

Orchestration for VMware Support Prior to Calgary

ServiceNow

Introduction

Orchestration VMware Support Plugin

Overview

The VMware application for cloud provisioning enables users to request VMware virtual servers through the ServiceNow service catalog. When a user requests a virtual server, Orchestration executes preconfigured approval and provisioning tasks. If the request is approved, Orchestration automatically creates a virtual server from a stored template, configures the virtual machine, and then starts the server. Cloud provisioning is available with the Calgary release.

VMware for cloud provisioning is a feature of Orchestration, which is available as a separate subscription from the rest of the ServiceNow platform.

Upgrade Instructions

After you upgrade from an earlier version to the Calgary release, the information in VMware vCenter must be updated. To add data and update the relationships, either run ServiceNow Discovery or discover vCenter details using the discovery utility that does not require the full Discovery product.

How it Works

Orchestration in the ServiceNow platform integrates with the vCenter ^[1] API and adds VMware workflow activities to the existing Workflow application. These activities enable Orchestration to clone new virtual machines from templates, configure virtual machines, and power virtual machines on and off.

Provisioning Tasks by Group

Tasks for setting up a virtualization product, provisioning virtual resources, and requesting virtual machines from the service catalog depend on the user group to which you belong.

- **Virtual Provisioning Cloud Administrator:** Members of this group own the cloud provisioning environment and are responsible for configuring the different virtualization providers used by cloud provisioning. Administrators can create service catalog items from VMware templates and Amazon EC2 images, approve requests for virtual machines, and monitor the cloud provisioning environment using the Service Monitoring Portal.
 - **Virtual Provisioning Cloud Operator:** Members of this group fulfill provisioning requests from users. Operators perform the day-to-day work of cloud provisioning by completing tasks that appear in the Cloud Operations Portal. Operators are assigned to specific virtualization providers and must be technically adept with the products they support.
 - **Virtual Provisioning Cloud Users:** Members of this group can request virtual machines from the service catalog and use the My Virtual Assets portal to manage any virtual machines that are assigned to them.
-

Asset Management Integration

The My Assets plugin creates a new model and model category called **VMware Instance**. The system creates a new asset for this model when cloud provisioning fulfills a virtual machine request, and then creates a VMware configuration item (CI). The new asset appears in the requester's My Assets portal. When the virtual machine is terminated, asset management retires the asset. The My Assets plugin is automatic for new Calgary instances, but must be activated for upgraded instances.

Activating the Plugin

Users with the admin role can activate the My Assets plugin on an instance upgraded to Calgary.

Click the plus to expand instructions for activating a plugin.

If you have the admin role, use the following steps to activate the plugin.

1. Navigate to **System Definition > Plugins**.
2. Right-click the plugin name on the list and select **Activate/Upgrade**.

If the plugin depends on other plugins, these plugins are listed along with their activation status.

3. [Optional] If available, select the **Load demo data** check box.

Some plugins include demo data—sample records that are designed to illustrate plugin features for common use cases. Loading demo data is a good policy when you first activate the plugin on a development or test instance. You can load demo data after the plugin is activated by repeating this process and selecting the check box.

4. Click **Activate**.

Requirements

- All virtual machine templates must contain VMware Tools.
- For Windows virtual machines (VMs), click here ^[2] to determine whether Microsoft Sysprep is required on the vCenter instance.
- The vCenter user must have proper credentials for cloning, customization, and powering on the virtual machine.
- On Windows 2003 templates, the password for an Administrator must be blank on the base image.

Activating the Plugin

This feature requires the Orchestration - VMware Support plugin. VMware for cloud provisioning is a feature of Orchestration, which is available as a separate subscription from the rest of the ServiceNow platform.

Selecting a role for the VMware vCenter integration

While configuring ServiceNow to connect to vCenter, you supply credentials for a vCenter user. The user's permissions in vCenter determine which VMware tasks the user can perform in the ServiceNow instance. Based on the role that you select, you can implement one of a variety of levels of permission.

Administrator role in VMware

The Administrator role provides all privileges available in vCenter. This includes access to every operation that ServiceNow supports plus all of the features that ServiceNow does not use. Using the Administrator role is a simple way to grant a ServiceNow instance full power.

Full access

It is possible to define a role that provides the ServiceNow instance enough access to perform all supported operations without granting full Administrator privileges. With this role, ServiceNow users can run Discovery, view all resources, perform all operations (Start, Stop, Pause, Snapshot, Terminate, VM Modifications), and provision new VMs (including guest customization).

One way to accomplish this is to clone the "Virtual Machine Power User (sample)" role that is provided with vCenter and then edit the role to add the following additional permissions:

- Datastore > Allocate Space
- Network > Assign Network
- Resource > Assign virtual machine to resource pool
- Virtual Machine > Inventory > Create from existing
- Virtual Machine > Inventory > Create new
- Virtual Machine > Inventory > Remove
- Virtual Machine > Provisioning (All in this category)

Virtual Machine Power user

The "Virtual Machine Power User (sample)" role that is provided with vCenter allows a user to browse the datastore, schedule tasks, and perform many VM operations. The role enables ServiceNow users to run Discovery, view all resources, and perform the Start, Stop, Pause, and Snapshot operations and to perform VM modifications like adding a disk.

This role does not have permission to provision new VMs or to terminate existing VMs.

Virtual Machine user

The "Virtual Machine User (sample)", slightly less powerful than the Power User role, allows a user to browse the datastore, schedule tasks, and perform some VM operations. It provides enough for ServiceNow users to run Discovery, view all resources, and perform the Start, Stop, and Pause operations.

The role does not have permission to provision new VMs, terminate existing VMs, manage snapshots, or make VM configuration modifications.

Read-only user

The "Read-only" role allows a user limited read access to the system without any other privileges. The role allows ServiceNow users to run Discovery and view resources.

The role does not have permission to provision new VMs or to run any VM operations.

Enhancements

Eureka

- The new activities Delete Snapshot, Get VM Events, and Get VM Guest Info are available.
- Configuration of Windows VMs has been updated to support Windows workgroups.
- An alternate IP address can be provided when using an IP pool to select a static IP address.
- DHCP is supported for configuring VMs.
- A cloud administrator can provision VMs to use datastores with the least remaining space sufficient to create the VM.

References

[1] <http://www.vmware.com/products/vcenter-server/>

[2] http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1005593

Requesting a Virtual Server - Versions Prior to Calgary

Overview

Users can request a Windows or Linux virtual server in the ServiceNow service catalog. Requested virtual servers are subject to normal approvals and some special provisioning tasks. A decommissioning workflow enables a user to make a service catalog request for the deletion of a virtual server. Any virtual server created from an instance can be destroyed from that instance. This functionality requires the Orchestration VMware Support plugin.



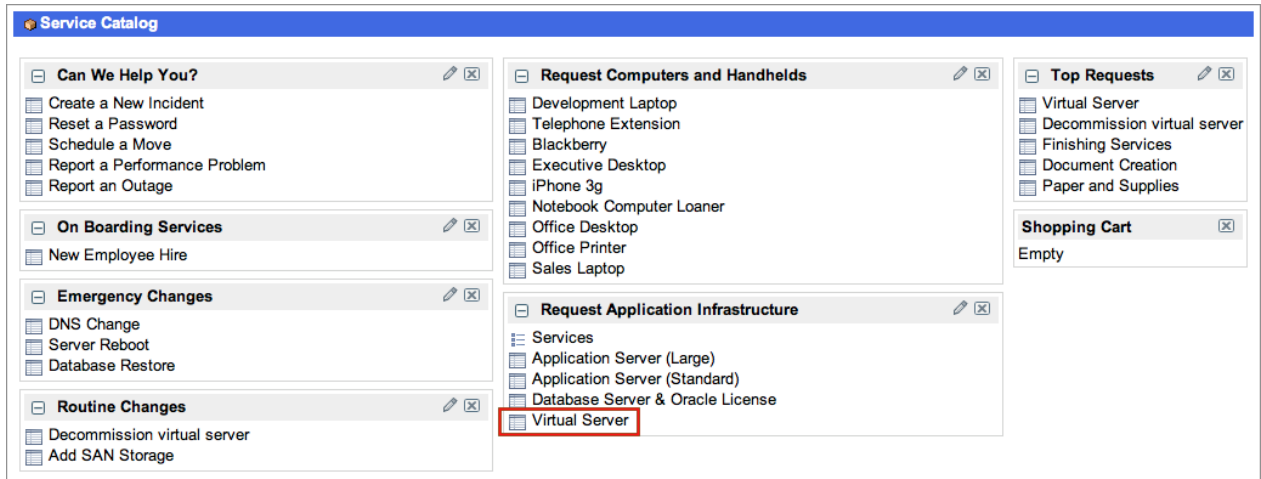
Note: *If you are using the ServiceNow Calgary release or later, see [Requesting a VMware Instance in Cloud Provisioning](#).*

Administrators

For details about provisioning virtual machines, see Enabling VMware Provisioning.

Requesting a Virtual Server

1. Navigate to *Self-Service* > *Service Catalog* and select **Virtual Server**.



2. In the Catalog Item form for this virtual server, complete the following fields:
 - **Operating System:** Select the OS of the virtual server you are requesting.
 - **Class:** Select a class of server for this operating system that has the desired features (memory, storage, CPU speed).
 - **Purpose of requested virtual server:** Type a brief justification for this request for the approvers.
 - **Notes for the provisioners:** Add any information that the provisioners should know, such as the virtual server's network name.
3. Click **Order Now**.

The Order Status form appears, displaying a request summary and a **Stage** indicator for tracking the progress of the request.

Description	Delivery Date	Stage	Price (ea.)	Qty	Total
Request a new virtual Windows or Linux server.	2011-01-06	⊕ →	\$50.00	1	\$50.00
Total:					\$50.00

- Bookmark this page and return to it to track the status of this request.

You are notified by email notification of the results of your request.

Decommissioning a Virtual Server


Requesting the decommissioning of virtual servers through the service catalog launches a workflow that uses the **Destroy VMware** activity.

- Navigate to **Self-Service > Service Catalog > Routine Services** and select **Decommission virtual server**.

- In the Catalog Item form, select a VM from the **Virtual server to decommission** list.
- Click **Order Now** to destroy this virtual server.

***Note:** This action is irrevocable and launches the **VMware - Decommission** Workflow immediately. The virtual server is destroyed without any further user involvement.*

The Order Status form appears, displaying a request summary and a **Stage** indicator for tracking the progress of the request.




 **Order Status**

Summary

Your request number is **REQ0010048**, which you can use to refer to this request in future interactions with the service desk.


You may also bookmark the following link to get back to [REQ0010048](#).


Note that clicking on the bookmark link (above) will simply take you back to this screen.


Description	Delivery Date	Stage	Price (ea.)	Qty	Total
Decommission a virtual server	2011-01-07	  	\$0.00	1	\$0.00
Total:					\$0.00

Delivery Information

Estimated Delivery Date of Complete Order: **2011-01-07**

 **Catalog**

 **Home**



4. Bookmark this page and return to it to track the status of this request.

Users are notified by email of the results of their request.

Configuration

Configuring VMware - Versions Prior to Calgary

Overview

Configuring Orchestration for VMware requires these steps, in order:

1. Install and configure vCenter.
2. Create virtual server templates on the ESX Server.
3. Create vCenter and ESX records in ServiceNow.
4. Configure the Windows and Linux connection information.
5. Allocate IP addresses for virtual servers on the network.
6. Assign users to the default approval and provisioning groups.
7. Configure the virtual server products that a user selects in the service catalog.
8. Configure the datastores.



Note: If you are using a version of ServiceNow earlier than Calgary, see previous version information in *Configuring VMware - Versions Prior to Calgary*.

Required Roles

Users who are members of the Virtual Provisioning Cloud Administrators group (cloud_admin role) can configure VMware accounts in ServiceNow.

vCenter and the ESX Server

vCenter is the VMware management console that manages the activities of ESX Servers. ESX Servers contain the virtual server templates and hosts running virtual machines. Refer to VMware product documentation for instructions about installing and configuring vCenter and ESX Servers. Observe the following requirements when setting up ServiceNow to interact with vCenter and the ESX Server:

- Ensure that all VMware products advertised in the ServiceNow service catalog have corresponding templates on the ESX Server. The names of the templates on the ESX Server should be descriptive enough to simplify selection during the manual phase of provisioning.
- The MID Server probe's user must log in to vCenter with the proper VMware role to execute the probe's action.
- ServiceNow supports Cloud Provisioning on vCenter versions 4.1 through 5.1. Using Cloud Provisioning with other versions of vCenter may cause unexpected results.

ESX Servers

With the proper credentials, ServiceNow Discovery can detect and explore all the ESX Servers in a network. Discovery returns the hardware characteristics of the ESX machines and the relationships to the other VMware components. If you are not using ServiceNow Discovery, you must configure each ESX Server record manually. To view the ESX records in ServiceNow, navigate to **VMware > Configuration > ESX Servers**.

To configure the relationships between VMware components manually, click the green plus sign (+) beside **Related Items** and use the Define Relationships form provided. See VMware Component Relationships for the relationships in the base ServiceNow system.

ESX Server [Update] [Delete CI]

Name: dev-esx Company: [Search]

Asset tag: [Search] Serial number: VMware-42 2e ff b4 ca f0 2b b8-66 6a 2e 10 92 37 0e ac

Manufacturer: [Search] Model ID: [Search]

Asset: [Search] Assigned to: [Search]

Configuration

URL: [Search] RAM (MB): 8,191

Operating System: ESX CPU manufacturer: [Search]

OS Domain: [Search] CPU type: [Search]

OS Version: [Search] CPU speed (MHz): 2,666

OS Service Pack: [Search] CPU count: 2

DNS Domain: [Search] CPU core count: 1

Disk space (GB): 123

Description: Intel(R) Xeon(R) CPU X5650 @ 2.67GHz

Related Items [Show 3 Levels]

- Member of - VMware vCenter Clusters
 - Dev Cluster
- Has registered - VMware Virtual Machine Templates
 - Dev-Server2008-StandardBuild-Template
 - Dev-RHEL6-CustomBuild-Template
 - Dev-RHEL6-StandardBuild-Template
 - Dev-Server2008-NightlyBuild-Template
 - Dev-RHEL6-NightlyBuild-Template
 - Dev-Server2008-CustomBuild-Template
- Has registered - VMware Virtual Machine Instances
 - Dev-RHEL6-CustomBuild

vCenter

Create a record for each vCenter instance in the network.

