The job execute command on a host.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Any command	Windows/UNIX: Any command -l

# Firewall

## Firewall Topology by SNMP

The job this adapter supports discovery of Juniper and Fortinet firewalls by SNMP.

Protocol: SNMP

Operation	Usage description	Objects and parameters
read	Juniper related	1.3.6.1.4.1.2636.3.39.1.4.1.1.2.1.7 1.3.6.1.4.1.2636.3.39.1.7.1.1.2.1.4 1.3.6.1.4.1.2636.3.39.1.7.1.1.2.1.1 1.3.6.1.4.1.2636.3.39.1.4.1.1.2.1.5 1.3.6.1.4.1.2636.3.39.1.7.1.1.2.1.2 1.3.6.1.4.1.2636.3.39.1.7.1.1.2.1.5 1.3.6.1.4.1.2636.3.39.1.7.1.1.2.1.6 1.3.6.1.4.1.2636.3.5.1.1.3 1.3.6.1.4.1.2636.3.5.1.1.2 1.3.6.1.4.1.2636.3.5.1.1.1 1.3.6.1.4.1.2636.3.39.1.4.1.1.2.1.1 1.3.6.1.4.1.2636.3.39.1.4.1.1.2.1.3

read	Fortinet related	1.3.6.1.4.1.12356.101.10.113.1.1 1.3.6.1.4.1.12356.101.10.113.1.2 1.3.6.1.4.1.12356.101.10.113.1.3 1.3.6.1.4.1.12356.101.10.113.1.4 1.3.6.1.4.1.12356.101.10.113.1.5 1.3.6.1.4.1.12356.101.10.113.1.6 1.3.6.1.4.1.12356.101.5.1.2.1.1.2 1.3.6.1.4.1.12356.101.5.1.2.1.1.1 1.3.6.1.4.1.12356.101.5.1.2.1.1.3 1.3.6.1.4.1.12356.101.10.112.5.1.6 1.3.6.1.4.1.12356.101.10.112.5.1.7 1.3.6.1.4.1.12356.101.8.2.1.1.9 1.3.6.1.4.1.12356.101.12.2.4.1.4 1.3.6.1.4.1.12356.101.8.2.1.1.7 1.3.6.1.4.1.12356.101.12.2.4.1.1 1.3.6.1.4.1.12356.101.8.2.1.1.8 1.3.6.1.4.1.12356.101.12.2.4.1.2 1.3.6.1.4.1.12356.101.8.2.1.1.10 1.3.6.1.4.1.12356.101.8.2.1.1.2 1.3.6.1.4.1.12356.101.8.2.1.1.1 1.3.6.1.4.1.12356.101.8.2.1.1.6 1.3.6.1.4.1.12356.101.8.2.1.1.5 1.3.6.1.4.1.12356.101.8.2.1.1.4 1.3.6.1.4.1.12356.101.12.2.4.1.5 1.3.6.1.4.1.12356.101.8.2.1.1.3 1.3.6.1.4.1.12356.101.10.112.5.1.1 1.3.6.1.4.1.12356.101.10.112.5.1.5 1.3.6.1.4.1.12356.101.10.112.5.1.4 1.3.6.1.4.1.12356.101.10.112.5.1.3 1.3.6.1.4.1.12356.101.10.112.5.1.2
------	------------------	--

## Firewall Topology by Shell

The job this adapter supports discovery of Juniper firewalls by Shell.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Get Firewall Configuration	show Donfiguration
exec	Get Chassis information	show chassis hardware
exec	Get Chassis Cluster ID	show chassis cluster status

# GettingStartedGuide

## SQLDiscoveryTutorial

The job getting Started Guide SQL Discovery Tutorial.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Gather users info	UDGettingStarted..Sample_Table_1
		UDGettingStarted..Sample_Table_2

# Google Cloud

## Google Cloud by RESTful API

The job discover Google Cloud by RESTful API.

Protocol: HTTP/HTTPS

Operation	Usage description	Objects and parameters
GET	Get RESTful API	<a href="https://www.googleapis.com/discovery/v1/apis/compute/v1/rest">https://www.googleapis.com/discovery/v1/apis/compute/v1/rest</a>
GET	List Regions	<a href="https://www.googleapis.com/compute/v1/projects/project/regions">https://www.googleapis.com/compute/v1/projects/project/regions</a>
GET	List Zones	<a href="https://www.googleapis.com/compute/v1/projects/project/zones">https://www.googleapis.com/compute/v1/projects/project/zones</a>
GET	List Disks	<a href="https://www.googleapis.com/compute/v1/projects/project/zones/zone/disks">https://www.googleapis.com/compute/v1/projects/project/zones/zone/disks</a>
GET	List Images	<a href="https://www.googleapis.com/compute/v1/projects/project/zones/zone/images">https://www.googleapis.com/compute/v1/projects/project/zones/zone/images</a>
GET	List Snapshots	<a href="https://www.googleapis.com/compute/v1/projects/project/zones/zone/snapshots">https://www.googleapis.com/compute/v1/projects/project/zones/zone/snapshots</a>
GET	List VM Instances	<a href="https://www.googleapis.com/compute/v1/projects/project/zones/zone/instances">https://www.googleapis.com/compute/v1/projects/project/zones/zone/instances</a>

# Hana Db

## Databases TCP Ports

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

Protocol: TCP

Operation	Usage description	Objects and parameters
connect	The probe host must not be blocked by ACL	socket

## HanaDb Connection by SQL

The job this adapter discovers databases using SQL protocol.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Check HanaDb database version	sys.m_database

## HanaDb Topology by SQL

The job discovers HanaDB instances and topology using SQL Connections.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Query information about the database	SYSINFO.ACTIVECONFIGURATION SYSINFO.VERSION SYSINFO.INSTANCE
select	Query information about DB users	DOMAIN.USERS
select	Query information about DB schemas	DOMAIN.SCHEMAS
select	Query information about DB trace files	SYSINFO.ACTIVECONFIGURATION
select	Query information about DB log files	SYSINFO.LOGVOLUMES
select	Query information about DB data files	SYSINFO.DATAVOLUMES
select	Query information about database configurations	SYSINFO.ACTIVECONFIGURATION

## HanaDb by Shell

The job discover HanaDb instances.

Protocol: shell

Operation	Usage description	Objects and parameters
exec	Execution of sql queries	\$hana_database_HOME/hdbclient/hdbsql -U -j



# **IDS Scheer ARIS**

## **Import CIs from ARIS**

The job populates CIs from IDS Scheer ARIS using an XML export file from ARIS.

Permissions information is unavailable or no permissions are required.

# Integration - Aperture Vista

## Vista Integration by SQL

The job discovers Aperture VISTA data centers and power infrastructure using the Aperture VISTA Database.

Protocol: sqlprotocol

Operation	Usage description	Objects and parameters
select	Datacenter and Power infrastructure	dbo.vip_dal_dv_devices
select	Power connections between HOST and PDU	dbo.vip_dal_pwr_device_power_sources

# Integration - EMC Control Center

## ECC Integration by SQL

The job populates 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 connects to the NNMi web service and populates 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	<p>http://&lt;nnm_server&gt;:&lt;port&gt;/IPv4AddressBeanService/IPv4AddressBean: getIPv4Addresses() offset, maxObjects</p> <p>http://&lt;nnm_server&gt;:&lt;port&gt;/InterfaceBeanService/InterfaceBean: getInterfaces() offset, maxObjects</p> <p>http://&lt;nnm_server&gt;:&lt;port&gt;/NmsSdkService/PortBean: getPorts() offset, maxObjects</p> <p>http://&lt;nnm_server&gt;:&lt;port&gt;/VLANBeanService/VLANBean: getVLANs() offset, maxObjects</p> <p>http://&lt;nnm_server&gt;:&lt;port&gt;/NmsSdkService/CardBean: getCards() offset, maxObjects</p> <p>http://&lt;nnm_server&gt;:&lt;port&gt;/L2ConnectionBeanService/L2ConnectionBean: getL2Connections() offset, maxObjects</p> <p>http://&lt;nnm_server&gt;:&lt;port&gt;/IPv4SubnetBeanService/IPv4SubnetBean: getIPv4Subnets() offset, maxObjects</p> <p>http://&lt;nnm_server&gt;:&lt;port&gt;/NodeBeanService/NodeBean: getNodes() offset, maxObjects</p>

### Update Ids in NNM

The job 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 Storage Essentials SRM database.

Protocol: sqlprotocol

Operation	Usage description	Objects and parameters
select	Get Storage Essentials version	SE version: appiq_system.version_info
select	Check if materialized views are being refreshed	Materialized view status for SE v6.10 to 9.3: appiq_system.mview_module_status  Materialized view status for SE v6.03 to 6.09: appiq_system.mview_status and appiq_system.mviewcore_status  Materialized view status for SE v6.0 to 6.02: appiq_system.mview_status  Materialized view status for SE v9.4 and above: appiq_system.mv_report_user_status
select	Fiber Channel Switch details	Additional FC Switch data: appiq_system.mvc_switichconfigvw  Fiber Channel Port: appiq_system.mvc_portsummaryvw  Fiber Channel Switch: appiq_system.mvc_switchsummaryvw
select	Storage Array details	Storage Pool: appiq_system.mvc_storagepoolconfigvw  Fiber Channel Port: appiq_system.mvc_portsummaryvw  Host Bus Adapter: appiq_system.mvc_cardssummaryvw  Logical Volume: appiq_system.mvc_storagevolumessummaryvw  Storage Processor: appiq_system.mvc_storageprocessorssummaryvw  Storage Array: appiq_system.mvc_storagesystemssummaryvw
select	Host/Server details	Fiber Channel Port: appiq_system.mvc_portsummaryvw  Additional host data: appiq_system.mvc_hostsummaryvw  Additional Logical Volume data: appiq_system.mvc_hostcapacityvw  Logical Volume: appiq_system.mvc_hostvolumessummaryvw  Host: appiq_system.mvc_assetsummaryvw

select	Depend links between Logical Disks and Logical Volumes	appiq_system.mvc_subpathvw appiq_system.mvc_storagevolumeports appiq_system.mvc_diskdrivesummaryvw appiq_system.mvc_pathvw appiq_system.mvc_protocolcontrollervw
select	FC connect links between FC Ports	appiq_system.mvc_portsummaryvw
select	Realization links between Storage Array Volumes	appiq_system.mvc_subpathvw
select	ExecutionEnvironment links between switches	appiq_system.mvc_switchsummaryvw

# Inventory Discovery

## Agent Driven Inventory Discovery

The job this adapter executed hardware and installed software inventory discovery by agent driven scanners.

Permissions information is unavailable or no permissions are required.

## Call Home Processing

The job call Home Processing.

Permissions information is unavailable or no permissions are required.

## Inventory Discovery by Manual Scanner Deployment

The job this adapter executed hardware and installed software inventory discovery by manually deployed scanfile.

Permissions information is unavailable or no permissions are required.

## Inventory Discovery by Scanner

The job this adapter executed hardware and installed software inventory discovery by scanners.

Permissions information is unavailable or no permissions are required.

## J2EE - JBoss

### JEE JBoss by Shell

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

Protocol: Shell

Operation	Usage description	Objects and parameters
select	Basic Login and Env Setup	UNIX: echo \$SHELL \$?  UNIX: uname -a -r  UNIX: locale -a  UNIX: set ComSpec  UNIX: date +%z  Windows: ver  Windows: wmic OS Get CodeSet OS Get OSLanguage
select	Discover files and JBoss AS details	Windows: dir <folder_path> /Q /-C /b "<folder_path>" /b "<file_path>"  UNIX: ls -lA <folder_path>  Windows: attrib <file_path>  Windows: cd /D <file_path>  UNIX: cat <file_path>  UNIX: ps -eo user,pid,lstart,command --cols 2530 --no-headers  UNIX: perl -e  Windows: type <file_path>  Windows: cmd /V:ON /c  Windows: wmic path Win32_Process get ParentProcessId, commandLine, creationdate, executablepath, name, processId /value  java -version

### JEE TCP Ports

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



Protocol: TCP

Operation	Usage description	Objects and parameters
connect	The probe host must not be blocked by ACL	socket

## JEE JBoss Connections by JMX

The job this adapter 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,*
select	Discover JNP and RMI ports	jboss.system:service=Naming,*

## JEE JBoss by JMX

The job this adapter 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,* jboss.messaging.destination:service=Topic,* jboss.messaging.destination:service=Queue,* org.hornetq:module=JMS,type=Topic,* org.hornetq:module=JMS,type=Queue,* jboss.as:subsystem=messaging,hornetq-server=*,jms-topic=* jboss.as:subsystem=messaging,hornetq-server=*,jms-queue=*
select	Get JVM info	jboss.management.local:j2eeType=JVM,* jboss:type=Service,name=SystemProperties,* jboss.system:type=ServerInfo,*

select	Get Server info	jboss.system:type=ServerConfig,* jboss.system:type=Server,* jboss.as:core-service=server-environment,* jboss.as:management-root=server
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,* jboss.web:j2eeType=Servlet,* jboss.web:j2eeType=WebModule,*
select	Discover JNP and RMI ports	jboss:service=Naming,* jboss.as:socket-binding-group=*,socket-binding=*
select	Get Applications info	jboss.management.local:j2eeType=J2EEApplication,* jboss.as:deployment=*
select	Get JDBC DataSource info	jboss.jca:service=ManagedConnectionPool,* jboss.jca:service=ManagedConnectionFactory,* jboss.as:subsystem=datasources,data-source=*

# J2EE - Oracle Application Server

## Oracle Application Server by Shell

The job discovers Oracle Application Server.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic login	UNIX: echo \$SHELL \$?  UNIX: uname -a -r  UNIX: locale -a  UNIX: set ComSpec  UNIX: rmdir /s /q  UNIX: mkdir
exec	Fetch file content	Windows: dir <folder_path>\*.wsdl /s /b  Unix: cat <file_path>  Windows: type <file_path>  Unix: find -name '*.wsdl' -f
exec	Get required process	Unix: ps -e  FreeBSD: ps -ax  Windows: wmic process get commandLine /value  HPUX: ps -ef
exec	Get windows version	Windows: ver
exec	Get codepage information	Windows: wmic OS Get CodeSet OS Get OSLanguage  Windows: chcp

## Web Services by URL

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

Permissions information is unavailable or no permissions are required.

# J2EE - WebLogic

## JEE TCP Ports

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

Protocol: TCP

Operation	Usage description	Objects and parameters
connect	The probe host must not be blocked by ACL	socket

## JEE 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 Domain information	Type=DomainRuntime
select	Get Server Name, Listen Address and Version	Type=ServerRuntime

## JEE Weblogic by JMX

The job this adapter 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=JDBCCConnectionPool Type=JDBCDataSourceConfig Type=JDBCTxDataSource Type=JDBCDataSource
select	Get JMS info	Type=JDBCDataSourceConfig Type=JMSServer Type=JMSServerRuntime Type=JMSDestinationRuntime Type=JDBCTxDataSource Type=JDBCDataSource
select	Get Deployment info	Type=DeploymentTaskRuntime
select	Get Execute Queue info	Type=ExecuteQueue

## JEE 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
exec	Basic Login	UNIX: uname -a -r UNIX: echo \$? \$SHELL UNIX: locale -a UNIX: date +%z Windows: ver Windows: wmic OS

exec	Discover files and WL details	Windows: dir <folder_path> /Q /-C Windows: dir /b "<file_path>" Windows: cd /D "<folder_path>" Windows: cmd /V:ON /c UNIX: ls -lA <folder_path> Windows: attrib <file_path> UNIX: cat <file_path> Windows: type <file_path> UNIX: ps -eo user,pid,lstart,command --cols 2530 --no-headers Windows: wmic path Win32_Process get ParentProcessId, commandLine, creationdate, executablepath, name, processId UNIX: readlink UNIX: perl -e
------	-------------------------------	--

## Oracle Access Management Connection by Web Services

The job using HTTP credential to connect Oracle Access Management.

Permissions information is unavailable or no permissions are required.

## Oracle Access Management Policies by Web Services

The job get Oracle Access Management policies.

Permissions information is unavailable or no permissions are required.

## Web Services by URL

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

Permissions information is unavailable or no permissions are required.

## J2EE - WebSphere

### JEE Inactive WebSphere by Shell

The job this adapter discovers WebSphere J2EE environment and components by shell only when the WebSphere Application Server is inactive.

Permissions information is unavailable or no permissions are required.

### JEE TCP Ports

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

Protocol: TCP

Operation	Usage description	Objects and parameters
connect	The probe host must not be blocked by ACL	socket

### JEE WebSphere Connections by JMX

The job this adapter 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,* *:type=JVM,*

### JEE WebSphere Liberty Core by Shell

The job this adapter discovers WebSphere Liberty Core J2EE environment and components by shell.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic Login	UNIX: uname -a -r UNIX: echo \$? \$SHELL UNIX: locale -a UNIX: date +%z Windows: ver Windows: wmic OS
exec	Discover files and WAS details	java -version Windows: dir <folder_path> /Q /-C Windows: dir /b "<file_path>" Windows: cd /D "<folder_path>" Windows: cmd /V:ON /c UNIX: ls -lA <folder_path> Windows: attrib <file_path> UNIX: cat <file_path> UNIX: find <folder_path> Windows: type <file_path> UNIX: ps -eo user,pid,lstart,command --cols 2530 --no-headers Windows: wmic path Win32_Process get ParentProcessId, commandLine, creationdate, executablepath, name, processId UNIX: readlink UNIX: perl -e

## JEE WebSphere by Shell

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

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic Login	UNIX: uname -a -r UNIX: echo \$? \$SHELL UNIX: locale -a UNIX: date +%z Windows: ver Windows: wmic OS



exec	Discover files and WAS details	<pre> java -version  Windows: dir &lt;folder_path&gt; /Q /-C  Windows: dir /b "&lt;file_path&gt;"  Windows: cd /D "&lt;folder_path&gt;"  Windows: cmd /V:ON /c  UNIX: ls -lA &lt;folder_path&gt;  Windows: attrib &lt;file_path&gt;  UNIX: cat &lt;file_path&gt;  UNIX: find &lt;folder_path&gt;  Windows: type &lt;file_path&gt;  UNIX: ps -eo user,pid,lstart,command --cols 2530 --no-headers  Windows: wmic path Win32_Process get ParentProcessId, commandLine, creationdate, executablepath, name, processId  UNIX: readlink  UNIX: perl -e </pre>
------	--------------------------------	--

## JEE WebSphere by Shell or JMX

The job this adapter discovers WebSphere J2EE environment and components.

Protocol: JMX

Operation	Usage description	Objects and parameters
select	Get Server info	<pre> *:type=Server,*  *:type=JVM,* </pre>
select	Get Cluster info	<pre> *:type=Cluster,* </pre>
select	Get Applications info	<pre> *:type=Application,*  *:type=WebModule,*  *:type=EjbModule,* </pre>
select	Get JMS Server info	<pre> *:type=JMSServer,* </pre>
select	Get JDBC Provider info	<pre> *:type=JDBCProvider,*  *:type=DataSource,* </pre>

## JEE - Glassfish

### JEE Glassfish by Shell

The job this adapter discovers Glassfish JEE environment and components using shell.

Protocol: Shell

Operation	Usage description	Objects and parameters
select	Basic Login	Windows: wmic OS Get CodeSet OS Get OSLanguage  Windows: cmd /V:ON /c  UNIX: uname  Windows: ver
select	Discover Java	Windows,UNIX: java -version
select	Discover files	Windows: dir /Q /A /-C "<folder_path>" /b "<file_path>"  Windows: wmic datafile where "name = '<file_path>' " get InstallDate /format:list datafile where "name = '<file_path>' " get LastModified /format:list datafile where "name = '<file_path>' " get version /format:list  UNIX: ls -lA <folder_path>  Windows: attrib <file_path>  UNIX: cat <file_path>  Windows: cd /D <file_path>  Windows: type <file_path>
select	Discover processes	Windows: wmic path Win32_Process get ParentProcessId, commandLine, creationdate, executablepath, name, processId /value

# Kubernetes

## Kubernetes Discovery by RESTful API

The job kubernetes Discovery using RESTful API.

Protocol: HTTP

Operation	Usage description	Objects and parameters
API Access		image top inspect containers version info

# **Mainframe - EView Agent**

## **CICS by EView**

The job this adapter discovers the IBM mainframe CICS subsystem along with its resources using the EView mainframe agent.

Permissions information is unavailable or no permissions are required.

## **DB2 by EView**

The job this job discovers the IBM mainframe DB2 subsystem along with its resources using the EView mainframe agent.

Permissions information is unavailable or no permissions are required.

## **EView Connection**

The job this job discovers the configured LPARs in the EView Client Application installed on the discovery probe.

Permissions information is unavailable or no permissions are required.

## **IMS by EView**

The job this adapter discovers the IBM mainframe IMS subsystem along with its resources using the EView mainframe agent.

Permissions information is unavailable or no permissions are required.

## **LPAR Resources by EView**

The job this job discovers the IBM mainframe z/OS host and network resources using the EView mainframe agent.

Permissions information is unavailable or no permissions are required.

## **MQ by EView**

The job this adapter discovers the IBM mainframe MQ subsystem along with its resources using the EView mainframe agent.

Permissions information is unavailable or no permissions are required.

# MaxDB

## Databases TCP Ports

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

Protocol: TCP

Operation	Usage description	Objects and parameters
connect	The probe host must not be blocked by ACL	socket

## MaxDb Connection by SQL

The job this adapter discovers databases using SQL protocol.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Check MaxDb database version	version()

## MaxDb Topology by SQL

The job discovers MaxDB instances and topology using SQL Connections.

Protocol: SQL

Operation	Usage description	Objects and parameters
select	Query information about the database	SYSINFO.ACTIVECONFIGURATION SYSINFO.VERSION SYSINFO.INSTANCE
select	Query information about DB users	DOMAIN.USERS
select	Query information about DB schemas	DOMAIN.SCHEMAS
select	Query information about DB trace files	SYSINFO.ACTIVECONFIGURATION
select	Query information about DB log files	SYSINFO.LOGVOLUMES
select	Query information about DB data files	SYSINFO.DATAVOLUMES
select	Query information about database configurations	SYSINFO.ACTIVECONFIGURATION

## MaxDb by Shell

The job discovers MaxDB instances and topology.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic login	wmic OS Get CodeSet OS Get OSLanguage uname locale -a ver echo \$
exec	MaxDb Topology	UNIX: dbmcli db_enum  ALL: dbmcli auto_extend show autolog_show backup_history_list -c label,action,start,stop,pages,media db_state param_directgetall param_getvolsall scheduler_state user_getall  ALL: xuser list  UNIX: cat some.cfg  WIN: dbmcli.exe db_enum  ALL: bmcli dbm_getpath

# NetApp Filer

## NetApp Filer Connection by WebServices

The job this job discovers and connects to NetApp Filer.

Permissions information is unavailable or no permissions are required.

## NetApp Filer by WebServices

The job this adapter discovers volumes, shares and other details on a NetApp filer.

Protocol: NetApp

Operation	Usage description	Objects and parameters
Manage ONTAP WebService API	Get appliance details including CPU and backplane information. (Head information in a sysconfig -a command). I/O information is not included	system-get-info
Manage ONTAP WebService API	Get current ONTAPI major and minor versions	system-get-ontapi-version
Manage ONTAP WebService API	Get information about ipspaces including IP addresses and relevant IP details. (Requires 'vfiler' license)	ipspace-list-info
Manage ONTAP WebService API	Get values for optional parameters	options-get
Manage ONTAP WebService API	Get details on volumes in the appliance	volume-list-info-iter-start volume-list-info-iter-next volume-list-info-iter-end
Manage ONTAP WebService API	Get details on snapshots for a specified volume	snapshot-list-info
Manage ONTAP WebService API	Get snapvault details from the appliance. <SnapvaultLevel> can be 'primary' and/or 'secondary'	snapvault-<SnapvaultLevel>-relationship-status-list-iter-start snapvault-<SnapvaultLevel>-relationship-status-list-iter-next
Manage ONTAP WebService API	Get details on CIFS shares on this appliance (Requires 'cifs' license)	cifs-share-list-iter-start cifs-share-list-iter-next cifs-share-list-iter-end



Manage ONTAP WebService API	Get details on CIFS sessions on this appliance (Requires 'cifs' license)	cifs-session-list-iter-start cifs-session-list-iter-next cifs-session-list-iter-end
Manage ONTAP WebService API	Get details on NFS shares on this appliance	nfs-exportfs-list-rules
Manage ONTAP WebService API	Get details on vFilers	security-api-vfiler nfs-exportfs-list-rules-2
Manage ONTAP WebService API	Get details on network interfaces	system-cli cli-ifconfig
Manage ONTAP WebService API	Get details on ISCSI	iscsi-adapter-list-info iscsi-node-get-name iscsi-interface-list-info iscsi-connection-list-info iscsi-adapter-initiators-list-info
Manage ONTAP WebService API	Gets information such as nodename/portname and link state about all the Fibre Channel target adapters	fc-adapter-list-info
Manage ONTAP WebService API	Get disk/array LUN status information from RAID	disk-list-info
Manage ONTAP WebService API	Get the status (size, online/offline state, shared state, comment string, serial number, LUN mapping) of all LUNs	lun-list-info
Manage ONTAP WebService API	Get aggregate status	aggr-list-info
Manage ONTAP WebService API	Returns the cluster identity information	cluster-identity-get
Manage ONTAP WebService API	Obtain the node information when the node is a part of the cluster in an iteration	system-get-node-info-iter
Manage ONTAP WebService API	Display information about Vservers. Information about Admin Vserver, Node Vserver, and Cluster Vservers is displayed	vserver-get-iter
Manage ONTAP WebService API	Iterate over a list of network interface objects	net-interface-get-iter
Manage ONTAP WebService API	Get information on what possibilities and parameters exist for aggregates on a given filer	aggr-get-iter

Manage ONTAP WebService API	Iterate over a list of volume objects	volume-get-iter
Manage ONTAP WebService API	Get disk information about one or more disks, from the Storage Subsystem. Clustered ONTAP iterator APIs return all information about all disks in the cluster	storage-disk-get-iter
Manage ONTAP WebService API	Iterate over a list of lun objects	lun-get-iter
Manage ONTAP WebService API	Iterate over the list of iSCSI Services	iscsi-service-get-iter
Manage ONTAP WebService API	Iterate over a list of iSCSI Target Portal Group objects	iscsi-tpgroup-get-iter
Manage ONTAP WebService API	Iterate over a list of iSCSI Connection objects	iscsi-connection-get-iter
Manage ONTAP WebService API	Iterate over a list of remote iSCSI initiator objects	iscsi-initiator-get-iter
Manage ONTAP WebService API	Iterate over the list of FCP Services	fcv-service-get-iter
Manage ONTAP WebService API	Iterate over a list of FCP Target Logical Interfaces (LIF)	fcv-interface-get-iter
Manage ONTAP WebService API	List all initiators connected to FCP target LIFs	fcv-initiator-get-iter
Manage ONTAP WebService API	Iterate over a list of snapshot objects	snapshot-get-iter
Manage ONTAP WebService API	Retrieve the list of CIFS servers on the cluster and their basic configurations	cifs-server-get-iter
Manage ONTAP WebService API	Gives information about one or more CIFS shares	cifs-share-get-iter
Manage ONTAP WebService API	Retrieve the list of the established CIFS sessions	cifs-session-get-iter

# NetApp SANscreen

## SANscreen Integration by WebService

The job this adapter discovers storage devices and SAN infrastructure from NetApp SANscreen/OnCommand.

Protocol: SANscreen

Operation	Usage description	Objects and parameters
Web Service calls	Permission to access SANscreen web service API	<p>Get information on Logical Volumes: <code>getVolumesByStorageArray()</code></p> <p>Get information on Fiber Channel Switches: <code>getSwitches()</code></p> <p>Login and establish a session with the SANscreen WebService API: <code>openSession()</code></p> <p>Get pathing information in the fiber channel network: <code>getPathsByHost()</code></p> <p>Get information on servers and hosts: <code>getHosts()</code></p> <p>Close the webservice session and exit gracefully: <code>closeSession()</code></p> <p>Get information on HBAs and Storage Processors: <code>getNodesOfDevice()</code></p> <p>Get information on Fiber Channel Ports: <code>getPortsOfDevice()</code></p> <p>Get information on Storage Arrays: <code>getStorageArrays()</code></p>

## Network - Basic

### Arp Table by SNMP

The job this adapter 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.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	HSRP group virtual IPs	iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoHsrpMIB.ciscoHsrpMIBObjects.cHsrpGroup.cHsrpGrpTable: 1.3.6.1.4.1.9.9.106.1.2.1

### Class B IPs by ICMP

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

Permissions information is unavailable or no permissions are required.

## Class C IPs by ICMP

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

Permissions information is unavailable or no permissions are required.

## Client Connection by SNMP

The job this job could collect ARP cache availability attribute by SNMP.

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,sysDesc,sysObjectID
get	Interfaces info	iso.org.dod.internet.mgmt.mib- 2.interfaces.ifTable.ifEntry: 1.3.6.1.2.1.2.2.1
get	ARP cache info	iso.org.dod.internet.mgmt.mib- 2.ip.ipNetToMediaTable.ipNetToMediaEntry: .1.3.6.1.2.1.4.22.1
get	HPE iLO cards	HPE iLO cards table: 1.3.6.1.4.1.232.9.2.5.1
get	Dell DRAC cards	Dell DRAC interfaces table: 1.3.6.1.4.1.674.10892.1.1900.30  Dell DRAC cards table: 1.3.6.1.4.1.674.10892.1.1900.10
get	EntPhysicalTable	entPhysicalSerialNum: 1.3.6.1.2.1.47.1.1.1.1.11

## DNS Resolver

The job discover DNS names on IPs and hosts.

Permissions information is unavailable or no permissions are required.

## **IP MAC Harvesting by SNMP**

The job this adapter collects IP MAC mapping by SNMP and reports delta information to UCMDB.