1. Navigate to **VMware > Configuration > vCenter Instances**.
2. Click **New**.
3. Enter the **Name** of an active vCenter machine and the **URL** to the instance, then save the record.

The location of this vCenter is for convenience and is not used anywhere else.

4. Click the **Discover vCenter Details** related link to have ServiceNow explore vCenter and record the relationships between the vCenter and the other VMware components.

This action does not require the ServiceNow Discovery application, but performs the same type of scan. For more information on this utility, see Gathering vCenter Data Without Running Discovery. A MID Server is required for this procedure. See VMware Component Relationships for the relationships provided in the base system.

VMware vCenter Instance [Update] [Delete]

Name: vCenter@server2008

Full name: VMware vCenter Server 5.0.0 build-455964

API version: 5.0

URL: <https://10.15.235.24/sdk>

Related Items: [List Icon] [Grid Icon] [Show 3 Levels]

Manages - VMware vCenter Datacenters

- San Diego Dev Data Center
- Seattle Staging Data Center
- Virginia QA Data Center
- San Jose Prod Data Center

[Update] [Delete]

Related Links

[Discover vCenter Details](#)

[Subscribe](#)

Scheduled discoveries [New] [Edit...] Go to [Scheduled discovery] [Search]

vCenter instance = vCenter@server2008

Scheduled discovery

Discovery
Monday morning

[Actions on selected rows...]

VM Configuration in ServiceNow

The VM configuration in ServiceNow provides the information necessary to create each type of virtual server offered in the service catalog and to power up the virtual machines on the network. This includes:

- List of available IP addresses (IP pools) to assign to virtual machines as they are added to the network.
- Credentials and connection information for Windows and Linux.
- Catalog offering configuration.

IP Pools

IP pools are collections of IP addresses that can be or have been assigned to newly-provisioned virtual machines (VMs). Each IP pool can be associated with one or more VMware networks. When the Select IP Address activity runs, it identifies the IP pools associated with the VMware network selected for the virtual machine (generally by the Select Datacenter, Network, and Folder activity), chooses the one with the most available IP addresses, and allocates an IP address to the virtual machine from that pool.

An administrator must ensure that there are IP pools associated with all active VMware networks and that the IP pools contain enough IP addresses to meet the demand for new virtual servers. Associate VMware networks with an IP pool by editing the **VMware Network** related list on the IP Pool form. When you provision a new virtual machine through vCenter, select a VMware network. Orchestration assigns an available IP address from the VMware network's IP pool to the new virtual machine. If the VMware network contains multiple IP pools, Orchestration selects an IP address from the pool with the most available addresses.



Note: vCenter contains VMware networks that Discovery (including DiscoverNow) adds to the CMDB as VMware CIs.

To add a new IP pool:

1. Navigate to **VMware > Rules > IP Pools** and click **New**.
2. Enter the specifics of the network in which virtual servers will be created. An optional **Alternate DNS Server IP** can be specified, starting with the Eureka release.

IP Pool

Name:

San Diego QA Data Center

Network:

10.0.15.0/24

Gateway IP:

10.0.15.1

DNS Server IP:

10.0.15.5

Alternate DNS Server IP:

10.0.15.15

Submit

VM IP Pool Configuration

3. Save the record.
4. To add IP addresses to the pool, click **Add Allocatable IPs** under **Related Links**.
5. Add ranges, networks, or individual addresses in a comma separated list.

IP Pool

Update

Delete

Name:

San Diego QA Data Center

Network:

10.0.15.0/24

Gateway IP:

10.0.15.1

DNS Server IP:

10.0.15.5

Alternate DNS Server IP:

10.0.15.15

Update

Delete

Related Links

Add Allocatable IPs

Virtual Machine Allocatable IP Addresses

Add Allocatable IP Addresses

Enter comma-separated IP address ranges, IP networks, or individual IPs describing the IP addresses to be added. For example:
10.0.1.0/24,10.0.2.1-10.0.2.15,10.0.3.176,10.0.3.222
This example specifies an IP network with valid IP addresses between 10.0.1.1 and 10.0.1.254 inclusive, an IP address range from 10.0.2.1 to 10.0.2.15 inclusive, and the two individual IP addresses 10.0.3.176 and 10.0.3.222. Any entries you make that cannot be interpreted will simply be ignored.

10.0.15.135-10.0.15.142-10.0.15.195-10.0.15.202

Allocate IP Addresses

Cancel

VM IP Pool Allocation

6. Click **Allocate IP Addresses**.

ServiceNow lists each IP address separately in the related list and marks them as not in use. When a VMware instance is provisioned, Orchestration marks the address as **In use** and associates the virtual machine name with the IP address in the IP pool record.

IP Pool

Update

Delete

Name:

San Diego QA Data Center

Network:

10.0.15.0/24

Gateway IP:

10.0.15.1

DNS Server IP:

10.0.15.5

Update

Delete

Related Links

Add Allocatable IPs

Virtual Machine Allocatable IP Addresses (16)

New

Go to

In use

2

IP Pool - San Diego QA Data Center

	In use	IP Address	VM Instance
<input checked="" type="checkbox"/>	true	10.0.15.202	QA-RHEL6-LoadTest-001
<input checked="" type="checkbox"/>	true	10.0.15.198	QA-RHEL6-UAT-001
<input checked="" type="checkbox"/>	true	10.0.15.142	QA-RHEL6-LoadTest-002
<input checked="" type="checkbox"/>	true	10.0.15.138	QA-RHEL6-LoadTest-002
<input checked="" type="checkbox"/>	true	10.0.15.197	QA-Win7-UAT-001
<input type="checkbox"/>	false	10.0.15.141	
<input type="checkbox"/>	false	10.0.15.135	
<input type="checkbox"/>	false	10.0.15.137	
<input type="checkbox"/>	false	10.0.15.201	
<input type="checkbox"/>	false	10.0.15.140	
<input type="checkbox"/>	false	10.0.15.200	
<input type="checkbox"/>	false	10.0.15.196	
<input type="checkbox"/>	false	10.0.15.199	
<input type="checkbox"/>	false	10.0.15.195	
<input type="checkbox"/>	false	10.0.15.139	
<input type="checkbox"/>	false	10.0.15.136	

Allocated IP addresses

Name that includes the operating system.

Windows VMs

The following describes how to configure Windows connection information starting with the Eureka release. If you are using an earlier release, see previous version information.

To configure Windows connection information:

1. Navigate to **VMware > Customization Specifications > Windows** and click **New**.

2. Enter a unique and descriptive

This value appears in the **Operating System** choice list for the catalog request item. The user's selection tells the provisioning task which configuration information to use.

3. Enter the registered user's name and organization.
4. Enter the **Product key**, select the **License mode**, and, if the selected license type is **Per server**, enter the maximum number of **Concurrent connections**.
5. Enter the **Administrator password**.
6. Choose a **Membership** option, either **Domain** or **Workgroup**. If you choose Workgroup, enter the workgroup name. If you choose, Domain, enter the domain name and login credentials.
7. [Optional] Add any number of Windows commands, each listed on a new line, to the **Run once** field.
8. In the **Choose networking through** field, choose whether to use **IP Pool** or **DHCP**.

9. Click **Submit**.

Windows configuration

Versions Prior to the Eureka Release

Click the plus to expand previous version information

- Navigate to **VMware > Customization Specifications > Windows** and click **New**.
- Enter a unique and descriptive **Name** that includes the operating system.

This value appears in the **Operating System** choice list for the catalog request item. The user's selection tells the provisioning task which configuration information to use.

- Enter the machine and domain login credentials for the virtual machine, the operating system product key, and the registered user's name.
- Select the **License type** and, if the selected license type is **Per server**, enter the maximum number of **Concurrent connections** (Dublin release).
- [Optional] Add any number of Windows commands, each listed on a new line, to the **Run once** field (Dublin release).

- Click **Submit**.


Linux VMs

To configure Linux connection information:

1. Navigate to **VMware > Customization Specifications > Linux** and click **New**.
2. Enter a unique and descriptive **Name** that includes the operating system.

This value appears in the **Operating System** choice list for the catalog request item. The user's selection tells the provisioning task which configuration information to use.

3. Enter the DNS name in the **Domain** field.
4. Choose whether to use IP Pool or DHCP in the **Choose networking through** field (Eureka release).



Virtual Machine Linux Configuration

Name: SUSE Linux Enterprise Desktop

Domain: servicenow.com

Configure networking through: IP pool

Submit

Linux configuration

5. Click **Submit**.

Group Membership

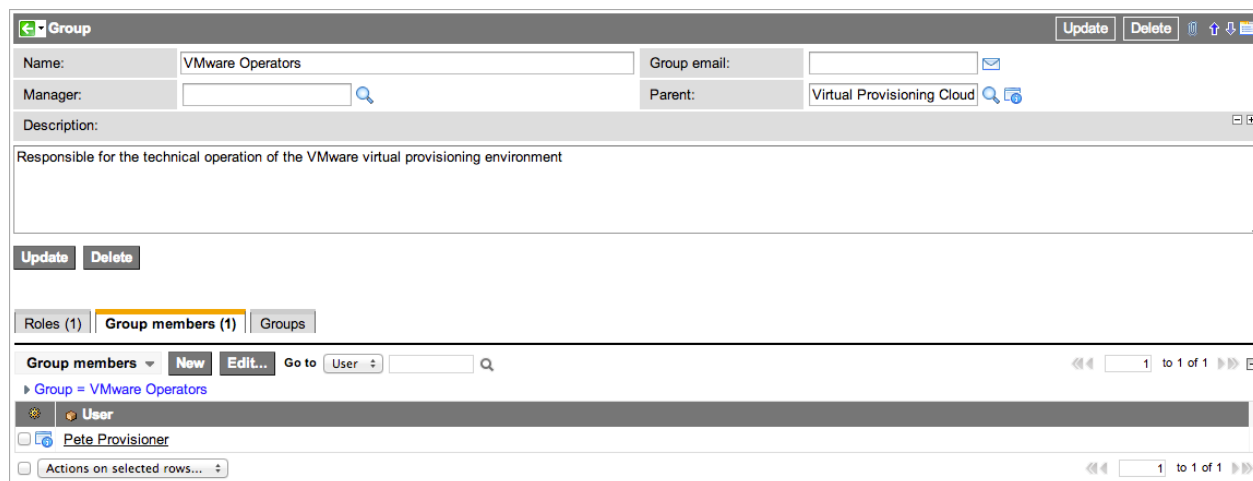
Activating the Orchestration - VMware Support plugin installs the following

groups:

- **VMware Approvers:** approve requests for VMware instances.
- **VMware Operators:** are responsible for the technical operation of the VMware cloud provisioning environment.

To add users to these groups:

1. Navigate to **User Administration > Groups**.
2. Open **VMware Operators** from the list of groups.
3. Go to the **Group Members** related list and click **Edit**.
4. Select one or more users from the list and click **Save**.



Group

Name: VMware Operators

Manager:

Group email:

Parent: Virtual Provisioning Cloud

Description:

Responsible for the technical operation of the VMware virtual provisioning environment

Update Delete

Roles (1) Group members (1) Groups

Group members New Edit... Go to User

Group = VMware Operators

User

Pete.Provisioner

Actions on selected rows...

5. Repeat this process to add members to the **VMware Approvers** group.

Configuring the Catalog Offering

The products you configure in the service catalog must represent accurately the items they offer. Users can select from lists of preconfigured virtual servers or build their own server.

Size Selections

A VMware size defines a virtual hardware package that includes predefined number of CPUs, amount of memory, data disk size, and related details. Users can choose a VMware size or select separate attributes. When the user selects a size, the individual selections for CPU, memory, and disk size are hidden.

1. Navigate to **VMware > Service Catalog > Sizes** and click **New**.
2. Complete the form with the following considerations:
 - The **Name** should indicate some increment of size, such as **Large** or **Standard**.
 - In the **CPUs**, **Memory**, and **Data disk size** fields, enter a *label* to appear in the service catalog. For example, enter **4 GB** of memory or **30 GB** for the data disk size.
 - In the corresponding **value** fields, enter the value of that element in the specified units. For example, a data disk size with a label of **30 GB** has a value of **30,720** (in MB).
3. Click **Submit**.

Name: Medium		Price: \$310.00	
Order: 2		Value: 2	
CPUs label: 2		Value (MB): 2,048	
Memory label: 2 GB		Value (MB): 15,360	
Data disk size label: 15 GB			
Description: 2 CPUs 2 GB memory 15 GB additional data disk			
Update		Delete	

Offering Selections

1. Navigate to **VMware > Service Catalog > Offerings** and click **New**.
2. Enter the virtual server's **Offering** description as it should appear in the service catalog.
Typically, this contains the operating system and some version information, such as **Windows Server 2003** or **CentOS 6**.
3. Click **Submit**.

Pricing

All prices for virtual servers or modifications to virtual servers are calculated from the per-unit price for the following components:

- CPU
- Memory
- Data disk size

The Catalog VM Element Price [sc_vm_element_price] table stores the prices for VMware components included in the base system. Each component has a single record that defines the units and the price per unit. Users with the cloud_admin role can access these records to change the unit price for each component.

To change the price for a component:

1. Navigate to **VMware > Service Catalog > Prices**.
2. Select a component.

3. Enter the new price per unit in the **Service catalog price** field.

4. Click **Update**.

ServiceNow recalculates the price for all items in the service catalog that use this **Element type**.