Permissions information is unavailable or no permissions are required.

## **Manual UriEndpoint Discovery**

The job this adapter discovers UriEndpoint CIs.

Permissions information is unavailable or no permissions are required.

## **Range IPs by ICMP**

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

Permissions information is unavailable or no permissions are required.

## **Range IPs by nmap**

The job this adapter performs an IP ping scan on probe range(s) by NMAP tool.

Permissions information is unavailable or no permissions are required.

# Network - Credentialless Discovery

## Host Fingerprint using nmap

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

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Host discovery using nmap (pcap dependency should be installed)	nmap.exe -O -ossan-guess -sS -sV --host_timeout 600000

## Microsoft Windows Domains

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

Permissions information is unavailable or no permissions are required.

## Microsoft Windows Domains Topology

The job discovers hosts on Microsoft Domain.

Permissions information is unavailable or no permissions are required.

# Network - DNS

## DNS Zone by DNS

The job discovers the DNS Resource Record topology of DNS Zone by querying name server from local shell (Probe) via DNS protocol.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec		ver  wmic OS Get CodeSet OS Get OSLanguage  nslookup

Protocol: DNS

Operation	Usage description	Objects and parameters
transfer zone records	DNS server should be configured to allow probe query name server for DNS Zone transfer	ls -d <domain name>

## DNS Zone by nslookup

The job discovers the DNS Resource Record topology of DNS Zone by querying name server using remote shell.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	List DNS Zones	Unix: ps -ef  Windows: reg query "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\DNS Server\Zones"  Unix: cat <name server configuration file path>
exec	Transfer zone by root domain	Windows: nslookup ls -d <domain>  Unix: dig @<server> <domain> axfr



## 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 locale info	wmic OS Get CodeSet OS Get OSLanguage
exec	Getting server and domain info	nslookup - echo exit
exec	Getting DNS info	nslookup {DNSServerName} ls -d {DNSServerName}
exec	Getting DNS info on non Windows	dig {DNSServerName} {ZoneName}

## Hosts using nslookup on Probe

The job discover hosts executing 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}

## Network - HP NonStop

### HPE NonStop Topology by Shell

The job hPE NonStop topology discovery.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Entering the SQL/MX Conversational Interface	mxci
set	Schema setting	schema nonstop_sqlmx_node_name.system_schema;
select	Selecting catalogs	select cat_name, cat_uid from catsys;
select	Selecting schemas	select schema_name, cat_uid from schemata;
exec	Entering the SQL Conversational Interface	gtac1 -p sqlci
exec		fileinfo \$system.system.sqlci2, detail;
select		select catalogname from name.catalogs

# Network - Host Resources and Applications

## Host Resources by PowerShell

The job discovers host resources, process connectivity and software elements on Windows machines using PowerShell protocol.

Protocol: PowerShell

Operation	Usage description	Objects and parameters
exec	Basic login	ver hostname
exec	Shared resources	wmic path Win32_Share get Description, Name, Path
exec	CPU	For Windows 2008: wmic path Win32_Processor get DeviceId,MaxClockSpeed,Manufacturer,LoadPercentage,Name,NumberOfCores  wmic path Win32_Processor get DeviceId,MaxClockSpeed,Manufacturer,LoadPercentage,Name,SocketDesignation
exec	Windows information	Language: wmic OS Get OSLanguage  Codepage: wmic OS Get CodeSet  wmic path Win32_OperatingSystem get BuildNumber, Caption, Version, csdversion, lastBootUpTime, organization, otherTypeDescription, registeredUser, totalVisibleMemorySize  wmic path Win32_ComputerSystem get Domain, Manufacturer, Model, Name, NumberOfProcessors
exec	File system	wmic logicaldisk get ProviderName, deviceId, driveType, freespace, size  dir %SystemRoot% /O:-D   find /I "system32"   Out-String -width 80
exec	Memory	Physical memory: wmic path Win32_PhysicalMemory get Capacity  Swap memory: wmic PAGEFILESET GET MaximumSize
exec	Processes	wmic Win32_Process get ParentProcessId, commandLine, creationdate, executablepath, name, processId
exec	User	wmic path Win32_UserAccount get Description, Disabled, Domain, FullName, Lockout, Name, SID

exec	Installed Software	wmic path Win32_Product get identifyingNumber, installDate, installLocation, name, vendor, version  For 32bit: reg query HKEY_LOCAL_MACHINE\SOFTWARE\Micros oft\Windows\CurrentVersion\Uninstall /S  For 64bit: reg query HKEY_LOCAL_MACHINE\SOFTWARE\Wow6 432Node\Microsoft\Windows\CurrentVersion\ Uninstall /S
exec	Windows Services	reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentC ontrolSet\Services /S  wmic service get AcceptPause, Description, DisplayName, Name, PathName, ServiceType, StartMode, State
exec	TCP Connections Info	Windows (XP Onwards), Includes process to port info: netstat -noa  Windows (before XP): netstat -na
exec	Code Page Info	chcp

## Host Resources 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.lanmanag er.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 by Shell

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

Protocol: Registry

Operation	Usage description	Objects and parameters
read	Microsoft MQ Plugin	Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters\setup  Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Parameters\MachineCache  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSMQ\Setup
read	Microsoft Operations Manager Management Server Plugin	HKLM\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Agent Management Groups  HKLM\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Setup  HKLM\SOFTWARE\Microsoft\Microsoft Operations Manager\2.0\Setup  HKLM\SOFTWARE\Mission Critical Software\OnePoint\Configurations  HKLM\SOFTWARE\Microsoft\Microsoft Operations Manager\3.0\Server Management Groups  HKLM\Software\Microsoft\Microsoft Operations Manager  HKLM\SOFTWARE\Mission Critical Software\DASServer

Protocol: Shell

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

exec	Environment variables query and setup, data parsing and processing	<p>Windows: set PATH=%PATH%;%WINDIR%\system32\wbem\</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: echo \$SHELL</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: echo \$?</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: grep .*</p> <p>AIX: egrep .*</p> <p>AIX: ioscli .*</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: awk .*</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: nice .*</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: export .*</p>
exec	Basic login	<p>AIX,FreeBSD,HP-UX,Linux,SunOS: uname -a</p> <p>AIX: uname -M</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: uname</p> <p>Unix: /usr/ios/cli/ioscli uname -L</p> <p>ver</p> <p>Windows: wmic OS Get Caption OS Get CodeSet OS Get OSLanguage path Win32_ComputerSystem get Name /value</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: locale -a</p>
exec	Fibre Channel info	<p>VIO AIX: command -v lsdev fcstat</p> <p>AIX: command -v lsdev lscfg /usr/sbin/lscfg fcstat</p> <p>VIO AIX: lsdev --help -type adapter -field name -vpd -dev fcsx</p> <p>AIX: lsdev --help -C -c adapter -r name</p> <p>AIX: lscfg usage lscfg -v -p -l fcsx</p> <p>AIX: lslpp -l '*&lt;driverid&gt;.rte'</p> <p>VIO AIX: lslpp -l '*&lt;driverid&gt;.rte'</p> <p>AIX: fcstat fcsx</p> <p>VIO AIX: fcstat fcsx</p> <p>HP_UX: ioscan -f -n -C fc</p> <p>HP_UX: fcmsutil &lt;port_name&gt; &lt;port_name&gt; vpd &lt;port_name&gt; get remote all</p> <p>SunOS: fcinfo -? hba-port remote-port -p &lt;port_name&gt;</p> <p>Windows: wmic /namespace:\\root\WMI path MSFC_FCAdapterHBAAttributes get Active, DriverVersion, FirmwareVersion, InstanceName, Manufacturer, Model, ModelDescription, NodeWWN, SerialNumber, UniqueAdapterId /value /namespace:\\root\WMI path MSFC_FibrePortHBAAttributes get Active, Attributes, HBASatus, InstanceName, UniquePortId /value</p>

exec	iSCSI Info	<p>Windows: wmic /namespace:\\root\\Microsoft\\Windows\\Storage path MSFT_iSCSI Session get InitiatorNodeAddress, SessionIdentifier, TargetNodeAddress /value</p> <p>/namespace:\\root\\Microsoft\\Windows\\Storage path MSFT_iSCSI SessionToDisk get Disk, iSCSI Session /value</p> <p>/namespace:\\root\\Microsoft\\Windows\\Storage path MSFT_Disk get FriendlyName, Number, ObjectId, Path, SerialNumber, Size /value</p> <p>/namespace:\\root\\Microsoft\\Windows\\Storage path MSFT_Partition get AccessPaths, DiskId, DiskNumber, DriveLetter, Size /value</p>
exec	CPU Info	<p>AIX: lsattr -El &lt;procId&gt;</p> <p>Windows: wmic cpu get * /translate:basicxml /format:rawxml.xml cpu get DeviceId,MaxClockSpeed,Manufacturer,LoadPercentage,Name,NumberOfCores /translate:basicxml /format:rawxml.xml cpu get DeviceId,MaxClockSpeed,Manufacturer,LoadPercentage,Name,SocketDesignation /translate:basicxml /format:rawxml.xml path Win32_Processor get DeviceId, LoadPercentage, Manufacturer, MaxClockSpeed, Name, SocketDesignation /value</p> <p>HP-UX: echo itick_per_usec/D   /usr/bin/adb -k /stand/vmunix /dev/kmem   /usr/bin/tail -n 1</p> <p>HP-UX: echo "sc product cpu;il"   /usr/sbin/cstm   grep 'CPU Module'</p> <p>FreeBSD: dmesg   grep "cpu\\ Multiprocessor"   grep -A 1 "CPU:"</p> <p>Linux: cat /proc/cpuinfo</p> <p>Windows: reg query HKEY_LOCAL_MACHINE\\HARDWARE\\DESCRIPTION\\System\\CentralProcessor /S</p> <p>FreeBSD: sysctl hw.model hw.ncpu hw.clockrate</p> <p>SunOS: /usr/sbin/psrinfo -v</p> <p>HP-UX: model</p> <p>SunOS: prtconf</p> <p>AIX: prtconf   grep "proc"</p> <p>AIX: lscfg -vpl sysplanar0   grep PROC</p> <p>HP-UX,SunOS: kstat -p cpu_info</p>

exec	Memory Info	<p>Linux: free -m</p> <p>Windows: wmic path Win32_PhysicalMemory get Capacity /format:csv MEMORYCHIP get Capacity /format:csv &lt; %SystemRoot%\win.ini PAGEFILESET GET MaximumSize /format:list &lt; %SystemRoot%\win.ini wmic path Win32_OperatingSystem get BuildNumber, Caption, Version, csdversion, lastBootUpTime, organization, otherTypeDescription, registeredUser, totalVisibleMemorySize /value</p> <p>HP-UX: swapinfo -tm   grep total</p> <p>HP-UX: echo "selclass qualifier memory;info;wait;infolog"   cstm   grep "Total Configured Memory"</p> <p>AIX: swap -s</p> <p>HP-UX: grep Physical /var/adm/syslog/syslog.log</p> <p>HP-UX: print_manifest   grep Memory</p> <p>SunOS: prtconf</p> <p>HP-UX: ls /usr/contrib/bin/machinfo</p> <p>HP-UX: /usr/contrib/bin/machinfo -v</p> <p>Windows: meminfo.exe</p> <p>FreeBSD: dmesg   grep \'real memory\'</p> <p>FreeBSD: swapinfo -m</p> <p>FreeBSD: sysctl hw.physmem</p> <p>AIX: prtconf   grep \'^Memory\'   awk \'{print \$1,\$3,\$4}\'</p> <p>VMKernel: esxcfg-info -F xml   sed -n \'/&lt;memory-info&gt;/,&lt;/memory-info&gt;/p\'</p> <p>SunOS: swap -l</p>
exec	Disks info	<p>Windows: wmic path win32_logicaldisk get ProviderName, deviceId, driveType, freespace, size /value</p> <p>Windows: diskinfo.exe</p> <p>AIX,HP-UX,Linux,SunOS: df -P -k -k   awk \'{print \$1,\$2,\$3,\$4,\$5,\$6}\'</p>
exec	Users info	<p>AIX,FreeBSD,HP-UX,Linux,SunOS: cat /etc/passwd</p> <p>Windows: wmic path Win32_UserAccount where "Domain = '&lt;host_name&gt;'" get Description, Disabled, Domain, FullName, Lockout, Name, SID /value</p>



exec	Processes info	<p>Windows: wmic path Win32_Process get commandLine, creationdate, executablepath, name, processId /value</p> <p>Windows: processlist.exe</p> <p>SunOS: zonename</p> <p>AIX, Linux, SunOS: uname -r</p> <p>SunOS: ps -agxwwu -e -o pid -o zone</p> <p>HP-UX: ps -ef</p> <p>AIX, FreeBSD, HP-UX, Linux: ps -ax -o pid,uid,user,cputime,command -e -o 'user,pid,time,args' -ef -eo user,pid,lstart,command --cols 4000 --no-headers</p> <p>Linux: date +%z</p> <p>SunOS: pkgchk -l -p</p> <p>VMKernel: esxcfg-info -F xml   sed -n \/&lt;vmfs-fileSystems&gt;/,&lt;\vmfs-fileSystems&gt;/p\"</p>
exec	Installed Software info	<p>AIX: lspp -Lc -q</p> <p>HP-UX: swlist -a name -a revision -a title -a install_date -a vendor_tag</p> <p>UNIX: pkg_info -a -I</p> <p>Windows: reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall /S</p> <p>Windows: wmic path Win32_QuickFixEngineering where "InstalledBy != "" get HotFixID, InstallDate /value</p> <p>UNIX: rpm -qa --qf '%{NAME}~%{VERSION}~%{RELEASE}~%{ARCH}~%{GROUP}~%{VENDOR}~%{installtime:date}~%{INSTALLTID}\n'</p> <p>SunOS: pkginfo -l</p>
exec	Windows Services	<p>Windows: reg query HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services /S</p> <p>Windows: wmic path Win32_Service get AcceptPause, Description, DisplayName, Name, PathName, ServiceType, StartMode, State /value</p>
exec	Discover TCP Connections Info	<p>Windows (XP Onwards), Includes process to port info: netstat -noa</p> <p>HP-UX: nestat -num -routinfo</p> <p>AIX, HP-UX, SunOS, Includes process to port info: lsof -i -P -n</p> <p>Windows, AIX, FreeBSD, HP-UX, Linux, SunOS: netstat -na</p> <p>SunOS, HP-UX, only process to port info: pfiles for i in `ps -e   awk '{print \$1}'`; do echo __[\$i]; pfiles \$i   grep 'sockname: AF_INET'; done</p> <p>Linux, Includes process to port info: netstat -nap</p>
exec	Shared resources	<p>Windows: wmic share where "Path &lt;&gt; "" get description, name, path /value</p>

exec	File version and modification date information	<p>Windows: wmic datafile where "name = '&lt;file_path&gt;'" get LastModified /format:list datafile where "name = '&lt;formattedPath&gt;'" get version</p> <p>Linux: rpm -qa --qf '%{NAME}~%{VERSION}\n'   grep -i</p> <p>SunOS: /usr/sbin/pkgchk -l -p \"" + file_path + ""\</p> <p>Unix: perl -e 'print ((stat(\$ARGV[0]))[9],\"\\n\\n\");' &lt;file_path&gt;</p> <p>Linux: rpm -qf "&lt;file_path&gt;" --qf '%{NAME}\\n' -qf "&lt;file_path&gt;" --qf '%{VERSION}\\n'</p> <p>Windows: Cscript.exe /nologo filever.vbs '+file_path+'</p>
exec	File location information	<p>Unix: which "&lt;file_name&gt;"</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: whereis -b "&lt;file_name&gt;"</p> <p>Unix: export "PATH=\$PATH:/opt/csw/bin:/opt/csw/sbin"</p>
exec	Postgres SQL plugin	postmaster --version
exec	Windows Registry read	<p>Windows: reg_mam &lt;path to key&gt; /S</p> <p>Windows: reg &lt;path to key&gt; /S</p>
exec	Plugins can execute nslookup for resolving host,	nslookup <hostname>
exec	HP-UX specific commands	<p>HP-UX: lstcpip -hostname</p> <p>HP-UX: cat /etc/hostname</p> <p>HP-UX: cat /etc/nodename</p> <p>HP-UX: lstcpip -interfaces</p> <p>HP-UX: netstat -num -routinfo</p> <p>HP-UX: lsmap -all -net</p> <p>HP-UX: lsdev -dev &lt;entry&gt; -attr</p>
exec	Service Guard by Shell plugin	<p>Unix: swlist   grep Serviceguard</p> <p>Unix: /usr/sbin/swlist   grep Serviceguard</p>
exec	Plugins can check if file exist	Unix: ls <file_name>
exec	Plugins can read file content	type <file_name>
exec	Set environment variable	<p>Windows: set &lt;variableName&gt;=&lt;variableValue&gt;</p> <p>Unix: export &lt;variableName&gt;=&lt;variableValue&gt;</p>
exec	DB version plugin	<p>Unix: type /etc/oratab</p> <p>sqlplus -v</p> <p>lsnrctl status</p>

exec	DB2 plugin	<p>Windows. Getting DB2 instance name by process pid: reg query "HKEY_LOCAL_MACHINE\SOFTWARE\IBM"</p> <p>Windows. Resetting ERRORLEVEL environment variable to 0: cmd.exe /c "exit /b 0"</p> <p>Unix. Setting DB2INSTANCE environment variable: export DB2INSTANCE="&lt;db2_instance_name&gt;"</p> <p>Getting version information: db2level</p> <p>Windows: db2cmd -c -w -i</p> <p>Getting Db2Instance, Db2Database and Db2Alias details: db2 list db directory list dcs directory list node directory show detail get dbm cfg</p> <p>Windows: find</p> <p>Windows: findstr</p> <p>Unix: grep</p> <p>Unix: echo ~&lt;db2_instance_name&gt;</p>
------	------------	--

## Host Resources by WMI

The job this adapter 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 Win32_PhysicalMemory
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
select	Fibre Channel info	root\WMI MSFC_FCAdapterHBAAttributes MSFC_FibrePortHBAAttributes

select	Windows Storage info	root\Microsoft\Windows\Storage MSFT_iSCSI Session MSFT_Partition MSFT_Disk MSFT_iSCSI SessionToDisk
--------	----------------------	---

# Network - HostConnection

## Host Connection by PowerShell

The job this adapter discovers PowerShell agents by trying to connect to a Windows machine using the PowerShell protocol.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Discover Basic Host Info	hostname
exec	Discover OS version info	Windows: ver
exec	Discover Host OS details	Windows: Get-WmiObject -Query "SELECT BuildNumber, Caption, Version, csdversion, lastBootUpTime, organization, otherTypeDescription, registeredUser, totalVisibleMemorySize FROM Win32_OperatingSystem"
exec	Discover network interfaces and IPs info	Windows: ipconfig /all
exec	Discover system locale and code page info	Windows: chcp Windows: wmic OS Get CodeSet OS Get OSLanguage
exec	Discover default gateway	Windows: Get-WMIObject -Query "SELECT nextHop, metric1 FROM Win32_IP4RouteTable WHERE destination = '0.0.0.0' and mask = '0.0.0.0'"
exec	Discover BIOS UUID and host model	Windows: Get-WmiObject -Query "SELECT name, uuid FROM win32_ComputerSystemProduct " -Query "SELECT smBiosAssetTag FROM Win32_SystemEnclosure "
exec	Discover host name	Windows: Nslookup
exec	Discover serial number	Windows: Get-WMIObject -Query "SELECT serialNumber FROM Win32_BIOS" -Query "SELECT serialNumber FROM Win32_SystemEnclosure"
exec	Discover system info	Windows: Get-WMIObject -Query "SELECT Manufacturer, Name, Model, Domain, NumberOfProcessors FROM Win32_ComputerSystem"

exec	Discover interface information	Windows: Get-WMIObject -Query "SELECT IPAddress, MACAddress, IPSubnet, Description, DhcpEnabled FROM Win32_NetworkAdapterConfiguration WHERE MACAddress <> NULL " -Query "SELECT DeviceID, Name FROM Win32_NetworkAdapter" -Query "SELECT Caption, Description, DhcpEnabled, IPAddress, IPSubnet, Index, MACAddress FROM Win32_NetworkAdapterConfiguration " -Query "SELECT dhcpServer FROM Win32_NetworkAdapterConfiguration WHERE dhcpServer <> NULL" -Query "SELECT WinsPrimaryServer, WinsSecondaryServer FROM Win32_NetworkAdapterConfiguration WHERE WinsPrimaryServer <> NULL or WinsSecondaryServer <> NULL" -Query "SELECT dnsServerSearchOrder FROM Win32_NetworkAdapterConfiguration WHERE domainDnsRegistrationEnabled <> NULL"
------	--------------------------------	---

## Host Connection by SNMP

The job discovers SNMP agents by trying to connect to a data center machine using the SNMP protocol, updates the node 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  iso.org.dod.internet.mgmt.mib-2.ipv6MIB.ipv6MIBObjects.ipv6AddrTable.ipv6AddrEntry: 1.3.6.1.2.1.55.1.8.1
get	Interfaces info	iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry: 1.3.6.1.2.1.2.2.1  iso.org.dod.internet.mgmt.mib-2.ifMIB.ifMIBObjects.ifXTable: 1.3.6.1.2.1.31.1.1
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
get	General Printer Table	iso.org.dod.internet.mgmt.mib-2.printmib.prtGeneral.prtGeneralTable: 1.3.6.1.2.1.43.5.1 prtGeneralPrinterName
get	Routes info	iso.org.dod.internet.mgmt.mib-2.ip.ipRouteTable: 1.3.6.1.2.1.4.21
get	Physical entity info	iso.org.dod.internet.mgmt.mib-2.entityMIB.entityMIBObjects.entityPhysical.entityPhysicalTable: 1.3.6.1.2.1.47.1.1.1
get	HSRP group virtual IPs	iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoHsrpMIB.ciscoHsrpMIBObjects.cHsrpGroup.cHsrpGrpTable: 1.3.6.1.4.1.9.9.106.1.2.1

get	HPE iLO cards	HPE iLO cards table: 1.3.6.1.4.1.232.9.2.5.1
get	Dell DRAC cards	Dell DRAC interfaces table: 1.3.6.1.4.1.674.10892.1.1900.30  Dell DRAC cards table: 1.3.6.1.4.1.674.10892.1.1900.10
get	EntPhysicalTable	entPhysicalSerialNum: 1.3.6.1.2.1.47.1.1.1.1.11

## Host Connection by Shell

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

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Environment variables query and setup, data parsing and processing	<p>Windows: set PATH=%PATH%;%WINDIR%\system32\wbem\ComSpec</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS,VIO Server: echo \$SHELL</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS,VIO Server: echo \$?</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS,VIO Server: grep .*</p> <p>AIX: egrep .*</p> <p>AIX: ioscli</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: awk .*</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: cat ~/.discagnt/aioptionrc</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: export .*</p>
exec	Discover Basic Host Info	<p>AIX,HP-UX,Linux,SunOS: domainname</p> <p>SunOS: zonename</p> <p>Linux: dnsdomainname</p> <p>AIX,HP-UX,Linux,SunOS: hostname</p> <p>Windows: wmic path Win32_ComputerSystem get DNSHostName path Win32_OperatingSystem get PAEEnabled</p> <p>SunOS: cat /etc/nodename</p> <p>AIX: namerslv -s -n</p> <p>Linux: rpm -qa</p> <p>NXOS: sh ver   no-more</p> <p>NXOS: sh hostname   no-more</p>

exec	Discover Node Model	<p>HP-UX: model</p> <p>Linux: dmidecode -t system</p> <p>Linux: lshal</p> <p>AIX: uname -M</p>
exec	Discover OS version info	<p>AIX: oslevel -r</p> <p>AIX: ioslevel</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: uname</p> <p>HP-UX,Linux: uname -r</p> <p>SunOS: cat /etc/release</p> <p>Linux: cat /etc/redhat-release /etc/oracle-release /etc/SuSE-release</p> <p>HP-UX: swlist</p> <p>Windows: ver</p> <p>Windows: wmic path Win32_OperatingSystem get BuildNumber, Caption, Version, csdversion, lastBootUpTime, organization, otherTypeDescription, registeredUser, totalVisibleMemorySize</p> <p>NXOS: sh ver   no-more</p>
exec	Discover Host boot time info	<p>AIX,HP-UX,Linux,SunOS: uptime &amp;&amp; date -u '+%Y-%m-%d %H:%M:%S'</p> <p>UNIX: date '+%Y-%m-%d'</p> <p>Windows: wmic path Win32_OperatingSystem get BuildNumber, Caption, Version, csdversion, lastBootUpTime, organization, otherTypeDescription, registeredUser, totalVisibleMemorySize</p> <p>Windows: reg query "HKEY_CURRENT_USER\Control Panel\International" /v sShortDate</p> <p>UNIX: uptime</p> <p>Windows: net stats srv</p> <p>NXOS: sh ver   no-more</p>
exec	Discover host description	<p>Windows: reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /v "srvcomment"</p>



exec	Discover DNS, DHCP and WINS Information	<p>Windows: wmic path Win32_NetworkAdapterConfiguration where "domainDnsRegistrationEnabled &lt;&gt; NULL" get dnsServerSearchOrder /value</p> <p>Windows: wmic path Win32_NetworkAdapterConfiguration where "WinsPrimaryServer &lt;&gt; NULL or WinsSecondaryServer &lt;&gt; NULL" get WinsPrimaryServer, WinsSecondaryServer /value</p> <p>Windows: wmic path Win32_NetworkAdapterConfiguration where "dhcpServer &lt;&gt; NULL" get dhcpServer /value</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: cat /etc/resolv.conf</p> <p>SunOS,Linux: cat /etc/nsswitch.conf</p> <p>NXOS: sh hosts   no-more</p>
------	---	--

exec	Discover network interfaces and IPs info	AIX: ps -aef HP-UX: ioscan -FnkClan HP-UX: lanadmin -s SunOS,Linux: cat /etc/hosts HP-UX: netstat -in HP-UX: cat /etc/rc.config.d/netconf HP-UX: lanscan Windows: ipconfig /all Windows: wmic path Win32_NetworkAdapterConfiguration get Caption, Description, DhcpEnabled, IPAddress, IPSubnet, Index, MACAddress /value Windows: wmic path Win32_NetworkAdapter get DeviceID, Name /value SunOS: ifconfig -a HP-UX: ifconfig . * AIX: ifconfig -a inet AIX: entstat * AIX: lsdev -Cc adapter -S VIO Server: lsdev -type adapter -fmt VIO Server: lsmap -all -net VIO Server: lstcpip -interfaces AIX: lsdev -Cc adapter -F 'name:description' AIX: lscfg Linux: ip addr show Linux: ps aux SunOS: netstat -np SunOS: dladm show-dev show-aggr -p show-link -p show-linkprop -p zone NXOS: sh int   no-more
exec	Discover Virtualization Info	AIX: prtconf AIX LPARS: lparstat -i SunOS: /usr/bin/zonename Solaris Zones: ps -o zone IBM HMC: lshmc -V -n

exec	Discover Host Serial Number info	<p>Windows: reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion" /v "CurrentVersion"</p> <p>Windows: wmic path Win32_BIOS get serialNumber</p> <p>Windows: wmic path Win32_SystemEnclosure get serialNumber</p> <p>AIX: lsattr -El sys0 -a systemid</p> <p>VIO Server: lsdev -dev sys0 -attr systemid</p> <p>SunOS: sneep</p> <p>SunOS: eeprom nvramrc</p> <p>SunOS: hostid</p> <p>Linux,SunOS: dmidecode -t system</p> <p>Linux: lshal</p> <p>HP-UX: cstm</p> <p>HP-UX: getconf MACHINE_SERIAL</p>
exec	Discover Host Manufacture Info	<p>AIX: lsvpd</p> <p>Linux: dmidecode -t system</p> <p>Linux: lshal</p> <p>Windows: wmic path Win32_ComputerSystem get Domain, Manufacturer, Model, Name, NumberOfProcessors /value</p> <p>Windows: wmic path Win32_ComputerSystem get PartOfDomain /value</p> <p>SunOS: showrev</p> <p>SunOS: smbios -t SMB_TYPE_SYSTEM</p>
exec	Discover Host HW Architecture Info	SunOS: prtdiag
exec	Discover system locale and code page info	<p>Windows: chcp</p> <p>Windows: wmic OS Get CodeSet</p> <p>Windows: wmic OS Get OSLanguage</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS,VIO Server: locale -a</p>
exec	Discover Node Asset Tag	Windows: wmic path Win32_SystemEnclosure get smBiosAssetTag /value
exec	Discover Node Bios UUID	<p>Linux,SunOS: dmidecode -t system</p> <p>Linux: lshal</p> <p>Windows: wmic path win32_ComputerSystemProduct get name, uuid</p>
exec	Discover OS Name	<p>Windows: reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion" /v "ProductName"</p>

exec	Discover build number	Windows: reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion" /v "CurrentBuildNumber"
exec	Discover version and service pack information	Windows: reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion" /v "CSDVersion"
exec	Discover host default gateway	Windows: wmic path Win32_IP4RouteTable where "destination = '0.0.0.0' and mask = '0.0.0.0'" get metric1, Hop /value  AIX,FreeBSD,HP-UX,Linux,SunOS,Windows: netstat -r -n
exec	General information about HPE NonStop system	NonStop: gtacl -p scf sysinfo
exec	Information about HPE NonStop system IPs	NonStop: gtacl -p scf info subnet'\$*.*'
exec	Information about HPE NonStop system network interfaces	NonStop: gtacl -p scf info lif '\$zzlan.*'

## Host Connection by WMI

The job this adapter discovers WMI agents by trying to connect to a Windows machine using the WMI protocol.