Editing Prices

By default, the price of an instance is determined by the selection in the **VM Size** field in the VMware Catalog Item form. If a requester changes the desired size when ordering a virtual machine, or an administrator changes the price of the size, ServiceNow recalculates the instance price automatically. The administrator can make price changes by modifying the specifications of the instance in the VMware Size Definition form or override the calculated price in the VMware Catalog Item form when creating a service catalog item. You cannot adjust instance size prices by editing quantities in the VMware Size Definitions list view.

1. Navigate to **VMware > Service Catalog > Sizes**.
2. Select a size.
3. Change the quantity of CPUs, the memory, or the data disk size.
4. Click **Update**.

ServiceNow calculates the price of the modified size.

CPU Selections

You can customize service catalog hardware selections so that users can request the number of CPUs for a virtual server. The service catalog shows the CPU option only when the user declines the choice of a predefined virtual server size.

1. Navigate to **VMware > Service Catalog > CPU Selections** and click **New**.
2. In the **CPUs label** field, enter a description of this CPU selection to be displayed in the service catalog.
3. In the **Value** field, enter the quantity for this CPU selection.

Be sure the **CPU label** quantity matches the number in the **Value** field. ServiceNow calculates the cost for each CPU quantity based on the configured price per unit.

4. Click **Submit**.

Memory Selections

You can customize service catalog hardware selections so that users can request a specific amount of memory for a virtual server. The service catalog shows the VM memory option when the user declines the choice of a predefined virtual server size.

1. Navigate to **VMware > Service Catalog > Memory Selections** and click **New**.
2. In the **Memory label** field, enter the memory quantity to be displayed in the service catalog.

This field typically includes a number and size abbreviation, such as **4 GB**.

3. Enter the **Value** for this memory selection as an integer representing the total number of MB.

In the example used here, 4 GB of memory would have a value of **4,096**. ServiceNow calculates the cost for the amount of memory selected based on the configured price per unit.



4. Click **Submit**.

Data Disk Size Selections


You can customize service catalog hardware selections so that users can request the virtual server's data disk size. The service catalog shows the data disk size option only when the user declines the choice of a predefined virtual server *class*.

1. Navigate to **VMware > Service Catalog > Data Disk Size Selections** and click **New**.
2. In the **Data disk size label** field, enter the name to be displayed in the service catalog.

This field typically includes a number and size abbreviation, such as **20GB**.

3. In the **Value** field, enter the number of megabytes of disk space this option represents.

In this examples the data disk would have a value of 20,480. ServiceNow calculates the cost for the disk size selected based on the configured price per unit.



4. Click **Submit**.

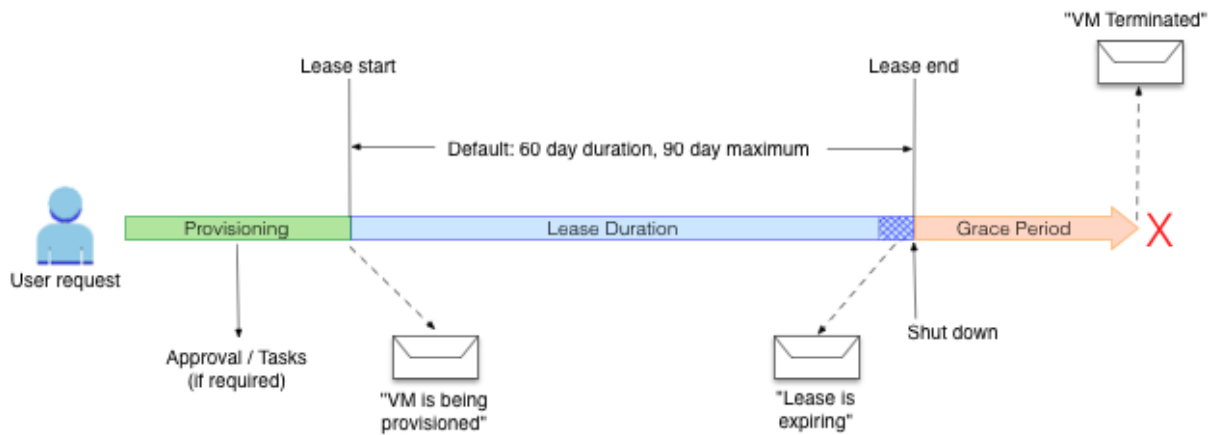
Lease Duration

The default setting for a lease period and the maximum allowed duration of a virtual server lease are controlled by the following properties found in **Cloud Provisioning > Management > Properties** (Calgary release). For instructions on configuring lease start and end times for individual virtual machines, see Requesting a VMware Instance in Cloud Provisioning.

- **Default lease duration:** This property (`glide.vm.lease_duration`) controls the length of the lease period automatically configured for a virtual server request. The default duration is 60 days from the lease start time, which always begins on the current date and time.
- **Max lease duration:** This property (`glide.vm.max_lease_duration`) controls the maximum length of the lease period permitted for a virtual server. The default maximum duration is 90 days from the lease start time. This property prevents virtual resources that have been ignored from running indefinitely.



Note: ServiceNow applies the same values to both Amazon EC2 and VMware lease durations.



Grace Period

A configurable *grace period* enables an administrator to delay the termination of a virtual machine when the lease end date expires. When the lease ends, the virtual machine is powered off, but is available for use until the end of the grace period. To change the default grace period of 7 days, navigate to **Cloud Provisioning > Management > Properties** and edit the value in the **Grace period after lease end until VM termination** property (`glide.vm.grace_period`).

When the lease ends, the platform runs the VMware End of Lease workflow, which notifies the requestor that the lease has expired, and then powers off the virtual machine. The VMware End of Lease workflow evaluates the `glide.vm.grace_period` property to determine when the VMware Termination workflow should run. The requestor is notified when the virtual machine is terminated, or if termination failed.

To configure a different workflow to run when a lease is terminated.

1. In the application navigation filter, enter **task_action_workflow.list**.
2. Select the **end_of_lease** action for the VMware Virtual Machine Instance [`cmdb_ci_vmware_instance`] table.

3. Select a different workflow to run in the **Workflow** field.
4. Click **Update**.

Managing Datastores

Datastores represent storage locations for virtual machine files. The VM vCenter Datastores form shows the most recent datastore availability and capacity information for the the datastores, and allows you to manage how storage space is handled when provisioning VMs. Using this form you can make most efficient use of space, reducing the amount of wasted space. This section describes datastore functionality available starting with the Eureka release.

How Datastore Space Is Allocated

By allocating reserved space when a VM is requested and accounting for recently provisioned space, the user can be assured that sufficient space will still be available for provisioning when the request is fulfilled. To accomplish this, space on the datastore is processed as follows:

- When a VM is requested, the amount of reserved space is incremented to account for the requested disk size (template size plus additional disk size). If the reserve space request fails because of insufficient space after

discovery, a task to fix the issue is created for the cloud operator. If the VM request is canceled, the reserved space is decremented to remove requested disk space.

- For automated provisioning, the datastore with the least disk space, but sufficient for the VM request, is automatically selected.
- When the VM is provisioned, the reserved space is decremented to remove provisioned disk size, and recently provisioned space is updated to provisioned disk size.
- Whenever a datastore is rediscovered and updated accordingly, the amount of recently provisioned space is reset to 0. When a VM provisioned from a ServiceNow instance is terminated, the provisioned space is released and the free space is incremented. If the workflow is canceled before the VM is provisioned, the reserved space is updated to remove not provisioned disk size.
- When a VM is modified, the requested amount of space is reserved, and the reserved space field is updated. When the Modify VM workflow finishes, the reserved space is updated to decrease the disk size added and the recently provisioned space is increased. When the VM is terminated (Terminate VM), the recently provisioned space in all affected datastores is released.

When a catalog task is created and a cloud operator chooses a datastore, only those datastores with the enough space to continue are shown in the choice list.

Configuring Datastores

The Datastores module allows cloud administrators to configure the VMware vCenter datastores. Cloud administrators can modify recently provisioned space and reserved space fields to manually adjust space usage, and can block VM provisioned space or reserve extra space for specified datastores.

To manage datastores:

1. Navigate to **VMware > Datastores**.

Current information on each datastore is displayed in the table.

2. To set availability for a datastore, double-click the **Availability for provisioning** field and select **Include** or **Exclude**.

Name	Capacity (GB)	Free space (GB)	Recently provisioned space (GB)	Reserved space (GB)	Availability for provisioning
DataStore_0	499.75	7.9140625	0		Include
DataStore_1	616.75	5.9140625	0		Include
DataStore_2	1023.75	5.4609375	0		Include
DataStore_3	1674.75	555.4775390625	0		Include

Datastore configuration

Field	Description
Name	The name of the datastore.
Capacity	The total storage capacity of the datastore.
Free space (GB)	The free space available for VM provisioning on the datastore.
Recently provisioned space (GB)	The space requested by recent VM provisioning requests since the most recent discovery. Whenever a datastore is rediscovered and updated accordingly, the amount of recently provisioned space is reset to 0. If a VM was terminated, the provisioned space may be a negative number.
Reserved space (GB)	The amount of space reserved on the datastore for scheduled VM provision requests and extra disk space requests for modify VM requests. The Reserved space for the requested VM must be less than Free space - (Recently provisioned space + Reserved space) - Minimum free space in order for that datastore to be used by the VM.
Availability for provisioning	Indicates whether the datastore is available (Include) or unavailable (Exclude) for provisioning. For newly discovered datastores, the default value is Include. Running Discovery does not change this field.

Setting the Minimum Free Disk Space

The minimum free disk space property allows you to set the amount of free disk space on a datastore to ensure the vCenter functions correctly. To set the property, navigate to **Cloud Provisioning > Management > Properties**. This property is available starting with the Eureka release. If you are using an earlier release, see previous version information.

Property	Description
Minimum free disk space on each VMware datastore (MB) [glide.vmware.provisioning.datastore.reserved_space]	The amount of free disk space required on a datastore. The default value is 1024 MB.

Versions Prior to the Eureka Release

Click the plus to expand previous version information

To view datastore information, navigate to **VMware > Datastores**. The Datastore form shows the following for each datastore:

Field	Description
Name	The name of the datastore.
Capacity	The total storage capacity of the datastore.
Free space (GB)	The free space available for VM provisioning on the datastore.

Accessing the vCenter API - Versions Prior to Calgary




Discovery

Orchestration

Related Topics

- Cloud Provisioning
- Help the Help Desk
- Help the Help Desk Login Script
- ECC Queue
- Useful Related Lists in CI Forms
- Creating a Workflow
- Using Workflow Activities

Get the Book

-  Discovery
-  Data Collected by Discovery
-  Orchestration for VMWare

Overview

ServiceNow VMware Orchestration activities require specific user privileges to access the vCenter APIs necessary to run workflows for VMware support. These login privileges are not for use within the ServiceNow platform, but are configured for the VMware activities on the vCenter instance. Refer to the vCenter documentation^[1] for assistance.

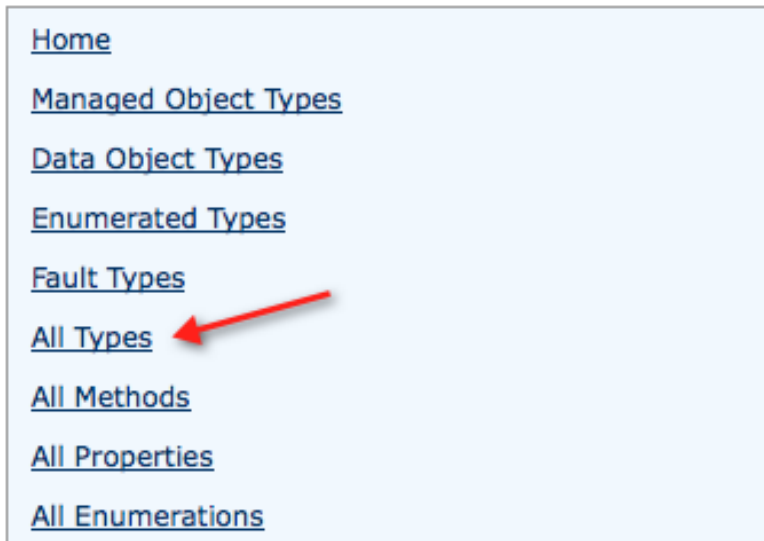


Note: If you are using the ServiceNow Calgary release or later, see *User Privileges for vCenter API for Cloud Provisioning*.

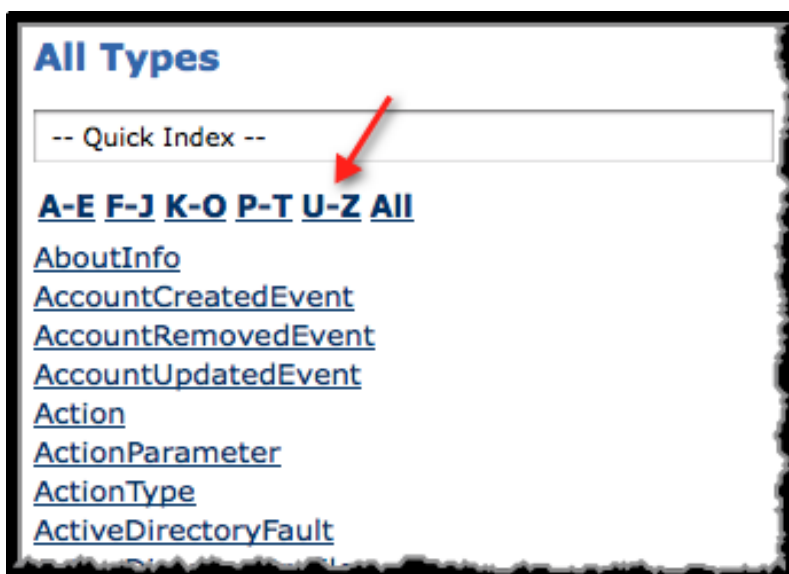
Determining Privileges

To determine the user privileges required by the VMware activity that logs into vCenter:

1. Navigate to the VMware API **documentation**^[2].
2. In the vCenter API page, select **All Types** in the left navigation menu.




3. Click **U-Z** in the API index that appears.



4. Select **VirtualMachine** in the index.

Information appears about a VirtualMachine object in the API.

5. Select **Local Methods** from the navigation menu at the top of the page.

Managed Object Types	Data Object Types	Local Properties	Local Methods 
		All Properties	All Methods

Managed Object - VirtualMachine

Property of

[AutoStartPowerInfo](#), [CannotChangeDrsBehaviorForFtSecondary](#), [CannotChangeHaSettingsForFtSecondary](#), [CheckResult](#), [ClusterAffinityRuleSpec](#), [ClusterAntiAffinityRuleSpec](#), [ClusterAttemptedVmInfo](#), [ClusterDasVmConfigInfo](#), [ClusterDrsFaultsFaultsByVm](#), [ClusterDrsMigration](#), [ClusterDrsVmConfigInfo](#), [ClusterNotAttemptedVmInfo](#), [ClusterVmGroup](#), [Datastore](#), [DVSSummary](#), [FailToLockFaultToleranceVms](#), [FaultToleranceCannotEditMem](#), [FaultTolerancePrimaryConfigIn](#)

6. Click the following methods to see the required vCenter login privileges:

- **CloneVM_Task**: No privileges are required.
- **CustomizeVM_Task**: Requires **VirtualMachine.Provisioning.Customize**
- **PowerOnVM_Task**: Requires **VirtualMachine.Interact.PowerOn**

Methods

METHODS DEFINED IN THIS MANAGED OBJECT
AcquireMksTicket , AcquireTicket , AnswerVM , CheckCustomizationSpec , CloneVM_Task , CreateScreenshot_Task , CreateSecondaryVM_Task , CreateSnapshot_Task , CustomizeVM_Task , DefragmentAllDisks , DisableSecondaryVM_Task , EnableSecondaryVM_Task , ExportVm , ExtractOvfEnvironment , MakePrimaryVM_Task , MarkAsTemplate , MarkAsVirtualMachine , MigrateVM_Task , MountToolsInstaller , PowerOffVM_Task , PowerOnVM_Task , PromoteDisks_Task , QueryChangedDiskAreas , QueryFaultToleranceCompatibility , QueryUnownedFiles , RebootGuest , ReconfigVM_Task , RefreshStorageInfo , reloadVirtualMachineFromPath_Task , RelocateVM_Task , RemoveAllSnapshots_Task , ResetGuestInformation , ResetVM_Task , RevertToCurrentSnapshot_Task , SetDisplayTopology , SetScreenResolution , ShutdownGuest , StandbyGuest , StartRecording_Task , StartReplaying_Task , StopRecording_Task , StopReplaying_Task , SuspendVM_Task , TerminateFaultTolerantVM_Task , TurnOffFaultToleranceForVM_Task , UnmountToolsInstaller , UnregisterVM , UpgradeTools_Task , UpgradeVM_Task
Methods inherited from ManagedEntity
Destroy_Task , Reload , Rename_Task
Methods inherited from ExtensibleManagedObject
setCustomValue

References

- [1] <http://www.vmware.com/support/pubs/>
- [2] <http://www.vmware.com/support/developer/vc-sdk/visdk41pubs/ApiReference/index.html>

ESX Resource Pools - Versions Prior to Calgary

Discovery

Orchestration

Related Topics

- Cloud Provisioning
- Help the Help Desk
- Help the Help Desk Login Script
- ECC Queue
- Useful Related Lists in CI Forms
- Creating a Workflow
- Using Workflow Activities

Get the Book

[Discovery](#)[Data Collected by Discovery](#)[Orchestration for VMWare](#)

Overview

Resource pools are configured on the ESX Server and define the maximum amount of resources that templates using that pool can consume. An ESX Server property enables resource pools to expand when necessary if the ESX Server has additional resources to spare. The **Name** and **Owner** fields of each resource pool on the ESX Server must be configured within the ServiceNow platform in the `cmdb_ci_esx_resource_pool` table. When Orchestration for VMware executes its manual provisioning tasks, the provisioner must select the proper resource pool for the virtual server requested. Discovery finds resource pools on ESX machines and populates the fields on the ESX Resource Pool form automatically.

Prerequisite Step

Ensure that vCenter and the ESX Server have been fully configured, including the creation of the templates and resource pools. Complete the tasks in Configuring VMware for Orchestration before proceeding with the procedures on this page.

Configuring Resource Pools in ServiceNow

The ESX Server has a default resource pool called **Resources** that defines *normal* resources for a virtual machine. These levels are dynamically generated from *shares* of the total resources allocated to virtual machines on the ESX Server. For details about how these resources are calculated, see the ESX Server Administration Guide ^[1]. ServiceNow Discovery finds this default resource pool and adds a record to the ESX Resource Pools module automatically. If Discovery is not running on the ServiceNow instance, create a record for the **Resources** pool. Ensure that the **Owner** field is correct and leave the resource fields blank. If a provisioner selects the **Resources** pool when provisioning a virtual server, the ESX Server will create a virtual machine for use under a normal load.

1. Navigate to **VMware Provisioning > Virtual Servers > ESX Resource Pools**.
2. Click **New** in the list.

3. Create a new record for each resource pool in the ESX Server, ensuring that the **Name** and **Owner** fields are correct.

The additional fields are for display purposes only, except for the **CPU expandable** and **Memory expandable** fields. Select these check boxes to allow for expansion of the CPU and memory limits when needed if those resources are available on the ESX Server. When granted, these extra resources can be revoked if needed to provision other virtual machines.

4. Click **Submit**.

ESX Resource Pool [Update] [Delete CI] [Icons]

Name:	Resources		
Owner:	labesx01.lab2.service-now		
CPU reserved (MHz):	17561	Memory reserved (MB):	67883
CPU limit (MHz):	17561	Memory limit (MB):	67883
CPU shares:	4000	Memory shares:	163840
CPU expandable:	<input checked="" type="checkbox"/>	Memory expandable:	<input checked="" type="checkbox"/>

Related Items: [Icons] Show 3 Levels [Icon]

- Depends on - MSFT SQL Instances**
 - [vCenter@labvc01] → JSQLEXP_VIM@labvc01(Microsoft SQL Server)
- Depends on - VMwares**
 - [vCenter@labvc01] → JVMWare@labesx01
- Runs on - Computers**
 - [vCenter@labvc01] → Jlabvc01
- Defines resources for - ESX Servers**
 - labesx01.lab2
 - labesx01.lab2
- Managed by - VMware vCenter Instances**
 - [labesx01.lab2] → JvCenter@labvc01

[Update] [Delete CI]

What Do I Do Next?

After recording the ESX Resource Pools, enter the names and hardware characteristics of the VMware templates into the ServiceNow platform.

References

- [1] http://www.vmware.com/support/pubs/esx_pubs.html

MID Server

MID Server Plugin



Note: This article applies to Fuji and earlier releases. For more current information, see *MID Server*^[1] at <http://docs.servicenow.com>. **The ServiceNow Wiki is no longer being updated. Visit <http://docs.servicenow.com> for the latest product documentation.**

Overview

The Management, Instrumentation, and Discovery (MID) Server is a Java application that runs as a Windows service or UNIX daemon. The MID Server facilitates communication and movement of data between the ServiceNow platform and external applications, data sources, and services.

For specific requirements for using the MID Server with Discovery, see *MID Server Requirements for Discovery*. See the following pages for installation and configuration information:

- MID Server Installation
- MID Server Configuration

The MID Server performs the following tasks:

- Communicates securely with the ServiceNow instance to determine what Discovery probes to run
- Runs Discovery probes on the local network to gather data on network devices
- Sends Discovery probe results back to the ServiceNow instance for processing



Note: MID Server communications are initiated inside the enterprise's firewall and therefore do not require any special firewall rules or VPNs.

Functional Architecture

The MID Server is a Java process that oversees 2 main functional groups of sub-processes, namely *Monitors* and *Workers*. A *Monitor* runs in a separate thread as a timer object and is configured to execute a task periodically, returning its result to ServiceNow's **ECC Queue** (External Communication Channel Queue). A *Worker* is an on-demand thread that executes a task when a corresponding ECC output queue record is read from ServiceNow (The Queue Monitor reads the ECC output queue and triggers a Worker). For example, a **Discovery probe** is a Worker.

Monitors

1. Auto Upgrade
2. Heartbeat
3. Queue Monitor
4. Queue Sender
5. Synchronizers
 - Altiris
 - LanDesk

- Microsoft SMS
- JDBC

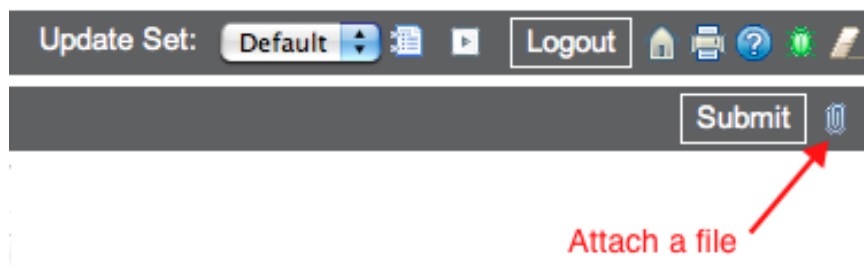
Workers

1. Command Line
2. JDBC
3. File
4. Probes
 - HTTP
 - WMI
 - SNMP
 - SSH

JAR File Synchronization

An administrator can upload a JAR file to an instance and synchronize it to all MID Servers. The administrator can then write custom probes that use the synchronized JAR file. To upload a JAR file to the instance:

1. Navigate to **MID Server > JAR Files**.
2. Click **New**.
3. Complete the following fields:
 - **Name:** A unique and descriptive name for identifying the file in the instance.
 - **Version:** A version number for the file, if one is available.
 - **Source:** Location of the JAR file for reference purposes. Source information is not used by the system.
 - **Description:** Short description of the JAR file and its purpose in the instance.
4. Click the paper clip icon in the banner and attach the JAR file to the record.



5. Click **Submit**.
6. Restart the MID Server service.

The platform makes the JAR file available to any MID Server configured to communicate with the instance.

System Requirements

ServiceNow has tested the MID Server in the following environments:

- Windows Server 2003, 2008, and 2012. All Windows Server 2008 and 2012 editions are supported. Virtual machines and 64-bit systems are supported.
- Linux: Virtual machines and 64-bit systems are supported. On 64-bit Linux systems, you must install the 32-bit GNU C library ^[2] (*glibc*). The installation command for CentOS is: `yum install glibc.i686`

The minimum suggested configuration is:

- 4GB of available RAM per MID Server
- 2+GHZ CPU (Multi-core preferred)

- 500MB of disk space per MID Server
- Can *ride-along* with other services (dependent on server utilization and resource availability)

Java Version Support

The MID Server installs with JRE version 1.8. If you upgrade with a MID Server using JRE 1.6, the system automatically upgrades that MID Server to use version 1.8. Both the 32 bit and 64 bit MID Server use JRE 1.8.

Applications

The MID Server is used by the following applications:

- Discovery
- Orchestration
- Import Sets
- Altiris
- Microsoft SMS / SCCM
- Avocent LANDesk
- HP OpenView Operations
- Microsoft System Center Operations Manager (SCOM)
- Borland Starteam Integration
- Microsoft MIIS

Reports

The following global reports are available for MID Server analytics (starting with the Eureka release).

- MID: Avg Max Memory Percent Use Last 30 Days
- MID Host: Avg CPU Use Percent Per Last 30 Days

MID Servers and System Clones

See KB0547597 ^[3] for a information on what to do with MID servers when you are cloning your instance.

Enhancements

Fuji

- The following records can no longer be modified or deleted:

Table	Record
Public Page [sys_public]	InstanceInfo
Scripted Web Service [sys_web_service]	<ul style="list-style-type: none"> • InstanceInfo • GetMIDInfo • MIDAssignedPackages • MIDFieldForFileProvider • MIDFileSyncSnapshot • MIDServerCheck • MIDServerFileProvider

Eureka

- MID Server upgrades support an HTTPS connection over port 443.
- Provides a new SSH client with improved connectivity.
- Provides new reports for MID Server analytics.

Dublin

- Administrators can install a 64-bit MID Server on a 64-bit host system.
- Script File synchronization stores all MID Server scripts in the ServiceNow instance to simplify distribution and security. It is no longer necessary to manually unblock MID Server scripts on the host machine.
- Several new business rules ensure that changing a MID Server's name in the configuration parameter also changes the name in MID Server record. See Available Parameters.
- The first MID server to successfully connect with the ServiceNow instance automatically becomes the default MID Server.

References

- [1] <https://docs.servicenow.com/bundle/jakarta-it-operations-management/page/product/mid-server/reference/r-MIDServer.html>
- [2] <http://www.gnu.org/s/libc/>
- [3] https://hi.service-now.com/kb_view.do?sysparm_article=KB0547597

Requirements



Note: This article applies to Fuji and earlier releases. For more current information, see *MID Server*^[1] at <http://docs.servicenow.com>. **The ServiceNow Wiki is no longer being updated. Visit <http://docs.servicenow.com> for the latest product documentation.**

Overview

The ServiceNow MID Server is used for enterprise application and service management, Orchestration, and Discovery. The requirements in this page are specifically for the use of MID Servers with the ServiceNow Discovery and Orchestration products.

System Requirements

ServiceNow has tested the MID Server in the following environments:

- Windows Server 2003, 2008, and 2012. All Windows Server 2008 and 2012 editions are supported. Virtual machines and 64-bit systems are supported.
- Linux: Virtual machines and 64-bit systems are supported. On 64-bit Linux systems, you must install the 32-bit GNU C library^[2] (*glibc*). The installation command for CentOS is: `yum install glibc.i686`

The minimum suggested configuration is:

- 4GB of available RAM per MID Server
- 2+GHZ CPU (Multi-core preferred)
- 500MB of disk space per MID Server
- Can *ride-along* with other services (dependent on server utilization and resource availability)

Java Version Support

The MID Server installs with JRE version 1.8. If you upgrade with a MID Server using JRE 1.6, the system automatically upgrades that MID Server to use version 1.8. Both the 32 bit and 64 bit MID Server use JRE 1.8.