Protocol: WMI

Operation	Usage description	Objects and parameters
select	Obtains basic host information	root\cimv2 Win32_BIOS Win32_BaseBoard Win32_ComputerSystem Win32_ComputerSystemProduct Win32_IP4RouteTable Win32_NetworkAdapterConfiguration Win32_OperatingSystem Win32_SystemEnclosure

## Host Connection to AS400

The job connects to the AS400 Server using the JT400 Toolbox.

Protocol: AS400

Operation	Usage description	Objects and parameters
-----------	-------------------	------------------------

get	Get System Information	*EXCLUDE *ADD *OBJMGT *SHRNUP *READ *EXECUTE *OBJEXIST SYSNAME QMODEL QSRLNBR
get	Get Network Information	*USE *EXCLUDE *ADD *OBJMGT *SHRNUP *READ *EXECUTE *CHANGE *OBJEXIST /QSYS.LIB/QUSRTVUS.PGM /QSYS.LIB/QSZRTVPR.PGM /QSYS.LIB/QUSDLTUS.PGM /QSYS.LIB/QUSCRTUS.PGM /QSYS.LIB/QTOCNETSTS.SRVPGM
get	Get Network Interface Information	*USE *EXCLUDE *ADD *OBJMGT *SHRNUP *READ *EXECUTE *CHANGE *OBJEXIST

# Network - HostPlatform

## Host Platform by Shell

The job discovers host platform detail on UNIX and Windows machines using SSH, NTCMD or UDA protocols.

Protocol: Shell

Operation	Usage description	Objects and parameters
powershell	Discover AWS External ID on Windows	
curl	Discover AWS External ID on Linux	

## 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  iso.org.dod.internet.mgmt.mib- 2.ifMIB.ifMIBObjects.ifXTable: 1.3.6.1.2.1.31.1.1  ifName: 1.3.6.1.2.1.31.1.1.1
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.dot1dBaseBridgeAddre ss: 1.3.6.1.2.1.17.1.1

### Layer2 Topology Bridge-based by SNMP

The job this adapter 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.dot1d StpPortEntry: 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.dot1dT pFdbEntry: 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 CDP-LLDP based by SNMP

The job this adapter discovers Layer 2 neighbors network devices.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	CDP info	iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoCdpMIB.ciscoCdpMIBObjects.cdpCacheTable.cdpCacheEntry: 1.3.6.1.4.1.9.9.23.1.2.1.1
get	LLDP info	so.std.iso8802.ieee802dot1.ieee802dot1mibs.lldpMIB.lldpObjects.lldpRemoteSystemsData.lldpRemTable.lldpRemEntry: 1.0.8802.1.1.2.1.4.1
get	Interfaces info	iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry: 1.3.6.1.2.1.2.2.1  iso.org.dod.internet.mgmt.mib-2.ifMIB.ifMIBObjects.ifXTable: 1.3.6.1.2.1.31.1.1

## Layer2 Topology VLAN-based by SNMP

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

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	System info	iso.org.dod.internet.mgmt.mib-2.system: 1.3.6.1.2.1.1
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  iso.org.dod.internet.mgmt.mib-2.dot1dBridge.qBridgeMIB.dot1qTp.dot1qTpFdbTable.dot1qTpFdbEntry.dot1qTpFdbPort: 1.3.6.1.2.1.17.7.1.2.2.1.2  iso.identified-organization.dod.internet.private.enterprise.hp.nm.icf.hpIcfObjects.hpIcfSwitch.hpSwitch.hpSwitchStatistics.hpSwitchFdbInfo.hpSwitchVlanFdbAddrTable.hpSwitchVlanFdbAddrEntry.hpSwitchVlanFdbPort: 1.3.6.1.4.1.11.2.14.11.5.1.9.4.1.1.3
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 by Shell

The job reports Layer2 and networking related data by ssh or shell from network switches.

Protocol: Read

Operation	Usage description	Objects and parameters
exec	Get interface details	sh int   no-more
exec	Get vlans and corresponding ports	sh vlan all-ports   no-more
exec	get Layer2 information	sh cdp neighbors detail   no-more

## Merge VLANs by Ports

The job used to create links between VLAN and physical ports across different switches in case the corresponding interfaces have connectivity. Connectivity between interfaces is determined based on the Layer2Connection CI presence.

Permissions information is unavailable or no permissions are required.

## Process Layer2 Saved Files

The job adapter Description.

Permissions information is unavailable or no permissions are required.

## Report Linux with Duplicated MAC Layer2

The job this adapter is acting as a port processing logic after the "Layer2 Vlan based by SNMP" Job has run.

Permissions information is unavailable or no permissions are required.

## VLAN ports by SNMP

The job discovers the physical ports on a VLAN.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	sysDescr	iso.org.dod.internet.mgmt.mib-2.system: 1.3.6.1.2.1.1
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 adapter discovers VLANs on a switch by SNMP.

Protocol: SNMP

Operation	Usage description	Objects and parameters
-----------	-------------------	------------------------

get	VLAN info	<p>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</p> <p>iso.org.dod.internet.mgmt.mib-2.dot1dBridge.qBridgeMIB.qBridgeMIBObjects.dot1qVlan.dot1qVlanStaticTable.dot1qVlanStaticEntry.dot1qVlanStaticName: 1.3.6.1.2.1.17.7.1.4.3.1.1</p> <p>iso.org.dod.internet.private.enterprises.hp.nm.icf.hpIcfObjects.hpIcfSwitch.hpSwitch.hpVLAN.hpVlanLevelOne.hpVlanObjects.hpVlanIdentTable.hpVlanIdentEntry.hpVlanIdentName: 1.3.6.1.4.1.11.2.14.11.5.1.3.1.1.4.1.2</p>
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
get	Bridges, Bridging type, Physical ports, Interfaces	<p>iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dBase: 1.3.6.1.2.1.17.1</p> <p>iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dBase.dot1dBasePortTable.dot1dBasePortEntry: 1.3.6.1.2.1.17.1.4.1</p> <p>iso.org.dod.internet.mgmt.mib-2.dot1dBridge.qBridgeMIB.qBridgeMIBObjects.dot1qVlan.dot1qPortVlanTable.dot1qPortVlanEntry.dot1qPvid: 1.3.6.1.2.1.17.7.1.4.5.1.1</p> <p>iso.org.dod.internet.private.enterprises.hp.nm.icf.hpIcfObjects.hpIcfSwitch.hpSwitch.hpVLAN.hpVlanLevelOne.hpVlanObjects.hpVlanMemberTable.hpVlanMemberEntry.hpVlanMemberIndex: 1.3.6.1.4.1.11.2.14.11.5.1.3.1.1.5.1.2</p>

## Network - Mainframe

### Mainframe TCP by SNMP

The job this adapter discovers IBM mainframe.

Protocol: snmp

Operation	Usage description	Objects and parameters
get	Discover TCP connections info (Resource name)	iso.org.dod.internet.private.enterprises.ibm.ibmP rod.mvsSNMPagent.ibmTCPIPmvsMIB.ibmTCPI PmvsMIBObjects.ibmTcpiMvsTcpGroup.ibmTc piMvsTcpConnTable.ibmTcpiMvsTcpConnEntry .ibmMvsTcpConnResourceName: 1.3.6.1.4.1.2.6.19.2.2.7.1.1.37
get	Discover TCP connections info (Subtask ID)	iso.org.dod.internet.private.enterprises.ibm.ibmP rod.mvsSNMPagent.ibmTCPIPmvsMIB.ibmTCPI PmvsMIBObjects.ibmTcpiMvsTcpGroup.ibmTc piMvsTcpConnTable.ibmTcpiMvsTcpConnEntry .ibmMvsTcpConnSubtask: 1.3.6.1.4.1.2.6.19.2.2.7.1.1.38

### Mainframe topology by SNMP

The job this adapter discovers IBM mainframe topology.

Permissions information is unavailable or no permissions are required.

# Network Connections - Active Discovery

## TCP Data by SNMP

The job collects network data by SNMP.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	Discover TCP Connections Info	iso.org.dod.internet.mgmt.mib-2.tcp: 1.3.6.1.2.1.6.13.1.1
get	Discover TCP Connections Info	hrSWRunName: 1.3.6.1.2.1.25.4.2.1.2
get	Discover TCP Connections Info	hrSWRunPath: 1.3.6.1.2.1.25.4.2.1.4
get	Discover TCP Connections Info	hrSWRunParameters: 1.3.6.1.2.1.25.4.2.1.5
get	Discover TCP Connections Info	hrSWRunStatus: 1.3.6.1.2.1.25.4.2.1.7
get	Discover TCP Connections Info	tcpConnLocalAddress: 1.3.6.1.2.1.6.13.1.2

## TCP Data by Shell

The job collects TCP data by Shell.

Protocol: Shell

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

exec		<p>HP-UX, LINUX, SunOS, Get environment variables: echo &lt;variable&gt;</p> <p>LINUX, Get time zone: date +%z</p> <p>HP-UX, LINUX, SunOS, Get locale information: locale -a   grep -E &lt;en_US.* ^C POSIX&gt; -a   /usr/xpg4/bin/grep -E &lt;en_US.* ^C POSIX&gt;</p> <p>HP-UX, LINUX, SunOS, Get process information: ps -ef -eo user,pid,lstart,command --cols 2530 --no-headers</p> <p>SunOS, Get process information: /usr/ucb/ps -agxwww</p> <p>Window, Get language info: wmic OS Get CodeSet OS Get OSLanguage</p> <p>SunOS, Get current zone name: zonename</p> <p>Window, Get process info: wmic path Win32_Process get ParentProcessId, commandLine, creationdate, executablepath, name, processId /value</p>
------	--	---

## **Network Connections - Passive Discovery**

### **Collect Network Data by NetFlow**

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

Permissions information is unavailable or no permissions are required.

### **Network Connectivity Data Analyzer**

The job discover client server connections on the network according to the chosen parameters. Brings data from DFM database.

Permissions information is unavailable or no permissions are required.

# Operational Discovery

## Operational Host Discovery by Shell

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

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Environment variables query and setup, data parsing and processing	Windows: set PATH=%PATH%;%WINDIR%\system32\wbem\ComSpec  AIX,FreeBSD,HP-UX,Linux,SunOS,VIO Server: echo \$SHELL  AIX,FreeBSD,HP-UX,Linux,SunOS,VIO Server: echo \$?  AIX,FreeBSD,HP-UX,Linux,SunOS,VIO Server: grep .*  AIX: egrep .*  AIX: ioscli  AIX,FreeBSD,HP-UX,Linux,SunOS: awk .*  AIX,FreeBSD,HP-UX,Linux,SunOS: cat ~/.discagnt/aioptionrc  AIX,FreeBSD,HP-UX,Linux,SunOS: export .*
exec	Discover Basic Host Info	AIX,HP-UX,Linux,SunOS: domainname  SunOS: zonename  Linux: dnsdomainname  AIX,HP-UX,Linux,SunOS: hostname  Windows: wmic path Win32_ComputerSystem get DNSHostName path Win32_OperatingSystem get PAEEEnabled  SunOS: cat /etc/nodename  AIX: namerslv -s -n  Linux: rpm -qa  NXOS: sh ver   no-more  NXOS: sh hostname   no-more
exec	Discover Node Model	HP-UX: model  Linux: dmidecode -t system  Linux: lshal  AIX: uname -M



exec	Discover OS version info	<p>AIX: oslevel -r</p> <p>AIX: ioslevel</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: uname</p> <p>HP-UX,Linux: uname -r</p> <p>SunOS: cat /etc/release</p> <p>Linux: cat /etc/redhat-release /etc/oracle-release /etc/SuSE-release</p> <p>HP-UX: swlist</p> <p>Windows: ver</p> <p>Windows: wmic path Win32_OperatingSystem get BuildNumber, Caption, Version, csdversion, lastBootUpTime, organization, otherTypeDescription, registeredUser, totalVisibleMemorySize</p> <p>NXOS: sh ver   no-more</p>
exec	Discover Host boot time info	<p>AIX,HP-UX,Linux,SunOS: uptime &amp;&amp; date -u '+%Y-%m-%d %H:%M:%S'</p> <p>UNIX: date '+%Y-%m-%d'</p> <p>Windows: wmic path Win32_OperatingSystem get BuildNumber, Caption, Version, csdversion, lastBootUpTime, organization, otherTypeDescription, registeredUser, totalVisibleMemorySize</p> <p>Windows: reg query "HKEY_CURRENT_USER\Control Panel\International" /v sShortDate</p> <p>UNIX: uptime</p> <p>Windows: net stats srv</p> <p>NXOS: sh ver   no-more</p>
exec	Discover host description	<p>Windows: reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" /v "srvcomment"</p>
exec	Discover DNS, DHCP and WINS Information	<p>Windows: wmic path Win32_NetworkAdapterConfiguration where "domainDnsRegistrationEnabled &lt;&gt; NULL" get dnsServerSearchOrder /value</p> <p>Windows: wmic path Win32_NetworkAdapterConfiguration where "WinsPrimaryServer &lt;&gt; NULL or WinsSecondaryServer &lt;&gt; NULL" get WinsPrimaryServer, WinsSecondaryServer /value</p> <p>Windows: wmic path Win32_NetworkAdapterConfiguration where "dhcpServer &lt;&gt; NULL" get dhcpServer /value</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS: cat /etc/resolv.conf</p> <p>SunOS,Linux: cat /etc/nsswitch.conf</p> <p>NXOS: sh hosts   no-more</p>

exec	Discover network interfaces and IPs info	AIX: ps -aef HP-UX: ioscan -FnkClan HP-UX: lanadmin -s SunOS,Linux: cat /etc/hosts HP-UX: netstat -in HP-UX: cat /etc/rc.config.d/netconf HP-UX: lanscan Windows: ipconfig /all Windows: wmic path Win32_NetworkAdapterConfiguration get Caption, Description, DhcpEnabled, IPAddress, IPSubnet, Index, MACAddress /value Windows: wmic path Win32_NetworkAdapter get DeviceID, Name /value SunOS: ifconfig -a HP-UX: ifconfig . * AIX: ifconfig -a inet AIX: entstat * AIX: lsdev -Cc adapter -S VIO Server: lsdev -type adapter -fmt VIO Server: lsmap -all -net VIO Server: lstcpip -interfaces AIX: lsdev -Cc adapter -F 'name:description' AIX: lscfg Linux: ip addr show Linux: ps aux SunOS: netstat -np SunOS: dladm show-dev show-aggr -p show-link -p show-linkprop -p zone NXOS: sh int   no-more
exec	Discover Virtualization Info	AIX: prtconf AIX LPARS: lparstat -i SunOS: /usr/bin/zonename Solaris Zones: ps -o zone IBM HMC: lshmc -V -n

exec	Discover Host Serial Number info	<p>Windows: reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion" /v "CurrentVersion"</p> <p>Windows: wmic path Win32_BIOS get serialNumber</p> <p>Windows: wmic path Win32_SystemEnclosure get serialNumber</p> <p>AIX: lsattr -El sys0 -a systemid</p> <p>VIO Server: lsdev -dev sys0 -attr systemid</p> <p>SunOS: sneep</p> <p>SunOS: eeprom nvramrc</p> <p>SunOS: hostid</p> <p>Linux,SunOS: dmidecode -t system</p> <p>Linux: lshal</p> <p>HP-UX: cstm</p> <p>HP-UX: getconf MACHINE_SERIAL</p>
exec	Discover Host Manufacture Info	<p>AIX: lsvpd</p> <p>Linux: dmidecode -t system</p> <p>Linux: lshal</p> <p>Windows: wmic path Win32_ComputerSystem get Domain, Manufacturer, Model, Name, NumberOfProcessors /value</p> <p>Windows: wmic path Win32_ComputerSystem get PartOfDomain /value</p> <p>SunOS: showrev</p> <p>SunOS: smbios -t SMB_TYPE_SYSTEM</p>
exec	Discover Host HW Architecture Info	SunOS: prtdiag
exec	Discover system locale and code page info	<p>Windows: chcp</p> <p>Windows: wmic OS Get CodeSet</p> <p>Windows: wmic OS Get OSLanguage</p> <p>AIX,FreeBSD,HP-UX,Linux,SunOS,VIO Server: locale -a</p>
exec	Discover Node Asset Tag	Windows: wmic path Win32_SystemEnclosure get smBiosAssetTag /value
exec	Discover Node Bios UUID	<p>Linux,SunOS: dmidecode -t system</p> <p>Linux: lshal</p> <p>Windows: wmic path win32_ComputerSystemProduct get name, uuid</p>
exec	Discover OS Name	<p>Windows: reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion" /v "ProductName"</p>

exec	Discover build number	Windows: reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion" /v "CurrentBuildNumber"
exec	Discover version and service pack information	Windows: reg query "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion" /v "CSDVersion"
exec	Discover host default gateway	Windows: wmic path Win32_IP4RouteTable where "destination = '0.0.0.0' and mask = '0.0.0.0'" get metric1, Hop /value  AIX,FreeBSD,HP-UX,Linux,SunOS,Windows: netstat -r -n
exec	General information about HPE NonStop system	NonStop: gtacl -p scf sysinfo
exec	Information about HPE NonStop system IPs	NonStop: gtacl -p scf info subnet'\$*.*'
exec	Information about HPE NonStop system network interfaces	NonStop: gtacl -p scf info lif '\$zzlan.*'