External Connectivity Requirements

The MidServer communicates securely on port 443 to the instance and requires *no* inbound connections. In some cases, it might be necessary to allow this communication through the firewall if the MID Server fails to register on the instance. To determine if the application or a network security restriction is to blame for connection failure, attempt to telnet to the instance on port 443 from the server that is hosting the MID Server application. If this connection fails, then the problem could be a web proxy (since 443 is a https connecton) or a Firewall rule preventing external TCP connections from that host. Contact network security personnel for the proxy information to add to the *config.xml* file, or request that the Firewall be configured to allow access using one of the following syntaxes:

- `<source IP> to <any>`
- `<source IP> to <ServiceNow> any established`
- `<source IP> to <instance_name.service-now.com> 443`

Additionally, ensure the MID server can connect to *install.service-now.com* to download and install updates.

Internal Requirements

The three methods used for discovering various devices on a network are SSH, WMI and SNMP. SSH is used for accessing UNIX-like machines. Discovery logs into a machine with SSH and runs commands within an encrypted session to gather system information. Orchestration logs in to UNIX and Linux machines using SSH to perform Workflow activities. WMI is used by Discovery for Windows based machines and is used for querying the remote WMI protocol on targets for gathering of Windows information. Orchestration uses **PowerShell** to run activities on Windows machines. And lastly, SNMP v1/v2c/v3 is used on various network devices (Routers, Switches, Printers) by Discovery and Orchestration. Detailed information is listed below about these methods.

SSH - UNIX

For UNIX-like machines, Discovery and Orchestration use **SSH protocol, version 2** ^[1] to access target machines. SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices. SSH communicates on port 22 within an encrypted datastream and requires a login to access the targets using two available methods of authentication: a user name and password combination and a user name and shared private key. Specify SSH authentication information and type in the **Credentials** module. If multiple credentials are entered, the platform tries one after the other until a successful connection is established or all are ultimately denied. To provide for application relationships a limited number of SUDO commands must be available to be run. Additional details to these requirements can be found in **UNIX/Linux commands requiring root privileges for Discovery and Orchestration**.

WMI - Windows

For Windows machines, Discovery uses the **Windows Management Instrumentation (WMI)** ^[2] interface to query devices. Due to Microsoft security restrictions for WMI, the MID Server application executing the WMI queries must **run as** a domain user with local (target) administrator privileges. When Discovery detects activity on port 135, it launches a WMI query. The response from the Windows device is sent over a Distributed Component Object Model (DCOM) port configured for WMI on Windows machines. This can be any **port** ^[3]. Ensure that the MID Server application host machine has access to the targets on all ports due to the unique nature of the WMI requirements.

Windows PowerShell

PowerShell ^[4] is built on the Windows .NET Framework and is designed to control and automate the administration of Windows machines and applications. Orchestration uses PowerShell to run **Workflow activities** on Windows machines. PowerShell must be installed on any MID Server that executes these activities. MID Servers using PowerShell must be installed on a supported Windows operating system. ServiceNow supports PowerShell 2.0 and 3.0. Orchestration activities for PowerShell require a **credentials Type** of **Windows**.

SNMP - Network

For network devices, Discovery uses a SNMP scan ^[5] to get device specific MIBs and OIDs. SNMP is a common protocol used on most routers, switches, printers, load balancers and various other network enabled devices. Use a "community string" (password) for authentication when scanning a device via SNMP. Many devices have an out-of-box community string of **public** which Discovery (by default) uses when querying a target. Define additional community strings in the **Credentials** module which are tried in succession, along with **public**, until a successful query returns. In addition to the credentials, the platform also requires the ability to make **port 161** SNMP requests from the MID Server to the target. If Access Control Lists (ACLs) are in place to control the IP addresses that can

make these queries, ensure that the IP address of the MID Server is in the ACL. ServiceNow Discovery supports SNMP versions 1 and 2c ^[6].

The out-of-box Orchestration activity SNMP Query returns the OID of a device and requires SNMP **credentials**.

WBEM

Web-Based Enterprise Management (WBEM ^[7]) defines a particular implementation of the **Common Information Model (CIM** ^[8]), including protocols for discovering and accessing each CIM implementation. WBEM requires either of two ports, 5989 or 5988 and uses the HTTP transport protocol. WBEM supports SSL encryption and uses CIM user name/password credentials. ServiceNow Discovery launches a **WBEM port probe** to detect activity on the target ports and to append gathered data to a classification probe that explores CIM Servers.

References

- [1] http://en.wikipedia.org/wiki/Secure_Shell
- [2] http://en.wikipedia.org/wiki/Windows_Management_Instrumentation
- [3] <http://support.microsoft.com/kb/832017>
- [4] <http://support.microsoft.com/kb/968929>
- [5] <http://en.wikipedia.org/wiki/SNMP>
- [6] http://www.paessler.com/manuals/prtg_traffic_grapher/snmpversion12cand3
- [7] http://en.wikipedia.org/wiki/Web-Based_Enterprise_Management
- [8] [http://en.wikipedia.org/wiki/Common_Information_Model_\(computing\)](http://en.wikipedia.org/wiki/Common_Information_Model_(computing))

Installation



Note: This article applies to Fuji and earlier releases. For more current information, see *MID Server Installation* ^[1] at <http://docs.servicenow.com> **The ServiceNow Wiki is no longer being updated. Visit <http://docs.servicenow.com> for the latest product documentation.**

Overview

The Management, Instrumentation, and Discovery (MID) Server is a Java server that facilitates communication and movement of data between the ServiceNow platform and external applications, data sources, and services.

Video Tutorials

How to Set Up a MID Server	How to Set Up Multiple MID Servers on the Same Host Computer
--	--

Satisfying Connection Prerequisites

You must install a MID Server on a local network resource and configure it to communicate with the machines it will probe. The local network resource must have these network privileges:

- **Firewall access:** Configure any firewalls between the MID Server and the target devices to allow a connection. If your network uses a DMZ ^[2], and if your network security protocols limit port access from within the network to the DMZ, you might have to deploy a MID Server to a machine within the DMZ to probe the devices there.
 - **Network access:** Configure target devices to allow the MID Server probe to connect. If network security prevents you from configuring new machines that can connect to the targets, install the MID Server on an existing machine
-

with connection privileges.

- **Network account:** Install the MID Server with the proper account, either local or domain administrator.

Additionally, for the MID Server to access your ServiceNow instance, satisfy these prerequisites:

1. Configure the network to allow MID Server network connectivity to the ServiceNow instance over TCP port 443.
2. Configure basic authentication for SOAP communications with the ServiceNow instance.
3. Navigate to **System Web Services > Scripted Web Services** and confirm that the following web services are active:
 - GetMIDInfo
 - InstanceInfo
 - MIDAssignedPackages
 - MIDFieldForFileProvider
 - MIDFileSyncSnapshot
 - MIDServerCheck
 - MIDServerFileProvider
4. Navigate to **sys_public.list** and verify that the **InstanceInfo** public page is active to allow the MID Server to validate its version.

Setting up MID Server User and Role

The MID Server connects to a ServiceNow instance by using the SOAP web service. To allow authentication with the ServiceNow instance, create a separate user account for each MID Server or share the same account across multiple MID Servers. Each MID Server account must use the `mid_server` role to access protected tables.

To create a MID Server user account on the instance:

1. From the ServiceNow instance, navigate to **User Administration > Users**.
2. Click **New**.
3. Fill in the following:
 - **User ID:** The same user ID that will be specified in the `mid.instance.username` parameter of `config.xml`.
 - **Password:** - The same password that will be specified in the `mid.instance.password` parameter of `config.xml`.
 - **First name:** The user's first name.
 - **Last name:** The user's last name.
4. Right-click the header and select **Save**.
5. Under the **Roles** related list, click **Edit**.
6. Move **mid_server** from the Collection list to the Roles List.
7. Click **Save**.

Verifying the MID Server Account Access

You can confirm that the MID Server account was created successfully and the account has connectivity to the ServiceNow instance.



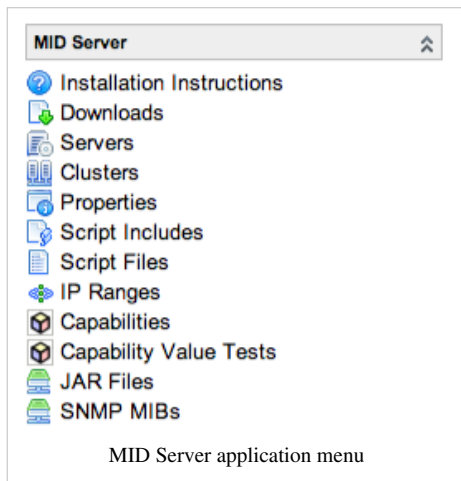
Note: Use a supported browser on the MID Server host to validate connectivity.

1. On the MID Server host, open a supported web browser.

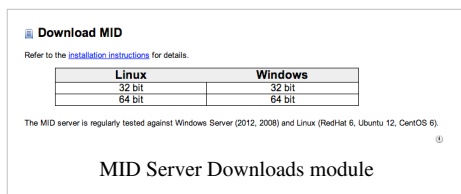
2. Navigate to the ServiceNow instance.
3. If the account is already logged into the instance, log out.
4. Use the previously created MID Server user credentials and sign in.

Downloading MID Server Files

Enabling Discovery, Orchestration, or any integration that requires the use of the MID Server, automatically activates the MID Server plugin. After activation, the MID Server application menu appears in the application navigator.



To download and install a MID Server, navigate to **Mid Server > Downloads** on your instance. Select and download the MID Server for the appropriate operating system. If the download does not begin immediately, try the download at a later time as the system may be busy.



Installing a MID Server on Linux

1. If you are using a 64-bit operating system with a version of ServiceNow prior to Dublin, you can install a 32-bit MID Server on a 64-bit Linux operating system by installing 32-bit libraries. Run the command for your Linux operating system version:

- **Ubuntu:** `sudo apt-get install ia32-libs ia32-libs-multiarch libgphoto2-2`
- **Red Hat:** `sudo yum -y install glibc.i686`

2. Create the installation directory by running:

```
mkdir -p /servicenow/<mid server name>
```

3. Extract the downloaded MID Server archive file, `mid.<os>.zip` into the `/servicenow/<mid server name>` directory.

The resulting directory structure is `/servicenow/<mid server name>/agent`.

4. Change to the `/servicenow/<mid server name>/agent` directory, and edit the `config.xml` file as follows:

- Find the `<parameter name="url" value=" UNIQ-nowiki-0-08e6ca633a6b9973-QINU //YOUR_INSTANCE.service-now.com"/>` element and change the value to the URL of your instance.
- Enter the MID user credentials in the `mid.instance.username` and `mid.instance.password` parameters. By default, the MID Server, uses basic authentication for SOAP messages. The password value is also encrypted authentication.
- Find the `<parameter name="name" value="YOUR_MIDSERVER_NAME_GOES_HERE"/>` element and change the value for the MID Server name.
- (Optional) Enter connection information for the proxy server. Remove the appropriate comment tags from the proxy configuration information. For example, you can configure the `mid.proxy.use_proxy`,

`mid.proxy.host`, `mid.proxy.port`, `mid.proxy.username`, and `mid.proxy.password`.

5. Execute the *start.sh* shell script.
6. Log in to the ServiceNow instance identified in the *config.xml* file.
7. Navigate to **MID Server > Servers**. Alternatively, if Discovery is installed, navigate to **Discovery > MID Servers**.
8. Verify that all MID Servers connected to this instance are listed.

Uninstalling

A MID Server running on Linux operates as a single process. You can end this process to accommodate such tasks as redeploying the MID Server to another host machine or changing the unique name of a MID Server when deploying multiple MID Servers.

1. Stop the MID Server process by executing the *stop.sh* shell script.
2. Verify that the MID Server is running by executing the *bin/mid.sh status* shell script.
3. After the MID Server stops, delete the files in the *agent* directory.

Installing a MID Server on Windows

Use the following procedures to install one or more MID Servers on a single machine.

1. Log in to the host machine where you want to install the MID Server.
2. Create a directory for the MID Server on the top level of the drive, with a distinctive name, such as *ServiceNow\MID Server1*.
3. Move the MID Server archive file into the new directory.
4. Right-click the archive and select **Extract All**.
5. Navigate to the *\agent* directory that was created when the file was extracted.
6. Edit the *config.xml* file with a text editor such as WordPad:
 - Find the `<parameter name="url" value=" UNIQ-nowiki-1-08e6ca633a6b9973-QINU //YOUR_INSTANCE.service-now.com"/>` element and change the value to the URL of your instance.
 - Enter the MID user credentials in the `mid.instance.username` and `mid.instance.password` parameters. By default, the MID Server, uses basic authentication for SOAP messages. The password value is also encrypted authentication.
 - Find the `<parameter name="name" value="YOUR_MIDSERVER_NAME_GOES_HERE"/>` element and change the value to define the name of your MID Server.
 - (Optional) Enter connection information for the proxy server. Remove the appropriate comment tags from the proxy configuration information. For example, you can configure the `mid.proxy.use_proxy`, `mid.proxy.host`, `mid.proxy.port`, `mid.proxy.username`, and `mid.proxy.password`.

NOTE: If this MID Server is installed on a system that contains other MID Servers, edit the *wrapper.conf* file as described in the procedure for installing multiple MID Servers.

Installing the MID Server as a Windows Service

To run a MID Server as a Windows service:

1. Click the **Start** button.
2. In the search box, type **command prompt** or **cmd.exe**.
3. In the results list, right-click **Command Prompt** or **cmd.exe**, and then click **Run as administrator**.