## Oracle VM for x86

### Oracle VM for x86 by Manager Main CLI

The job make discovery of virtualization inventory using manager's main CLI accessible by SSH protocol.

Protocol: ovmcli

Operation	Usage description	Objects and parameters
exec	Switch to XML output format	set OutputMode=Xml
exec	List Virtual Machines	list Vm
exec	List Servers	list Server
exec	Show Server details	show Server
exec	Show Virtual Machine details	show Vm
exec	Show Oracle Vm Manager version	showversion

# Proxy Servers - Reverse Proxy - IBM

## Webseal Connection by Web Services

The job discovers the Webseal topology by pdadmin rest api.

Permissions information is unavailable or no permissions are required.

## Webseal Connection by Shell

The job discovers credentials applied and generic topology for Webseal by shell.

Protocol: Execute

Operation	Usage description	Objects and parameters
execute	Run the utility to fetch all the webseal data	pdadmin

## Webseal Policy Server Connection by Shell

The job this adapter is used to find valid pdadmin credentials and store the reference to the ISAMPolicy Server CI.&#10;

Protocol: Execute

Operation	Usage description	Objects and parameters
execute	Run the utility to fetch all the webseal data	pdadmin

## Webseal Policy Server Topology by Shell

The job adapter provides the capability to discover all WebSeal related topology triggering on PolicyServer.

Protocol: Execute

Operation	Usage description	Objects and parameters
execute	Run the utility to fetch all the webseal data	pdadmin

## Webseal Topology by Web Services

The job discovers the Webseal topology by pdadmin rest api.

Permissions information is unavailable or no permissions are required.

## Webseal Topology by Shell

The job this is the adapter for reporting topology of Webseal and junctions using shell protocols.

Protocol: Execute

Operation	Usage description	Objects and parameters
execute	Run the utility to fetch all the webseal data	pdadmin

# Red Hat Cluster Suite

## Red Hat Cluster by Shell

The job discovers Red Hat Cluster information.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Cluster configuration, file system configuration	Linux: clustat .* AIX,FreeBSD,HP-UX,Linux,SunOS: cat .* AIX,FreeBSD,HP-UX,Linux,SunOS: grep .* Linux: gfs2_edit .* Linux: blkid .*
exec	Basic login	AIX,FreeBSD,HP-UX,Linux,SunOS: uname -a AIX: uname -M AIX,FreeBSD,HP-UX,Linux,SunOS: uname Unix: /usr/ios/cli/ioscli uname -L ver AIX,FreeBSD,HP-UX,Linux,SunOS: locale -a
exec	Environment variables query and setup, data parsing and processing	Windows: set PATH=%PATH%;%WINDIR%\system32\wbem\ AIX,FreeBSD,HP-UX,Linux,SunOS: echo \$SHELL AIX,FreeBSD,HP-UX,Linux,SunOS: echo \$? AIX,FreeBSD,HP-UX,Linux,SunOS: grep .* AIX: egrep .* AIX: ioscli .* AIX,FreeBSD,HP-UX,Linux,SunOS: awk .* AIX,FreeBSD,HP-UX,Linux,SunOS: nice .* AIX,FreeBSD,HP-UX,Linux,SunOS: export .*
exec	Can execute nslookup for resolving host	nslookup <hostname>



# SMI-S

## Storage Devices Connection by CIM

The job this adapter is used for initial connection to CIM Agent.

Protocol: CIM

Operation	Usage description	Objects and parameters
get	get always existing class to check connectivity	CIM_OrganizationalEntity  TPD_StorageSystem  HPEVA_StorageSystem  LSISSI_StorageSystem  EMC_ComputerSystem

## Storage Devices Topology by CIM

The job adapter used for discovery of storage topology via CIM protocol.

Protocol: CIM

Operation	Usage description	Objects and parameters
Get	Storage Pool information	HPEVA_StoragePool  CIM_StoragePool  TPD_StoragePool  LSISSI_StoragePool  EMC_StoragePool
Get	Storage basic information.	TPD_StorageSystem  CIM_StorageSystem  HPEVA_StorageSystem  LSISSI_StorageSystem  EMC_StorageSystem
Get	Fibre Chanel Port information	TPD_FCPort  HPEVA_DiskFCPort  CIM_FCPort  LSISSI_FCPort  EMC_FCPort

Get	Storage/Logical Volume Information	HPEVA_StorageVolume TPD_StorageVolume CIM_StorageVolume LSISSI_StorageVolume EMC_StorageVolume
Get	Connected nodes information	HPEVA_ProtocolControllerForVolume CIM_Node TPD_NodeSystem HPEVA_ViewProtocolController LSISSI_ControllerCanister LSISSI_ControllerFirmwareIdentity EMC_StorageSystemSoftwareIdentity EMC_ArrayChassis EMC_SCSIProtocolController
Get	Storage Processor System information	HPEVA_StorageProcessorSystem LSISSI_StorageProcessorSystem EMC_StorageProcessorSystem
Get	Physical Volume / Disk information	HPEVA_DiskExtent LSISSI_DiskExtent EMC_DiskExtent

## SSL Certificates

### SSL Certificate Discovery by HTTPS

The job adapter Description.

Permissions information is unavailable or no permissions are required.

## **Security - Oracle Access Management**

### **Oracle Access Management Connection by Web Services**

The job using HTTP credential to connect Oracle Access Management.

Permissions information is unavailable or no permissions are required.

### **Oracle Access Management Policies by Web Services**

The job get Oracle Access Management policies.

Permissions information is unavailable or no permissions are required.

### **Oracle Access Management Dependencies via URL**

The job searching for real product URL from OAM and its Consumer Provider dependency mapping with WebGate URL.

Permissions information is unavailable or no permissions are required.

## Storage - SNMP

### Storage Devices Topology by SNMP

The job adapter used for discovery of storage topology via SNMP protocol.

Protocol: SNMP

Operation	Usage description	Objects and parameters
get	Dell EMC Data Domain	Dell EMC dataDomainMib: 1.3.6.1.4.1.19746
get	Dell EMC Isilon	Dell EMC IsilonMib: 1.3.6.1.4.1.12124

# TIBCO

## TIBCO BusinessWorks by Shell

The job discover TIBCO BusinessWorks and its resources.

Protocol: Shell, TIBCO

Operation	Usage description	Objects and parameters
exec	Execute AppManage utility	AppManage -batchExport -dir {output directory} -domain {domain} -user {username} -pw {password} -noear

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Get processes information (Linux)	echo . ps aux
exec	Get processes information (HPUX)	ps -ef
exec	Get processes information (FreeBSD)	ps -ax
exec	Get processes information (*nix)	ps -e
exec	Removing temporary UCMDB directory created during discovery	rm -rf {temporary UCMDB directory}
exec	Get file contents using cat command	cat {XML file in temporary directory}
exec	Make temporary directory for UCMDB	mkdir -p {temporary directory path}
exec	Change directory	cd {AppManage utility directory}
exec	Get present working directory	pwd
exec	Basic login	Windows: cmd.exe /c ver UNIX: ioscli uname -a UNIX: uname UNIX: locale -a UNIX: PATH=\${PATH}"/bin:/usr/bin" && export PATH
exec	Check file existence	UNIX: perl perl -e 'if(!-f \$ARGV[0] and !-d \$ARGV[0] and !-l \$ARGV[0]){exit(1)}' "<filename>"

## TIBCO EMS by Shell

The job discover TIBCO EMS and its resources.

Protocol: Shell, TIBCO

Operation	Usage description	Objects and parameters
exec	Permission to run tibemsadmin utility	tibemsadmin -server {server:port} - user {username} -password {password} -script {tibco command file}

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Permission to run cat command against TIBCO EMS config file	cat {TIBCO EMS config file}
exec	Permission to write file in temp directory	echo tibco show commands > {temp directory}

# Troux

## Import CIs from Troux

The job populates CIs from Troux using the Troux TUX File.

Permissions information is unavailable or no permissions are required.



# UD Agent Management

## Install UD Agent

The job this adapter installs UD Agent.

Protocol: NTCMD

Operation	Usage description	Objects and parameters
UD Agent installation	Install UD Agent as part of UD Agent Lifecycle Managent	Windows: full administrative permissions

Protocol: SSH

Operation	Usage description	Objects and parameters
UD Agent installation	Install UD Agent as part of UD Agent Lifecycle Managent	Windows: full administrative permissions UNIX: root permissions Linux: root permissions

## UDA Status Collector

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

Permissions information is unavailable or no permissions are required.

## Uninstall UD Agent

The job this adapter uninstalls UD Agent.

Protocol: NTCMD

Operation	Usage description	Objects and parameters
UD Agent uninstall	Uninstall UD Agent as part of UD Agent Lifecycle Managent	Windows: full administrative permissions

Protocol: SSH

Operation	Usage description	Objects and parameters
UD Agent installation	Uninstall UD Agent as part of UD Agent Lifecycle Managent	Windows: full administrative permissions UNIX: root permissions Linux: root permissions

## Update UD Agent

The job this adapter updates UD Agent.

Protocol: NTCMD

Operation	Usage description	Objects and parameters
UD Agent update	Update/upgrade UD Agent as part of UD Agent Lifecycle Managent	Windows: full administrative permissions

Protocol: SSH

Operation	Usage description	Objects and parameters
UD Agent update	Update/upgrade UD Agent as part of UD Agent Lifecycle Managent	Windows: full administrative permissions UNIX: root permissions Linux: root permissions

## **Virtualization - Citrix**

### **Citrix Xen Connection**

The job this adapter is used to detect XenServer by connecting to trigger IP.

Permissions information is unavailable or no permissions are required.

### **Citrix Xen Topology**

The job this adapter is used to fetch topology of XenServer.

Permissions information is unavailable or no permissions are required.

# Virtualization - HP IVM

## HPE IVM by Shell

The job this adapter discovers HPE Integrity Virtual Machine topology by connecting to the physical or virtual server.

Protocol: shell

Operation	Usage description	Objects and parameters
exec	Get detailed information about the virtual servers	hpvmstatus -V -d -P <vm_name>
exec	Get information about the IVM version	hpvminfo -v

# Virtualization - HP nPartitions

## HPE nPars and vPars by Shell

The job this adapter discovers HPE partitionable server (either cell-based or not) topology by connecting to the vPar or nPar.

Protocol: shell

Operation	Usage description	Objects and parameters
exec	Getting information about the Complex	parstatus -X
exec	List general information about all cells	parstatus -M -C
exec	Get detailed information about the cell	<cell_id>: parstatus -V -c
exec	Get information about the I/O chassis	parstatus -M -I
exec	Get list of configured nPartitions	parstatus -M -P
exec	Get detailed information about nPartition	<npar_number>: parstatus -V -p
exec	Get the name of the current vPartition	vparstatus -M -w
exec	Get detailed information about the current vPartition	<vpar_name>: vparstatus -v -p
exec	Get the list of the names of the volume groups	vgdisplay   grep "VG Name"
exec	Get detailed information about the volume group	<volume_group_name>: vgdisplay -v
exec	Get information about the file systems	df -P
exec	Get information about the Fibre Channel devices	ioscan -FncCfc
exec	Get information about the network cards	ioscan -FncClan
exec	Get information about the SCSI adapters	ioscan -FncCdisk
exec	List network interfaces	lanscan
exec	Get information about aggregated interfaces	lanscan -q
exec	Get MAC address of the interface	lanadmin -a
exec	Get hardware path of the aggregated interfaces	lanscan -v

# Virtualization - Hyper-V

## Hyper-V Topology by Shell

The job adapter discovers Microsoft Hyper-V virtualization topology using shell protocol.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Get host system language and code page	wmic OS Get CodeSet OS Get OSLanguage
exec	Get process list	wmic path Win32_Process get ParentProcessId, commandLine, creationdate, executablepath, name, processId