This enables the MID Server to be installed with administrative rights under any Windows User Account Control (UAC) setting.

4. In the command prompt, navigate to `\agent` in the directory you created for the MID Server files. For example, the path might be `C:\ServiceNow\MID Server\agent`.
5. Run `start.bat`.

Configuring MID Server Service Credentials

By default, the MID Server service runs as a local system account. You can perform these steps to configure the service to run as a specific user or domain account.

1. Open the Windows Services console.
2. Double-click the **ServiceNow <MID Server name>** service for each MID Server.
3. To verify that the MID Server service name is correct, review the properties to ensure that the MID server service values match the values from the `wrapper-override.conf` file. The **Service name** value should match the **wrapper.name** value and the **Display name** value should match the **wrapper.displayname** value.
4. Select the **Log On** tab, and then do one of the following:
 - Select the **Local System Account** to assign the Windows system account. This account has account privileges to modify files in MID server agent folder.
 - Select **This account** and assign a local or domain admin account credentials. Use Windows Explorer to grant write permissions to the MID Server agent folder.
5. In the General tab, set **Startup type** to **Automatic**.
6. Click **OK**.
7. Restart the **ServiceNow <MID Server name>** service, and make sure that `ServiceNow\<MID Server name>\agent\logs\agent0.log` does not have error messages.
8. On the instance this MID Server is connected to, navigate to **MID Server > Servers**. Alternatively, if Discovery is installed, navigate to **Discovery > MID Servers**.
9. Verify that all MID Servers connected to this instance are listed.

Uninstalling

The MID Server runs as a standalone service. It can be removed easily to accommodate such tasks as redeploying the MID Server to another host machine or changing the unique name of a MID Server when deploying multiple MID Servers.

1. Stop the running MID Server service.
2. Open a command window (**Start > Run > cmd**).
3. Do one of the following:
 - From the Dublin versions and newer, navigate to the `\agent\bin` directory in the MID Server installation directory and double-click the `UninstallMID-NT.bat` file.
 - For versions prior to Calgary, navigate to the `\agent\bin` directory in the MID Server installation directory and double-click the `uninstall.bat` file.

Installing Multiple MID Servers on a Single System

You can install multiple MID Servers on a single host or on a virtual machine using either Linux or Windows. Installing multiple MID Servers may involve other setup steps depending on your network configuration. See *Deploying Multiple MID Servers* for other considerations. For instances using a version prior to Calgary, see the previous version information.

1. Log in to the host system or virtual machine where you want to install multiple MID Servers.
2. Create a directory for each MID Server on the top level of the drive.

Make sure you create a unique and descriptive name for each MID Server, such as *MIDServer_SMS_Int* or *MIDServer_Disc1*.

3. Extract the downloaded MID Server archive file into each MID Server directory.

When this is complete, there should be the a directory path that resembles the following for each MID Server:

`\ServiceNow\<MID Server name>\agent.`

4. Using a text editor such as WordPad, edit the *config.xml* file in each MID Server *\agent* directory, as follows:

- Find the `<parameter name="url" value=" UNIQ-nowiki-2-08e6ca633a6b9973-QINU //YOUR_INSTANCE.service-now.com" />` element and change the value to define the name of your MID Server.
- If basic authentication is enabled, as it is by default behavior, enter the user credentials in the `mid.instance.username` and `mid.instance.password` parameters.
- Find the `<parameter name="name" value="YOUR_MIDSERVER_NAME_GOES_HERE" />` element and change the value to define the name of your MID Server.
- Enter connection information for any proxy server used and remove the comment tags from the proxy configuration information.

5. For each Windows MID Server, edit the *\agent\conf\wrapper-override.conf* file with a text editor such as WordPad. Use the *wrapper-override.conf* configuration file to enter all configuration information. Do not edit the *wrapper.conf* file, which contains the default configuration for the MID Server. Any future ServiceNow upgrades overwrite the contents of the *wrapper.conf* file, but do not modify the *wrapper-override.conf* file.

- **wrapper.name** ^[3]: [Required] This name identifies the MID Server process, maps to the **Service name** and must be unique. The default value is **snc_mid**.
- **wrapper.displayname** ^[4]: [Required for Windows] This value maps to the **Display name** in the Windows Services console. For example, you might enter **ServiceNow DevMID01**. The default value is **ServiceNow MID Server**.
- **wrapper.java.command** ^[5]: [Optional] This property defines the path to the java bin directory, either relative to the agent directory or absolute. The default value is *jre/bin/java*.
- **wrapper.java.initmemory** ^[6]: [Optional] This property defines the initial Java heap size ^[7] in MB. The default value is **10**.
- **wrapper.java.maxmemory** ^[8]: [Optional] This value defines the maximum Java heap size in MB. The default is **512**.

Note: These values **cannot** be edited while the MID Server is running.

6. Confirm that the MID Server is running.
7. (Optional) Configure MID Server clustering for load balancing or failover as necessary.

Versions Prior to the Calgary Release

MID Servers in versions prior to Calgary

- Log in to the host machine or virtual machine where you want to install multiple MID Servers.
- Create a directory for each MID Server on the top level of the drive.

Make sure you create a unique and descriptive name for each MID Server, such as *MIDServer_SMS_Int* or *MIDServer_Disc1*.

- Extract the downloaded MID Server zip file into each MID Server directory.

When this is complete, you should have the a directory that resembles the following for each MID Server:

`\ServiceNow\<MID Server name>\agent.`

- Using a text editor such as WordPad, edit the *config.xml* file in each MID Server *agent* directory, as follows:

- Find the element `<parameter name="url" value="UNIQ-nowiki-3-08e6ca633a6b9973-QINU //YOUR_INSTANCE.service-now.com" />` and change the value to the URL of your instance.
- For basic authentication, which is the default, enter the MID user credentials in the `mid.instance.username` and `mid.instance.password` parameters. Set up additional authentication for SOAP messages.
- For encrypted authentication, enter the MID user credentials in the `mid.instance.username` and `mid.instance.password` parameters.
- Find the element `<parameter name="name" value="YOUR_MIDSERVER_NAME_GOES_HERE" />` and change the value to define the name of your MID Server.
- Enter connection information for any proxy server used. Be sure to remove the comment tags from the proxy configuration information.

- Edit the *wrapper.conf* file for each MID Server with a text editor such as WordPad. By default, this file is located here:

`\ServiceNow\<MID Server name>\agent\conf`

- **wrapper.console.title=<MID Server name>:** This is the title to use when running the MID Server as a console.
- **wrapper.ntservice.name=<MID Server name>:** This is the internal Windows name for the service and is not displayed. This name must be unique. For example, example: **snc_agent2**.
- **wrapper.ntservice.displayname=<MID Server name>:** This is the name that is displayed to the user in the Windows Services console. For example, you might enter **ServiceNow MID Server1**.
- **wrapper.ntservice.description=<New Custom Description>:** This is the optional long description of the service that appears in the Services console.

NOTE: These values **cannot** be edited in this file after you create the service. Make sure you name and describe the services correctly before continuing to the next step.

- Install the MID Server as a Windows service:

- a. For Windows XP, Windows 2000 Server, or Windows Server 2003:

1. Open the `\agent` folder in the directory you created for the MID Server installation files. For example, the path might be `C:\ServiceNow\MID Server\agent`.
2. Double-click the *start.bat* file to install the Windows service.

- b. For Vista, Windows 2008 Server, or Windows 7:

1. Click the **Start** button.
2. In the search box, enter **command prompt** or **cmd.exe**.

3. In the results list, right-click **Command Prompt** or **cmd.exe**, and then click **Run as administrator**.

This enables the MID Server to be installed with administrative rights under any Windows User Account Control (UAC) setting.

4. In the command prompt, navigate to *agent* in the directory you created for the MID Server files. For example, the path might be *C:\ServiceNow\MID Server\agent*.

5. Run *start.bat*.

- Edit each MID Server's credentials.
 - a. Open the Windows Services console.
 - b. Double-click the **ServiceNow <MID Server name>** service for each MID Server.
 - c. In the properties dialog box, select the Log On tab.
 - d. Set **Log on as** privileges with Domain User or Local Admin credentials.
 - e. In the General tab, set **Startup type** to **Automatic**.
 - f. Click **OK**.
- Restart each ServiceNow MID Server service and make sure that *\ServiceNow\<MID Server name>\agent\logs\agent0.log* does not have error messages.
- In each instance these MID Servers are connected to, navigate to **MID Server > Servers**. If Discovery is installed, navigate to **Discovery > MID Servers**.

All MID Servers connected to this instance are listed.

Confirming Connectivity

Use the following procedures to verify that each MID Server service instance has started properly with network connectivity.

1. Verify that the MID Server service is running:
 - **Windows:** In the Windows Services console, locate the **ServiceNow <MID Server name>** and confirm that each MID Server has the **Started Status**.
 - **Linux:** Ensure that the *agent0.log.0.lck* file appears in the */servicenow/<mid server name>/agent* folder.
2. After each ServiceNow MID Server restart, open the *agent0.log.0* file and address all error messages.
3. Confirm network connectivity by pinging the instance URL, executing a telnet to instance URL at port 443, and/or performing a traceroute to the instance URL.
4. From the ServiceNow instance, navigate to **MID Server > Servers**.
5. Review and verify that all MID Servers that are connected to the ServiceNow instance are listed.
6. Verify that the **Status** is **Up** for the MID Servers.

Upgrading and Testing

The MID Server is configured to check with the ServiceNow instance hourly to determine whether it needs to upgrade. This configurable behavior allows the MID Server to upgrade automatically when the instance upgrades. The system that hosts the MID Server must be able to access one of these URLs to automatically upgrade (starting with the Eureka release):

- **HTTPS:** https://install.service-now.com on the default HTTPS port (443)
- **HTTP:** http://install.service-now.com on the default HTTP port (80)

The MID Server automatically tests connectivity through a public scripted web service.



Note: In versions prior to Eureka, the MID Server upgrade URL was only available on the default HTTP port (80).

Upgrade Error Messages

The MID Server can display the following upgrade error messages.

Message	Description
Unable to refresh packages	The MID Server displays this as a generic error when the error is not handled by a defined error message.
Failed to query instance for MID Server buildstamp	Instance is offline or there is a major version mismatch between the MID Server and the instance.
Not a valid package buildstamp	InstanceInfo returned an assigned buildstamp that was not in the correct format, such as a version mismatch.

Using Basic Authentication

You can enforce basic authentication on each request. Basic authentication requires each SOAP request to contain an Authorization header as specified in the Basic Authentication ^[9] protocol.

To set basic authentication for SOAP messages:

1. Navigate to **System Properties > Web Services**.
2. Select the check box for **Require basic authorization for incoming SOAP requests**.
3. Click **Save**.

Supplying basic authentication information, regardless of whether it is required, has an added advantage. The web service invocation creates or updates data using the supplied credentials. As an example, when you create an incident record, the journal fields have the user id of the basic authenticated user instead of the default Guest user. This behavior allows you to identify data added by a specific MID Server.

To provide basic authentication credentials for a MID Server, navigate to *C:\Program Files\ServiceNow\<MID Server name>\agent* and edit the *config.xml* file, as follows:

- Find the element `<parameter name="mid.instance.username" value="" />` and enter your instance's administrator user name as the value. For example, you might enter `<parameter name="mid.instance.username" value="admin"/>`.
- Find the element `<parameter name="mid.instance.password" value="" />` and enter the configured password for this instance as the value. For example, you might enter `<parameter name="mid.instance.password" value="abc123"/>`.



Note: The setting for enforcing strict security controls how ServiceNow uses the credentials you provide for the MID Server. When the setting is enabled, you must provide a user ID with access to the tables the MID Server is trying to access. When the setting is disabled, any valid user ID allows the MID Server to access to all tables.



Note: The MID Server is not able to communicate through a proxy server if the proxy server supports only NTLM authentication. You can use basic authentication with a proxy server or create an exception for the MID server host.

Monitoring Your MID Server

Use the following procedures to monitor each Windows or Linux MID server:

1. For **Windows**, navigate to the Windows Services console, locate the service name that matches the name that appears from the *wrapper-override.conf* file. If the MID Server process is the only Java process running on the host, monitor the memory used by *java.exe* and alert on *less* than the maximum configured memory defined in *~\agent\conf\wrapper-override.conf*.
2. Ensure that the *agent0.log.0.lck* file appears in the *~\agent\logs* folder to confirm that the MID Server running and logging system activity in the *agent0.log.0* file.
3. Review the following logs for warning, critical, and severe errors:
 - *~\agent\logs\agent0.log.0*
 - *~\agent\logs\wrapper.txt*
4. Confirm network connectivity.
5. From the MID Server instance, navigate to the **MID Servers** page, and review the status of the MID Server. For additional information, click a **Name**.
6. Use Windows or Linux tools to monitor:
 - CPU
 - Memory
 - Disk utilization
 - Event logs
 - syslog
7. Set up Email and SMS notifications to alert you when issues occur with MID servers. The MID Server Down Notification is enabled by default.

References

- [1] https://docs.servicenow.com/bundle/jakarta-it-operations-management/page/product/mid-server/concept/c_MIDServerInstallation.html
- [2] [http://en.wikipedia.org/wiki/DMZ_\(computing\)](http://en.wikipedia.org/wiki/DMZ_(computing))
- [3] <http://wrapper.tanukisoftware.com/doc/english/prop-name.html>
- [4] <http://wrapper.tanukisoftware.com/doc/english/prop-displayname.html>
- [5] <http://wrapper.tanukisoftware.com/doc/english/prop-java-command.html>
- [6] <http://wrapper.tanukisoftware.com/doc/english/prop-java-initmemory.html>
- [7] http://publib.boulder.ibm.com/infocenter/javasdk/tools/index.jsp?topic=%2Fcom.ibm.java.doc.igaa%2F_1vg00014884d287-11c3fb28dae-7ff6_1001.html
- [8] <http://wrapper.tanukisoftware.com/doc/english/prop-java-maxmemory.html>
- [9] <http://www.w3.org/Protocols/HTTP/1.0/draft-ietf-http-spec.html#BasicAA>

Configuration



Note: This article applies to Fuji and earlier releases. For more current information, see *MID Server Configuration*^[1] at <http://docs.servicenow.com> **The ServiceNow Wiki is no longer being updated. Visit <http://docs.servicenow.com> for the latest product documentation.**

Overview

Administrators must configure a MID Server to ensure that it has access to sufficient system resources, probes the proper data sources, and communicates with the instance as expected. You must complete all the steps in MID Server Installation before attempting any of the configuration steps explained here.