Protocol: wmic:\\root\\virtualization

Operation	Usage description	Objects and parameters
exec	Get the name of the Hyper-V host	Msvm_ComputerSystem: ElementName
exec	Get virtual machines	Msvm_ComputerSystem: Name, ElementName, EnabledState, HealthState
exec	Get global settings for virtual machines	Msvm_VirtualSystemGlobalSettingData: SystemName, InstanceID, SnapshotDataRoot, ExternalDataRoot, AutomaticRecoveryAction, AutomaticShutdownAction, AutomaticStartupAction
exec	Get settings for virtual machines (VSSD)	Msvm_VirtualSystemSettingData: InstanceID, BaseBoardSerialNumber, BIOSGUID, BIOSSerialNumber, ChassisAssetTag, ChassisSerialNumber
exec	Get synthetic ethernet adapter info	Msvm_SyntheticEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
exec	Get emulated ethernet adapter info	Msvm_EmulatedEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
exec	Get internal ethernet adapter information	Msvm_InternalEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
exec	Get external ethernet adapter information	Msvm_ExternalEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
exec	Get logical connection point of network adapter	Msvm_VmLANEndpoint: ElementName, Name, SystemName
exec	Get logical connection endpoint for a network adapter	Msvm_SwitchLANEndpoint: ElementName, Name, SystemName
exec	Get association between service access point and how its implemented	Msvm_DeviceSAPImplementation: Antecedent, Dependent
exec	Get association between endpoint and global ethernet port	Msvm_GlobalEthernetPortSAPImplementation: Antecedent, Dependent

exec	Get references from Virtual Machines to settings (VSSD)	Msvm_SettingsDefineState: ManagedElement, SettingData
exec	Get references from Virtual Machine settings (VSSD) to components	Msvm_VirtualSystemSettingDataComponent: GroupComponent, PartComponent
exec	Get memory settings	Msvm_MemorySettingData: InstanceID, Limit, Reservation
exec	Get processor settings	Msvm_ProcessorSettingData: InstanceID, Limit, Reservation, Weight
exec	Get virtual switches	Msvm_VirtualSwitch: ElementName, Name
exec	Get ports of virtual switches	Msvm_SwitchPort: ElementName, Name
exec	Get references from virtual switches to ports	Msvm_HostedAccessPoint: Antecedent, Dependent
exec	Get interfaces of virtual machines	Msvm_VmLANEndpoint: Name, ElementName, MACAddress
exec	Get interfaces of Hyper-V host	Msvm_SwitchLANEndpoint: Name, ElementName, MACAddress
exec	Get references from port on virtual switches to interfaces	Msvm_ActiveConnection: Antecedent, Dependent

Protocol: WMI:\\root\\virtualization\\v2

Operation	Usage description	Objects and parameters
query	Get the name of the Hyper-V host	Msvm_ComputerSystem: ElementName
query	Get virtual machines	Msvm_ComputerSystem: Name, ElementName, EnabledState, HealthState
query	Get global settings for virtual machines	Msvm_VirtualSystemSettingData: InstanceID, SnapshotDataRoot, ExternalDataRoot, AutomaticRecoveryAction, AutomaticShutdownAction, AutomaticStartupAction
query	Get settings for virtual machines (VSSD)	Msvm_VirtualSystemSettingData: InstanceID, BaseBoardSerialNumber, BIOSGUID, BIOSSerialNumber, ChassisAssetTag, ChassisSerialNumber
query	Get references from Virtual Machines to settings (VSSD)	Msvm_SettingsDefineState: ManagedElement, SettingData
query	Get references from Virtual Machine settings (VSSD) to components	Msvm_VirtualSystemSettingDataComponent: GroupComponent, PartComponent
query	Get memory settings	Msvm_MemorySettingData: InstanceID, Limit, Reservation
query	Get processor settings	Msvm_ProcessorSettingData: InstanceID, Limit, Reservation, Weight
query	Get virtual switches	Msvm_VirtualEthernetSwitch: ElementName, Name

query	Get ports of virtual switches	Msvm_EthernetSwitchPort: ElementName, Name
query	Get interfaces of virtual machines	Msvm_LANEndpoint: Name, ElementName, MACAddress
query	Get interfaces of Hyper-V host	Msvm_LANEndpoint: Name, ElementName, MACAddress
query	Get references from port on virtual switches to interfaces	Msvm_ActiveConnection: Antecedent, Dependent
query	Get a synthetic Ethernet adapter	Msvm_SyntheticEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
query	Get an emulated Ethernet adapter.	Msvm_EmulatedEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
query	Get an internal Ethernet port (network adapter)	Msvm_InternalEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
query	Get an external Ethernet port (network adapter).	Msvm_ExternalEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
query	Get references from service access point (SAP) to it's implementation	Msvm_DeviceSAPIImplementation: Antecedent, Dependent
query	Get references from LAN endpoint to a global Ethernet port	Msvm_EthernetDeviceSAPIImplementation: Antecedent, Dependent

## Hyper-V Topology by WMI

The job adapter discovers Microsoft Hyper-V virtualization topology using WMI protocol.

Protocol: WMI:\\root\\cimv2

Operation	Usage description	Objects and parameters
query	Get OS language	Win32_OperatingSystem: CodeSet, OSLanguage

Protocol: WMI:\\root\\virtualization

Operation	Usage description	Objects and parameters
query	Get the name of the Hyper-V host	Msvm_ComputerSystem: ElementName
query	Get virtual machines	Msvm_ComputerSystem: Name, ElementName, EnabledState, HealthState
query	Get global settings for virtual machines	Msvm_VirtualSystemGlobalSettingData: InstanceID, SnapshotDataRoot, ExternalDataRoot, AutomaticRecoveryAction, AutomaticShutdownAction, AutomaticStartupAction



query	Get settings for virtual machines (VSSD)	Msvm_VirtualSystemSettingData: InstanceID, BaseBoardSerialNumber, BIOSGUID, BIOSSerialNumber, ChassisAssetTag, ChassisSerialNumber
query	Get references from Virtual Machines to settings (VSSD)	Msvm_SettingsDefineState: ManagedElement, SettingData
query	Get references from Virtual Machine settings (VSSD) to components	Msvm_VirtualSystemSettingDataComponent: GroupComponent, PartComponent
query	Get memory settings	Msvm_MemorySettingData: InstanceID, Limit, Reservation
query	Get processor settings	Msvm_ProcessorSettingData: InstanceID, Limit, Reservation, Weight
query	Get virtual switches	Msvm_VirtualSwitch: ElementName, Name
query	Get ports of virtual switches	Msvm_SwitchPort: ElementName, Name
query	Get references from virtual switches to ports	Msvm_HostedAccessPoint: Antecedent, Dependent
query	Get interfaces of virtual machines	Msvm_VmLANEndpoint: Name, ElementName, MACAddress
query	Get interfaces of Hyper-V host	Msvm_SwitchLANEndpoint: Name, ElementName, MACAddress
query	Get references from port on virtual switches to interfaces	Msvm_ActiveConnection: Antecedent, Dependent
query	Get a synthetic Ethernet adapter	Msvm_SyntheticEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
query	Get an emulated Ethernet adapter.	Msvm_EmulatedEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
query	Get an internal Ethernet port (network adapter)	Msvm_InternalEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
query	Get an external Ethernet port (network adapter).	Msvm_ExternalEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
query	Get references from service access point (SAP) to it's implementation	Msvm_DeviceSAPIImplementation: Antecedent, Dependent
query	Get references from LAN endpoint to a global Ethernet port	Msvm_GlobalEthernetPortSAPIImplementation: Antecedent, Dependent

Protocol: WMI:\\root\\virtualization\\v2

Operation	Usage description	Objects and parameters
query	Get the name of the Hyper-V host	Msvm_ComputerSystem: ElementName
query	Get virtual machines	Msvm_ComputerSystem: Name, ElementName, EnabledState, HealthState

query	Get global settings for virtual machines	Msvm_VirtualSystemSettingData: InstanceID, SnapshotDataRoot, ExternalDataRoot, AutomaticRecoveryAction, AutomaticShutdownAction, AutomaticStartupAction
query	Get settings for virtual machines (VSSD)	Msvm_VirtualSystemSettingData: InstanceID, BaseBoardSerialNumber, BIOSGUID, BIOSSerialNumber, ChassisAssetTag, ChassisSerialNumber
query	Get references from Virtual Machines to settings (VSSD)	Msvm_SettingsDefineState: ManagedElement, SettingData
query	Get references from Virtual Machine settings (VSSD) to components	Msvm_VirtualSystemSettingDataComponent: GroupComponent, PartComponent
query	Get memory settings	Msvm_MemorySettingData: InstanceID, Limit, Reservation
query	Get processor settings	Msvm_ProcessorSettingData: InstanceID, Limit, Reservation, Weight
query	Get virtual switches	Msvm_VirtualEthernetSwitch: ElementName, Name
query	Get ports of virtual switches	Msvm_EthernetSwitchPort: ElementName, Name
query	Get interfaces of virtual machines	Msvm_LANEndpoint: Name, ElementName, MACAddress
query	Get interfaces of Hyper-V host	Msvm_LANEndpoint: Name, ElementName, MACAddress
query	Get references from port on virtual switches to interfaces	Msvm_ActiveConnection: Antecedent, Dependent
query	Get a synthetic Ethernet adapter	Msvm_SyntheticEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
query	Get an emulated Ethernet adapter.	Msvm_EmulatedEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
query	Get an internal Ethernet port (network adapter)	Msvm_InternalEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
query	Get an external Ethernet port (network adapter).	Msvm_ExternalEthernetPort: DeviceID, ElementName, PermanentAddress, SystemName
query	Get references from service access point (SAP) to it's implementation	Msvm_DeviceSAPIImplementation: Antecedent, Dependent
query	Get references from LAN endpoint to a global Ethernet port	Msvm_EthernetDeviceSAPIImplementation: Antecedent, Dependent

## SCVMM Topology by Shell

The job sCVMM Topology Discovery.

Protocol: PowerShell

Operation	Usage description	Objects and parameters
SCVMM Administrator	Get SCVMM resources	Get-SCVMHost Get-SCVirtualNetwork Get-VM Get-SCVirtualNetworkAdapter

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Windows version	ver
exec	Execute command	cmd /c "<command>" powershell

# Virtualization - IBM

## IBM Virtualization by Shell

The job discovers topology of IBM Hardware Management Console and IVM.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	OS info and version	Get Windows OS family version: ver  Get Unix-like OS version: uname  Get AIX version: ioscli uname -a
exec	Get locale information	locale -a   grep -E "en_US.* ^C POSIX"
exec	Get environment variable value	echo \${variable}
exec	Get HMC version	lshmc -v -V -n
exec	Get HMC BIOS information	lshmc -b
exec	Get configuration information on all pSeries Frames managed by this instance of HMC	lssyscfg -r sys -r sys --all -z
exec	Get devices mapping	ioscli lsmapi -all
exec	Get processor information on the pSeries Frame specified as 'pSeriesName'	lshwres -r cpu -m 'pSeriesName' -F id:status:partition:assigned_to -r proc --level sys -m 'pSeriesName'
exec	Get memory information on the pSeries Frame specified as 'pSeriesName'	lshwres -r mem --level sys -m 'pSeriesName' -r mem -m 'pSeriesName' -F allocated:page_table:partition:assigned_to:lmb_size
exec	Get I/O slot information on the pSeries Frame specified as 'pSeriesName'	lshwres -r io --subtype slot -m 'pSeriesName'
exec	Get processor pool information on the pSeries Frame specified as 'pSeriesName'	lshwres -r proc --level pool -m 'pSeriesName'
exec	Get configuration information on the LPAR specified as 'lparName'	lssyscfg -r lpar -m 'lparName'
exec	Get profile information on the LPAR specified as 'lparName'	lssyscfg -r lpar --all -m 'pSeriesName' -z -r prof --all -m 'pSeriesName' -p 'lparName' -z -r prof -m 'lparName'
exec	Get memory information on the LPAR specified as 'lparName'	lshwres -r mem --level lpar -m 'lparName'
exec	Get processor information on the LPAR specified as 'lparName'	lshwres -r proc --level lpar -m 'lparName'

exec	Get network interface information on the LPAR specified as 'lparName'	lshwres -r virtualio --rsubtype eth --level lpar -m 'lparName'
exec	Get SCSI information on the LPAR specified as 'lparName'	lshwres -r virtualio --rsubtype scsi -m 'lparName'
exec	Get partition information on the pSeries Frame specified as 'pSeriesName'	lshwres -r virtualio --rsubtype slot --level slot -m 'pSeriesName'
exec	Get LPar assigned IP address.	lspartition -c 'Model_' 'Serial Number' -i -c 'Model_' 'Serial Number' -ix
exec	Get IVM related information	lsivm
exec	Get host name	hostname
exec	Get host ips	lstcpip -interfaces

## IBM LPAR and VIO Server Topology by Shell

The job adapter for Discovery of IBM VIO Server or any IBM LPar running system.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	General commands execution	echo \$  ioscli uname lsdev -dev <devName> -vpd  locale -a  grep *  lsattr -El
exec	get the relations between VSCSI adapter and backing devices	ioscli: lsmap -all
exec	get relations between virtual Ethernet, SEA and Link Aggregation interfaces	ioscli: lsmap -all -net
exec	get interface MAC addresses	ioscli: entstat -all
exec	get Media Speed and backing adapters	ioscli: lsdev -dev <devName> -attr -Cc adapter -F"name:physloc"
exec	get Fiber Channel Adapters	ioscli: lsdev -dev fcs* -field name physloc description -fmt :
exec	get Physical Volumes	lspv
exec	get logical voumes	lslv -l <logical volume>
exec	get Volume Groups	lsvg <volumeGroup>
exec	get relation between SCSI and Volumes	lspath

exec	updates internal system information, prerequisite for lsvio	vpdupdate
exec	lists virtual SCSI Adapters	lsvio -s
exec	get detailed interface information	lscfg -vpl <deviceName>
exec	lists Volume Groups	vgdisplay
exec	get detailed Logical Volume information	lvdisplay <lvName>
exec	get information about physical CPUs available	lsdev   grep proc prtconf   grep "proc"
exec	get detailed information about CPU by index	lsdev -dev proc<index> -attr lsattr -El <procName> -attr
exec	get number of cores per CPU	lsdev -dev sysplanar0 -vpd   grep PROC lscfg -vpl sysplanar0   grep PROC

## IBM PureFlex Topology by Shell

The job allows to discover IBM FSM managed resources and topology.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Enumerate supported managed entities	smcli: lssys -I

## IBM WPAR Topology by Shell

The job discovers topology of IBM WPAR.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	General commands execution	echo \$ ioscli uname lsdev -dev <devName> -vpd locale -a grep * lsattr -El
exec	get the relations between VSCSI adapter and backing devices	ioscli: lsmapi -all

exec	get relations between virtual Ethernet, SEA and Link Aggregation interfaces	ioscli: lsmapi -all -net
exec	get interface MAC addresses	ioscli: entstat -all
exec	get Media Speed and backing adapters	ioscli: lsdev -dev <devName> -attr -Cc adapter -F"name:physloc"
exec	get Fiber Channel Adapters	ioscli: lsdev -dev fcs* -field name physloc description -fmt :
exec	get Physical Volumes	lspv
exec	get logical volumes	lslv -l <logical volume>
exec	get Volume Groups	lsvg <volumeGroup>
exec	get relation between SCSI and Volumes	lspath
exec	updates internal system information, prerequisite for lsvio	vpdupdate
exec	lists virtual SCSI Adapters	lsvio -s
exec	get detailed interface information	lscfg -vpl <deviceName>
exec	lists Volume Groups	vgdisplay
exec	get detailed Logical Volume information	lvdisplay <lvName>
exec	get information about physical CPUs available	lsdev   grep proc prtconf   grep "proc"
exec	get detailed information about CPU by index	lsdev -dev proc<index> -attr lsattr -El <procName> -attr
exec	get number of cores per CPU	lsdev -dev sysplanar0 -vpd   grep PROC lscfg -vpl sysplanar0   grep PROC
exec	get information of WPARs	lswpar -G -d UCMDDB lswpar -N -d UCMDDB lswpar -R -d UCMDDB

# Virtualization - Oracle VM Server for SPARC Technology

## Oracle VM Server for SPARC Technology by Shell

The job adapter discovers LDOM topology via control domain.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Get version of LDM	ldm -V
exec	Get information about LDOMs configuration	ldm list-bindings -p
exec	Get hostname of control domain	cat /etc/nodename uname -n hostname
exec	Get networking information of control domain	/usr/sbin/ifconfig -a /usr/bin/netstat -np /usr/sbin/dladm show-aggr -p show-aggr -x -p -o link,port,address show-dev show-link -p show-linkprop -p zone /usr/sbin/prtpicl -c other   grep CORE   grep -v DVRM_CORE   grep -v NIU_CORE
exec	Get virtual interfaces created by virtual switches	find /devices/virtual-devices@100 -type c -name virtual-network-switch*
exec	Get additional details about target host	uname -a uname
exec	Get details about shell	echo \$SHELL echo \$?
exec	Get details about locale	locale -a
exec	Get virtual CPU count of LDOM	ldm list-devices -a -p cpu
exec	Get memory size of LDOM	ldm list-devices -a -p memory
exec	Get information of physical CPU	kstat -p cpu_info



# Virtualization - Red Hat

## Red Hat Virtualization Discovery by REST API

The job red Hat Enterprise Virtualization Discovery by REST API.