You must restart a MID Server after any configuration change for the changes to take effect.



Note: Using special characters in an XML configuration file requires you to encode them.

Available MID Server Setting Types

You can configure the following setting types on a MID Server. The setting type determines what components are affected by the MID Server setting. Choose a MID Server setting type that matches the scope you want the setting to affect.

Type of setting	Components affected	Overrides
MID Server Property	Either: <ul style="list-style-type: none">The behavior of all MID ServersThe behavior of a particular MID Server	MID Server properties override MID Server parameters
MID Server parameter	The behavior of a particular MID Server	None

Setting MID Server Properties

Use a MID Server property to control either the behavior of all MID Servers or a particular MID Server. Configure MID Server properties in the MID Server plugin. Do not configure MID Server properties in the **glide.properties** file that is located in the *properties* folder of the agent. The **glide.properties** file gets overwritten during the upgrade process.

1. Navigate to **MID Server > Properties**.
2. Click **New**.
3. Fill in the fields, as appropriate (see table).

Field	Description
Name	Enter the property name. See the Name(s) column in Required Parameters or Optional Configuration parameters for a list of parameter and property names.
Value	Enter the value you want the property to have.
MID Server	Leave this field blank to set a MID Server property that affects all MID Servers. To set a MID Server property for a particular MID Server, select the MID Server.

Setting MID Server Parameters

Use a MID Server parameter to control the behavior of a particular MID Server. Set MID Server configuration parameters in either of the following places:

- From the **Configuration Parameters** related list in the MID Server record.
- From the *config.xml* file in the *\agent* directory of your MID Server installation.



Note: *Changes to parameters only take effect when the MID Server is started (or restarted).*

Setting Parameters from the ServiceNow Instance

You can view and manage MID Server configuration from the ServiceNow instance.

1. Navigate to the list of MID Servers using one of the following paths:
 - **MID Server > Servers**
 - **Discovery > MID Servers**
 - **Orchestration > MID Servers** (starting with Dublin)
 - **Runbook Automation > MID Servers** (versions prior to Dublin)
2. From the list of MID Servers, select a MID Server to configure.

The **Configuration Parameters** related list shows all the parameters currently in the MID Server's configuration file. If there are any passwords, they are displayed in asterisks for security reasons.

Configuration Parameters (9) | IP Ranges | Capabilities | Logs (15) | Threads (12) | Properties

Configuration Parameters

New

Go to

Param name

1 to 9 of 9

MID Server = Surfpilot-MID1

Param name	Value
<input type="checkbox"/> url	http://10.0.4.176:8080/glide/
<input type="checkbox"/> mid.shazzam.chunk_size	10
<input type="checkbox"/> mid.shazzam.regulator.interval_ms	25
<input type="checkbox"/> mid.instance.password	*****
<input type="checkbox"/> threads.max	25
<input type="checkbox"/> mid.shazzam.regulator.packets_per_interval	1
<input type="checkbox"/> mid_sys_id	99c9f8d6a9fee3d2787bf0f01e6dcc6e
<input type="checkbox"/> mid.instance.username	admin
<input type="checkbox"/> name	Surfpilot-MID1

Actions on selected rows...

1 to 9 of 9

3. To add parameters, click **New**, and then complete the form.

After the form is submitted, the configuration file for that MID Server is modified to include the new parameter. Changes to existing parameters are reflected in the MID Server configuration file as well. Changes made to the MID Server configuration file do not take place immediately, but rather the next time the MID Server is restarted. The MID Server form has a related link for restarting the MID Server.



Note: ServiceNow prevents you from saving changes, such as modifying or deleting parameters, that would cause the MID Server to lose communications with the instance. For example, you cannot change the url parameter. Any changes to these protected properties must be made directly in the config.xml file for that MID Server.

Setting Parameters from the config.xml File

MID Server configuration is controlled by an XML file called *config.xml*. This file is located in the *\agent* directory, immediately under the directory where the MID Server is installed. Edit this file directly to make any configuration changes to protected parameters. Many configuration changes, such as those that do not disrupt communication between the MID Server and the ServiceNow instance, may also be made from the instance.

The structure of the *config.xml* file is simply an outer parameters tag and a series of inner parameter tags. Each parameter tag has name and value attributes.

- To change the value of a parameter, edit the value attribute.
- To add a parameter, add another parameter tag with its name and value.
- To delete a parameter, delete the entire parameter tag.

The order of the parameters within the file is not important. Notice the green comment sections in the sample. Use these elements to add useful comments to the configuration file.



Note: When configuring the MID Server for use with a proxy server, be sure to remove the comment tags around the proxy sections that you configure.

```
--<parameters>
  <!-- MID Server Configuration -->
  <parameter name="url" value="https://example.service-now.com"/>
  <parameter name="refresh_rate" value="65"/>
  <parameter name="name" value="Super Duper MID Server #1"/>
  <parameter name="mid_sys_id" value=""/>
  <!-- MID Server Threads -->
  <parameter name="threads.max" value="25"/>
  <!-- MID Server proxy configuration -->
  <parameter name="mid.proxy.host" value=""/>
  <parameter name="mid.proxy.port" value=""/>
  <parameter name="mid.proxy.username" value=""/>
  <parameter name="mid.proxy.password" value=""/>
--</--

  MID Server to instance configuration options

  mid.instance.use_proxy
    - when talking to instance, should we use the proxy config?

  mid.instance.username
  mid.instance.password
    - supply username and password if instance has basic authentication enabled

  ==>
  <parameter name="mid.instance.use_proxy" value="true"/>
  <parameter name="mid.instance.username" value=""/>
  <parameter name="mid.instance.password" value=""/>
--</--

  MID Server upgrade options

  mid.upgrade.use_proxy
    - when talking to upgrade server, should we use the proxy config?

  mid.upgrade.branch
    - define a branch our MID Server is pinned to

  -->
  <parameter name="mid.upgrade.use_proxy" value="true"/>
  <parameter name="mid.upgrade.branch" value=""/>
</parameters>
```



Note: The sample file here is from Firefox. Conventional text editors, such as Notepad, Wordpad, or TextEdit, do not display colors and variable fonts.

Required Configuration

All MID Servers require the following configuration settings.

Setting up MID Server User Credentials

Each MID Server must have a set of ServiceNow user credentials with the mid_server role. Any change to user credentials or roles used by the MID Server user requires a restart of the MID Server service.

Required Parameters

The following parameters are required for all MID Servers.



Note: Using special characters in an XML configuration file requires you to encode them.

Label	Names	Description
Instance URL	url	<p>Specifies the URL to the associated ServiceNow instance. Normally the URL is similar to https://instance.service-now.com, where you replace <i>instance</i> with the instance name. If you host your own ServiceNow instance, use the URL set by your organization.</p> <ul style="list-style-type: none">• Type: string• Default value: none
MID Server ID	mid_sys_id	<p>Records the MID Server record's unique identifier. This parameter should be empty when you initially configure a MID Server. Do not change the value.</p> <ul style="list-style-type: none">• Type: string• Default value: automatically set (GUID)
MID Server name	name	<p>Use this parameter to supply a name that is meaningful for you. If you do not supply this parameter, the MID Server uses the default value. A set of business rules synchronizes the name in the configuration file with the name in the MID Server record (starting with the Dublin release). The business rules ensure that changing the name in one location also changes the name in the other location.</p> <ul style="list-style-type: none">• Type: string• Default value: YOUR_MIDSERVER_NAME_GOES_HERE
Instance user name	mid.instance.username or glide.glidesoap.username	<p>If the ServiceNow instance has authentication enabled, as it is by default, set this parameter to define the user name the MID Server should use to log in to the instance. This user should have the mid_server role on the ServiceNow instance in order to access necessary tables and fields.</p> <ul style="list-style-type: none">• Type: string• Default value: none
Instance password	mid.instance.password or glide.glidesoap.password	<p>If your ServiceNow instance has authentication enabled, as it is by default, set this parameter to define the password the MID Server should use to log in to the instance.</p> <ul style="list-style-type: none">• Type: string• Default value: none

Optional Configuration

The following configuration settings are optional. While a MID Server should start with the default settings, you may want to change the default values to improve performance or follow your organization's business practices.

Setting MID Server Memory Size

In the base ServiceNow system, the MID Server memory is set to 512MB, which can be configured in the `\agent\conf\wrapper.conf` file in the MID Server installation directory. This setting might not be appropriate for the way your organization uses the MID Server. If you want the MID Server to work harder, allocate more resources to it. Or perhaps the MID Server is located in a small branch office with very few devices, and runs in an environment where memory allocation is shared between a print server, mail server, or web proxy server. In this situation, the MID Server memory allocation might have to be reduced.

To edit the memory allocation:

1. Navigate to `\ServiceNow\<MID Server name>\agent\conf` and open the `wrapper-override.conf` file in a text editor.

For more information about this file, see [Installing Multiple MID Servers on a Single System](#).

2. Locate the following lines in the file:

```
# OPTIONAL: Maximum Java Heap Size (in MB)
# wrapper.java.maxmemory=512
```

3. Edit the memory allocation.
4. Remove the comment tag (#) from the memory allocation parameter.
5. Save the file.
6. Restart the MID Server service.

Setting MID Server Thread Use

By default, the MID Server uses a maximum of 25 threads. If the MID Server is running on a host containing many other programs that must compete for CPU time, fewer threads than the default of 25 might be necessary. You can set the MID Server to use as few as 5 threads without issues. If the MID Server needs more speed, and the host is powerful enough or lightly loaded with other programs, raise the thread setting. The thread limit depends on the hardware and the operating system of the host. You might have to experiment to find the optimal value for your situation. The following general observations may be useful:

- Most MID Server tasks require *file handles* to do their job.
 - **Windows:** On the Windows operating system, file handles are available in a fixed quantity. If you configure too many MID Server threads on a Windows host, the MID Server can consume all the file handles before approaching maximum CPU usage. This situation appears as an **Out of file handles** error in the MID Server log and indicates that the MID Server is trying to use too many threads.
 - **Unix and Linux:** UNIX and Linux hosts have a much different scheme for allocating file handles. Generally, you can increase MID Server thread use on these operating systems until the CPU of the host is overloaded. See your OS documentation for monitoring CPU usage.
- Each thread on the MID Server requires some memory. Exactly how much memory varies considerably from task to task and depends on the equipment being discovered. To increase the number of threads, you might have to increase the amount of memory that Java uses. If you configure insufficient memory, an **Out of memory** error appears in the MID Server log.

To edit the maximum number of threads allowed for the MID Server:

1. Open the `\agent\config.xml` file using any text editor.
2. Locate the following lines:

```
<!-- MID Server Threads -->
<parameter name="threads.max" value="25"/>
```

3. Edit the value. Keep in mind the cautions described above.
4. Save the record.
5. Restart the MID Server service.

Enabling Script File Synchronization for Windows Enhanced Security

Windows Internet Explorer enhanced security blocks downloaded files that it determines are potentially dangerous. Without script file synchronization, Internet Explorer blocks files downloaded for use by the MID Server, forcing ServiceNow administrators to unblock each file manually. File synchronization creates the files on the MID Server rather than downloading them, which does not trigger security blocking. Also, file synchronization between script records on the instance and the MID Server protects any customer updates in those records from being overwritten during a ServiceNow upgrade.

Script file synchronization is available starting with the Dublin release. If you are using an older version, see the previous version information.

How File Synchronization Works

Script files synchronized with the MID Server are stored on the ServiceNow instance in the MID Server Script File [ecc_agent_script_file] table (**MID Server > Script Files**). When the MID Server first connects to the instance, ServiceNow creates a directory called `\scripts` in the MID Server root. The instance then creates a parent directory in the path `\scripts\<parent name>` using definitions from the ecc_agent_script_file table. Finally, the instance creates the script files themselves inside the parent directory using the records from the ecc_agent_script_file table.

The record for the parent directory looks like this:

Name	Description	Active	Directory
Credentials.psm1	Manages credential testing to see if the...	true	false
LaunchProc.psm1	Launches a process and fetches the output...	true	false
PSScript.ps1	Main wrapper script for all PowerShell s...	true	false
WMIFetch.psm1	Collection of functions used to fetch da...	true	false
XMLUtil.psm1	Collection of methods for managing XML c...	true	false

The instance creates each script file in the parent directory on the MID Server using the record **Name** from the ecc_agent_script_file table as the file name and the **Script** field payload as the file contents. A script file record looks like this:

MID Server Script File

Name: Credentials.psm1

Description: Manages credential testing to see if there is proper access to a target system

Parent: PowerShell

Active: ☒

Directory: ☐

Script:

```
<#####>
# Turn user/password into a credential object for use in cmdlets that take a credential
#####>
function getCredential {
    param([string]$user, [string]$password)

    if ($password) {
        $passwordSecure = convertto-securestring -string $password -asplaintext -force;
    } else {
        # If no password was supplied, use an empty instance of SecureString
        $passwordSecure = new-object System.Security.SecureString;
    }

    $cred = new-object -typename System.Management.Automation.PSCredential -argumentlist "$user",$passwordSecure;

    return $cred;
}
```

Update Delete

Unblocking PowerShell Scripts Prior to the Dublin Release

Click the plus for previous version information

Enhanced security on the Windows operating systems can block PowerShell from working with Discovery and Orchestration. If PowerShell does not run with Discovery or Orchestration, *unblock* the MID Server archive:

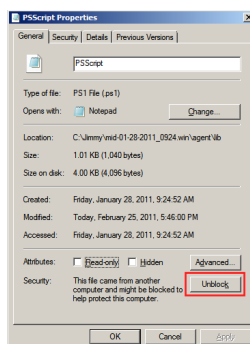
- **MID Server archive:** mid.<build date>.<operating system>.<system bit>.zip

If you do not unblock the archive, unblock each individual file:

- Credentials.psm1
- LaunchProc.psm1
- MSSqlAuth.ps1 (Removed in the Calgary release)
- MSSqlWinAuth.ps1 (Removed in the Calgary release)
- PSScript.ps1
- WMIFetch.psm1
- XmlUtil.psm1

Perform this procedure on *each* MID Server machine:

1. Navigate to the MID Server archive file.
2. Right-click the first file in the list and select **Properties** from the menu.
3. In the Properties dialog box, click **Unblock**.
4. Repeat the procedure for each of the remaining files, if necessary.