Protocol: HTTP

Operation	Usage description	Objects and parameters
GET	It retrieves a representation of the main entry point for version 3 of the API.	api
GET	It retrieves a representation of the data center collection.	api/datacenters
GET	It retrieves a representation of the host clusters collection.	api/clusters
GET	It retrieves a representation of the logical networks collection.	api/networks
GET	It retrieves a representation of the hosts collection.	api/hosts
GET	It retrieves a representation of the interfaces of hosts.	api/hosts/.../nics
GET	It retrieves a representation of the virtual machine tools collection.	api/vmpools
GET	It retrieves a representation of the vnic profiles collection.	api/vnicprofiles
GET	It retrieves a representation of the virtual machines collection.	api/vms
GET	It retrieves a representation of the the interfaces of virtual machines.	api/vms/.../nics
GET	It retrieves a representation of the storage domains collection.	api/storagedomains
GET	It retrieves a representation of the disks collection.	api/disks

# Virtualization - Solaris Zones

## Solaris Zones by TTY

The job this adapter discovers Solaris Zones by shell protocols (SSH, Telnet or UDA) including non-global zones, resource pools, networking CPU and their dependencies.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic login	uname ver
exec	Get Solaris version	uname -r
exec	Find all predefined zones	zoneadm list -cp
exec	Get zones resources	zonecfg -z {ZONE_NAME} info
exec	Zone login to run commands in non-global zones	zlogin -l {USERNAME} {ZONE_NAME}
exec	Get Networking information	Interfaces: netstat -np IP information: ifconfig -a
exec	Get CPUs	psrinfo -v
exec	Get resource pools	pooladm
exec	Get Fiber Channel Adapters	fcinfo hba-port

# Virtualization - VMware

## Manual VMware VIM Connection

The job adapter 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 CIM

The job vMware ESX Connection by CIM adapter.

Protocol: CIM

Operation	Usage description	Objects and parameters
Get	Get registered profiles	root/interop: CIM_RegisteredProfile
Get Associators	Get UnitaryComputerSystem	root/cimv2: OMC_ElementConformsToBaseServerProfile
Get Associators	Get Chassis	root/cimv2: OMC_ComputerSystemPackage
Get	Get Interfaces	root/cimv2: VMware_EthernetPort
Get Associators	Get Hypervisor details	root/cimv2: VMware_InstalledSoftwareIdentity

## VMware ESX Connection by VIM

The job adapter 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 CIM

The job vMware ESX Topology by CIM.

Protocol: CIM

Operation	Usage description	Objects and parameters
Get Instance	Get UnitaryComputerSystem by UUID	root/cimv2: OMC_UnitaryComputerSystem
Get	Get Processors	root/cimv2: OMC_Processor
Get	Get Memory	root/cimv2: OMC_Memory
Get	Get ESX	vmware/esxv2: VMWARE_ESXComputerSystem
Get Associators	Get Virtual Machines	vmware/esxv2: VMWARE_HostedDependency

## VMware ESX Topology by VIM

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

Protocol: VMWare

Operation	Usage description	Objects and parameters
exec	Get licenses availability information (requires 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: configStatus ComputeResource: name ComputeResource: summary ComputeResource: resourcePool
exec	Get all ResourcePools along with their properties (requires System.Read permission)	ResourcePool: parent ResourcePool: config ResourcePool: vm ResourcePool: configStatus ResourcePool: resourcePool ResourcePool: name
exec	Get HostSystem of this ESX servers along with its properties (requires System.Read permission)	HostSystem: configStatus HostSystem: configManager.storageSystem HostSystem: config.network HostSystem: runtime.connectionState HostSystem: config.storageDevice HostSystem: config.product HostSystem: vm HostSystem: datastore HostSystem: summary HostSystem: name
exec	Get all VirtualMachines along with their properties (requires System.Read permission)	VirtualMachine: config VirtualMachine: configStatus VirtualMachine: datastore VirtualMachine: name VirtualMachine: runtime VirtualMachine: guest
exec	Get Datastores of this ESX servers along with its properties	Datastore: host Datastore: vm Datastore: info Datastore: summary

## VMware vMotion Monitor by VIM

The job adapter 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 vCenter Connection by VIM

The job adapter discovers connection to VMware vCenter server using Virtual Infrastructure Management protocol.

Protocol: VMWare

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

## VMware vCenter Topology by VIM

The job adapter collects Virtual Infrastructure topology information using vCenter Server by VI Management protocol.

Protocol: VMWare

Operation	Usage description	Objects and parameters
exec	Get all Datacenters along with their properties (requires System.Read permission)	Datacenter: configStatus  Datacenter: vmFolder  Datacenter: name  Datacenter: hostFolder

exec	Get licenses availability information (requires 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)	ClusterComputeResource (2.0): configuration ComputeResource: configStatus ComputeResource: name ComputeResource: summary ClusterComputeResource (2.5+): configurationEx ComputeResource: resourcePool
exec	Get all ResourcePools along with their properties (requires System.Read permission)	ResourcePool: parent ResourcePool: config ResourcePool: vm ResourcePool: configStatus ResourcePool: resourcePool ResourcePool: name

exec	Get all HostSystems (ESX servers) along with their properties (requires System.Read permission)	HostSystem: hardware.cpuPkg HostSystem: summary.runtime.connectionState HostSystem: hardware.systemInfo.otherIdentifyingInfo HostSystem: configManager.storageSystem HostSystem: config.virtualNicManagerInfo.netConfig HostSystem: config.network.dnsConfig HostSystem: config.network.pnic HostSystem: config.product HostSystem: config.network.vnic HostSystem: vm HostSystem: datastore HostSystem: summary.config.vmotionEnabled HostSystem: summary.runtime.inMaintenanceMode HostSystem: summary.runtime.bootTime HostSystem: config.network.vswitch HostSystem: summary.hardware HostSystem: config.network.proxySwitch HostSystem: config.storageDevice HostSystem: hardware.cpuInfo HostSystem: config.network.portgroup
exec	Get all VirtualMachines along with their properties (requires System.Read permission)	VirtualMachine: config VirtualMachine: configStatus VirtualMachine: datastore VirtualMachine: name VirtualMachine: runtime VirtualMachine: guest
exec	Get all Datastores along with properties	Datastore: host Datastore: vm Datastore: info Datastore: summary
exec	Get networks	Network: summary Network: host Network: vm



exec	Get all Distributed Virtual Switches with properties (4.0+)	DistributedVirtualSwitch: config.uplinkPortgroup  DistributedVirtualSwitch: config.maxPorts  DistributedVirtualSwitch: config.numPorts  DistributedVirtualSwitch: config.uplinkPortPolicy  DistributedVirtualSwitch: uuid  DistributedVirtualSwitch: config.host
exec	Get all Distributed Virtual Port Groups with properties (4.0+)	DistributedVirtualPortGroup: key  DistributedVirtualPortGroup: config.defaultPortConfig  DistributedVirtualPortGroup: config.distributedVirtualSwitch  DistributedVirtualPortGroup: config.type

## VMware vROps Connection Manual

The job adapter discovers the VMware vROps server connection.

Permissions information is unavailable or no permissions are required.

## VMware vROps Topology by WebServices

The job adapter discovers the VMware vROps Topology by the vROps API.

Permissions information is unavailable or no permissions are required.

# Virtualization - Xen

## Xen and KVM by Shell

The job kVM and Xen discovery adapter based on libvirt cli.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Virtual Domain Parameters	virsh dumpxml <domain_name>
exec	List of existing Virtual Domains	virsh list
exec	List bridge configuration	brctl show
exec	List Hypervisor version information	virsh version
exec	Host system information	uname echo <variable> locale -a ifconfig -a

# Web Servers - Apache Tomcat

## Apache Tomcat by Shell

The job discovers Apache Tomcat Web servers.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic login	echo \$  locale -a  uname  ver  wmic OS Get CodeSet OS Get OSLanguage
exec	Discover Apache Tomcat Topology	type <file_path>  cat <file_path>  dir <file_path> /s /b <file_path> /B /A:D <file_path> /B /A:-D  ls -lA <folder_path>  hostname  PATH=\${PATH}"/bin:/usr/bin" && export PATH  find <file_path> -name <file_name> -type f  Windows: wmic path Win32_Process get ParentProcessId, commandLine, creationdate, executablepath, name, processId /value  java -version

# Web Servers - Basic

## Web Server Detection using TCP Ports

The job this adapter discovers web servers using TCP ports.

Permissions information is unavailable or no permissions are required.

## WebSphere to Web Server Dependency

The job pattern discovers dependencies between web servers and WebSphere application servers.

Permissions information is unavailable or no permissions are required.

## Web Server by Shell

The job discovers Apache web servers using the Shell protocols.

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic Login	Windows: chcp Windows: ver UNIX: uname Windows: wmic OS Get CodeSet OS Get OSLanguage UNIX: locale -a UNIX: ls -lLF -d UNIX: echo \${SHELL} \${PATH:-}
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" Windows: wmic datafile where "name='<file_path>' get LastModified /format:list 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 - IIS

### IIS Applications by NTCMD or UDA or PowerCmd

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

Protocol: Shell

Operation	Usage description	Objects and parameters
exec	Basic login	ver  uname  wmic OS Get CodeSet OS Get OSLanguage
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 W3SVC/{SITENUM}/Root/{IIS_DIR} adsutil.vbs ENUM /p "W3SVC/{SITENUM}/Root" adsutil.vbs ENUM /p "W3SVC/{SITENUM}/Root/{IIS_DIR}" 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  type <file_path>  wmic datafile where "name='<file_path>'" get LastModified  dir /B  nslookup <hostname>  hostname

### Web Services by URL

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

Permissions information is unavailable or no permissions are required.

## **iSeries By Eview**

### **IBM i Connection**

The job this discovery adapter connects to the Eview iSeries Agent.

Permissions information is unavailable or no permissions are required.

### **IBM i Objects**

The job this adapter discovers the IBM ISeries Objects such as Job Queues , Output Queues, Libraries, Files, Programs.

Permissions information is unavailable or no permissions are required.

### **IBM i Resources**

The job this adapter discovers the IBM ISeries Resources on the on an Iseries box such as CPUs , Memory, Disks, Network Controllers, Installed Software.

Permissions information is unavailable or no permissions are required.

# vCloud

## vCloud Director URL by vCloud API

The job adapter discovers VMware vCloud Director using direct connection URL by vCloud API.

Protocol: vCloud

Operation	Usage description	Objects and parameters
exec	Login to vCloud	vcloudClient: login
exec	Get organizations	vcloudClient: getOrgRefsByName vcloudClient: getOrganizationByReference organizationReference
exec	Get vDC	vcloudClient: getVdcRefsByName organization vcloudClient: getVdcByReference vdcReference
exec	Get vApps	vcloudClient: getVappRefsByName vdc vcloudClient: getVappByReference vappReference
exec	Get Virtual Machines in vApp	vcloudClient: getChildrenVms vApp vcloudClient: getNetworkConnectionSection vm
exec	Get Catalogs and contents	vcloudClient: getCatalogRefs organization vcloudClient: getCatalogByReference catalogReference vcloudClient: getCatalogItemReferences catalog vcloudClient: getCatalogItemByReference catalogItemReference vcloudClient: getMediaByReference mediaReference vcloudClient: getVappTemplateByReference vappTemplateReference
exec	Get Administrative Client	vcloudClient: getVcloudAdmin
exec	Get System Organization	vcloudAdmin: getSystemAdminOrg
exec	Get administrative settings of organizations	vcloudAdmin: getAdminOrgRefsByName vcloudAdmin: getAdminOrgByReference adminOrganizationReference
exec	Get Provider vDC	vcloudAdmin: getProviderVdcRefsByName vcloudAdmin: getProviderVdcByReference providerVdcReference
exec	Get administrative settings of vDC	vcloudAdmin: getAdminVdcRefsByName providerVdc vcloudAdmin: getAdminVdcByReference adminVdcReference



exec	Get Admin Extension and global settings	vcloudClient: getVcloudAdminExtension vcloudAdminExtension: getVcloudAdminExtensionSettings
------	---	---

## vCloud Director by vCloud API

The job adapter discovers VMware vCloud Director using vCloud API.

Protocol: vCloud

Operation	Usage description	Objects and parameters
exec	Login to vCloud	vcloudClient: login
exec	Get organizations	vcloudClient: getOrgRefsByName vcloudClient: getOrganizationByReference organizationReference
exec	Get vDC	vcloudClient: getVdcRefsByName organization vcloudClient: getVdcByReference vdcReference
exec	Get vApps	vcloudClient: getVappRefsByName vdc vcloudClient: getVappByReference vappReference
exec	Get Virtual Machines in vApp	vcloudClient: getChildrenVms vApp vcloudClient: getNetworkConnectionSection vm
exec	Get Catalogs and contents	vcloudClient: getCatalogRefs organization vcloudClient: getCatalogByReference catalogReference vcloudClient: getCatalogItemReferences catalog vcloudClient: getCatalogItemByReference catalogItemReference vcloudClient: getMediaByReference mediaReference vcloudClient: getVappTemplateByReference vappTemplateReference
exec	Get Administrative Client	vcloudClient: getVcloudAdmin
exec	Get System Organization	vcloudAdmin: getSystemAdminOrg
exec	Get administrative settings of organizations	vcloudAdmin: getAdminOrgRefsByName vcloudAdmin: getAdminOrgByReference adminOrganizationReference
exec	Get Provider vDC	vcloudAdmin: getProviderVdcRefsByName vcloudAdmin: getProviderVdcByReference providerVdcReference

exec	Get administrative settings of vDC	vcloudAdmin: getAdminVdcRefsByName providerVdc  vcloudAdmin: getAdminVdcByReference adminVdcReference
exec	Get Admin Extension and global settings	vcloudClient: getVcloudAdminExtension  vcloudAdminExtension: getVcloudAdminExtensionSettings