Adding SSL Certificates

You can configure the MID Server to connect over SSL by adding the following certificates to the cacerts keystore file:

- Signing Certificate Authority (CA) certificate
- MID Server certificate

To add a certificate to a MID Server:

1. Open a command prompt and navigate to the folder containing the JRE keytool ^[2]. For example:
`cd C:\Program Files (x86)\ServiceNow\<MidServer(s)>\agent\jre\bin`
2. Enter the following keytool command to import a certificate into the MID Server's cacerts keystore:
`keytool -import -alias <certificate alias> -file "<path to certificate>" -keystore "<path to MID Server(s)>\agent\jre\lib\security\cacerts"`

For example:

```
keytool -import -alias MyCA -file "C:\myca.cer" -keystore "C:\Program Files (x86)\ServiceNow\MIDserver\agent\jre\lib\security\cacerts"
```



Note: Keytool prompts for a certificate password. If the certificate is for a CA, keytool also asks whether to trust the certificate authority.

To add a certificate to an instance, see [Uploading a Certificate](#).

MID Server Properties

Use the following properties to control the behavior of all probes on a MID Server or all probes on all MID Servers. See [Setting MID Server Properties](#).

Label	Names	Description
Max length of a payload that a MID Server will return	mid.discovery.max_payload_size	<p>Specifies the maximum string length of Discovery probe results that the MID Server will send to the instance. The MID Server verifies the size of the Discovery probe results before sending them to the instance. If the Discovery probe results exceed the limit, the MID Server discards them and returns a warning message. This applies only to probes where the Used by Discovery field is true. Set the value to any negative number to disable the payload limit and allow Discovery payloads of any size to be sent to the instance. For example, -1. This parameter is available starting with the Eureka release.</p> <ul style="list-style-type: none">• Type: integer (bytes)• Default value: 5000000
Max length of an ECCQ payload XML that a MID Server will send to the instance	mid.eccq.max_payload_size	<p>Specifies the maximum string length of a payload that the MID Server will send to the instance. The MID Server verifies the size of the payload before sending it to the instance. If the payload size exceeds the limit, the MID Server saves a copy of the payload to the filesystem on the MID Server host, and returns an error message that contains the location of the file.</p> <ul style="list-style-type: none">• Type: integer (bytes)• Default value: 20000000

CIM Parameters

This parameters determine how a MID Server conducts CIM Discovery.

Label	Names	Description
Interval to wait between requests to the same CIMOM (ms)	mid.cim.request.interval	<p>Specifies the number of milliseconds to wait between requests to the same Common Information Model Object Manager (CIMOM). This parameter is available starting with the Eureka release.</p> <ul style="list-style-type: none"> • Type: integer (milliseconds) • Default value: 0
The maximum amount of simultaneous connections allowed per CIMOM	mid.cim.host.connection.limit	<p>Specifies the maximum number of simultaneous connections to each Common Information Model Object Manager (CIMOM). A value of zero disables simultaneous connections. This parameter is available starting with the Eureka release.</p> <ul style="list-style-type: none"> • Type: integer (number of connections) • Default value: 0

Connection Parameters

Label	Names	Description
The maximum amount of standard messages to queue in memory for processing	mid.max.messages	<p>Specifies the maximum number of messages to hold in memory for processing. The default value is computed from the <code>threads.max</code> parameter.</p> <ul style="list-style-type: none"> • Type: integer • Default value: <code>[10 * threads.max]</code>
Instance date format	instance.date.format	<p>Specifies the format the instance uses for dates and times. The primary impact of setting this parameter is to allow the MID Server to correctly refresh its start and stop times on the MID Server record in ServiceNow. The format of this date/time string is identical to that used by the Java SimpleDateFormat class, documented here ^[3] in the section titled <i>Date and Time Patterns</i>.</p> <ul style="list-style-type: none"> • Type: string (Date format) • Default value: <code>yyyy-MM-dd HH:mm:ss</code>
MID Server immediate response enable	glide.mid.fast.responses	<p>Instructs the MID Server to try sending messages to the instance as soon as they are ready. Normally the MID Server sends message to the ServiceNow instance <i>serially</i> (that is, one message at a time). Since many probes can be run in parallel, there can be multiple messages simultaneously transmitted to the instance. Setting this parameter to true may decrease the time between a probe's completion and its response arriving at the instance. However, the multiple simultaneous messages consume resources, decreasing the overall instance responsiveness. If there are communications problems, this parameter's value can also cause a <i>logjam</i> on the MID Server, as threads normally used for running probes may become consumed for sending messages. Generally, leave this parameter out of your configuration. Setting it to true is meaningful only under very special circumstances.</p> <ul style="list-style-type: none"> • Type: <code>true false</code> • Default value: <code>false</code>
MID Server JMX enable	mid.jmx.enabled	<p>Enables a JMX server on the MID Server, which exposes some management information to JMX consoles. Implementing JMX requires additional configuration of the Java runtime environment. Setting this parameter to true is only recommended for those with detailed knowledge of the Java security architecture and a specific need for JMX.</p> <ul style="list-style-type: none"> • Type: <code>true false</code> • Default value: <code>false</code>

MID Server max transmission queue size	glide.mid.max.sender.queue.size	<p>Places an upper limit on how large the queue is allowed to get. The MID Server starts deleting queued messages if this limit is exceeded. When the MID Server generates messages to the ServiceNow instance faster than it can send them, it queues them temporarily on the file system of the MID Server's host. This queue is normally quite small, and is completely emptied as soon as the MID Server processing slows for a short period. However, this queue can grow in size when there are communication problems between the MID Server and the instance, and especially if there is an integration running on the MID Server, .</p> <p>The parameter is of the form {number}{multiplier}, where {number} is any positive decimal number including non-integers, and the optional multiplier is any spelling of <i>bytes</i>, <i>kilobytes</i>, <i>megabytes</i>, <i>gigabytes</i>, or <i>terabytes</i> (only the first character is tested, and the test is case-insensitive). The default multiplier is bytes. White space is liberally tolerated. The following strings all represent valid parameters: "1000000000", "0.5m", "5 GB", "7.67gigas", "145.69392 meg", and "1.1 terra".</p> <ul style="list-style-type: none"> • Type: string • Default value: 0.5g
MID Server maximum number of probe threads	threads.max	<p>Controls the number of execution threads (simultaneous work) that probes may use. This parameter provides direct control over what CPU resources the MID Server consumes on the computer that hosts it. To decrease the MID Server's CPU consumption, lower the number of threads. To make the MID Server work faster, increase the number of threads. See Setting MID Server Thread Use.</p> <ul style="list-style-type: none"> • Type: integer (threads) • Default value: 25
MID Server poll time	mid.poll.time	<p>Sets the MID Server polling interval (in seconds).</p> <ul style="list-style-type: none"> • Type: integer (seconds) • Default value: 15

Credentials Parameters

Label	Names	Description
Credentials provider	mid.credentials.provider	<p>Specifies the Java class name of the credentials provider.</p> <ul style="list-style-type: none"> • Type: string • Default value: com.service_now.mid.creds.standard.StandardCredentialsProvider

Debug Parameters

Label	Names	Description
Debug logging enable	debug.logging	<p>Specifies whether to enable logging of MID Server events and messages (both sent and received). Normally this parameter is only used by developers, but it is occasionally useful when troubleshooting a problem. Be aware that setting this parameter to true causes intensive logging on the MID Server, potentially using considerable disk space.</p> <ul style="list-style-type: none"> • Type: true false • Default value: false
Debug mode enable	debug	<p>Specifies whether to enable debug logging on the MID Server. Normally this parameter is only used by developers, but it is occasionally useful when troubleshooting a problem. Be aware that setting this parameter to true causes intensive logging on the MID Server, potentially using considerable disk space.</p> <ul style="list-style-type: none"> • Type: true false • Default value: false

Enables debug logging for CIM / WBEM / SLP / SMI-S	mid.cim.debug	<p>Specifies whether to enable debug logging for CIM, WBEM, SLP, or SMI-S.</p> <ul style="list-style-type: none"> • Type: true false • Default value: false
Enable debug logging for ServiceNow SSH Client	mid.ssh.debug	<p>Enables SSH debug information in the log file. The parameter usage depends on whether the ServiceNow SSH client is enabled (starting with the Eureka release).</p> <p>When the ServiceNow SSH client is enabled, the parameter functions as follows:</p> <ul style="list-style-type: none"> • Type: string • Default value: false <p>The following string values are valid for the ServiceNow SSH client:</p> <ul style="list-style-type: none"> • true: Enables SSH debug information in the log file. • false: Disables SSH debug information in the log file. • <IP Addresses>: Specify which IP ranges to enable SSH debug information in the log file. You can enter IP addresses in the following formats: <ul style="list-style-type: none"> • An IP range defined by a slash and the number of bits in the subnetmask ^[4]. For example, the string <code>10.10.10.0/24</code> scans 24 bits of IP addresses from <code>10.10.10.0</code> to <code>10.10.10.254</code>. • An IP range defined by a dash. For example, the string <code>10.10.11.0-10.10.11.165</code> scans the IP addresses from <code>10.10.11.0</code> to <code>10.10.11.165</code>. • A comma-separated list of specific IP addresses. For example the string <code>10.10.11.200,10.10.11.235</code> scans the IP addresses <code>10.10.11.200</code> and <code>10.10.11.235</code>. • deferred: Logs SSH debug information in memory unless an error or warning occurs. If an error or warning occurs, the platform publishes the debug information to the log file. This ensures that only the part of the log file pertaining to the error or warning is recorded. If no error or warning is detected, the platform deletes the unused log data from memory when the session closes. Each session stores up to 1000 log messages. If the session exceeds 1000 log messages, the deferred log discards the oldest log message to make room for the newest log message. <p>When the ServiceNow SSH client is disabled, the parameter enables or disables SSH debug information in the log file:</p> <ul style="list-style-type: none"> • Type: true false • Default value: false

DNS Parameters

Label	Names	Description
DNS scanning regulator interval (ms)	mid.dns_scan.regulator.interval_ms	<p>Specifies the interval between DNS scans in milliseconds.</p> <ul style="list-style-type: none"> • Type: integer • Default value: 10
DNS scanning regulator packets per interval	mid.dns_scan.regulator.packets_per_interval	<p>Specifies the number of regulator packets per DNS scan.</p> <ul style="list-style-type: none"> • Type: integer • Default value: 1
DNS scanning default name servers	mid.dns_scan.default_name_servers	<p>Specifies the host names or IP addresses of the default name servers.</p> <ul style="list-style-type: none"> • Type: string • Default value: none
DNS scanning additional name servers	mid.dns_scan.additional_name_servers	<p>Specifies the host names or IP addresses of any additional name servers.</p> <ul style="list-style-type: none"> • Type: string • Default value: none

DNS scanning load balancing enable	mid.dns_scan.load_balancing_enable	Specifies whether to enable load balancing of name servers.
<ul style="list-style-type: none"> • Type: true false • Default value: false 		

ECC Queue Parameters

Label	Names	Description
The amount of time to look-behind on the ECCQ when querying for more work (s)	mid.eccq.monitor.window	Specifies the time period to look behind on the ECC Queue in seconds. The default value is 30 minutes. <ul style="list-style-type: none"> • Type: integer • Default value: 1800 seconds
MID Server ECC query interval	query_backoff	Allows the interval at which the MID Server queries the ECC Queue to lengthen if the MID Server is idle. By default, the MID Server queries the ECC Queue for work every 15 seconds. In a system that employs a large number of MID Servers, these queries can produce unnecessary traffic during periods of light MID Server activity. When the <code>query_backoff</code> parameter is set to true , the query interval slowly lengthens for an idle MID Server. Eventually, the interval slows to one query every four minutes and holds at that rate until the MID Server has a job to do. When the MID Server starts work again, the query interval for that MID Server immediately increases to once every 15 seconds and continues at that rate until the demand on the MID Server backs off again. <ul style="list-style-type: none"> • Type: true false • Default value: false

Logging Parameters

Label	Names	Description
Disable monitor checking	disable_monitors	Specifies whether to disable the MID Server from actively checking for monitors on the instance. <ul style="list-style-type: none"> • Type: true false • Default value: false
Query logging enable	mid.show.queries	Instructs the MID Server whether to log details about every query it makes to the ServiceNow instance. Typically this parameter is only used by developers, but it is occasionally useful when troubleshooting a problem. Be aware that setting this parameter to true causes intensive logging on the MID Server, potentially using considerable disk space. <ul style="list-style-type: none"> • Type: true false • Default value: false
Remote logging disable	disable.remote.logging	Prevents the MID Server from logging any information to the MID Server log on the ServiceNow instance. Relatively little information is logged on the instance in any case, but setting this parameter to true eliminates all logging to the instance. <ul style="list-style-type: none"> • Type: true false • Default value: false
Status sending disable	disable.status	Prevents the MID Server from sending a status report to the ServiceNow instance every 10 minutes. <ul style="list-style-type: none"> • Type: true false • Default value: false

Proxy Server Parameters

Use these parameters to configure how your MID Server communicates through a proxy server to access the ServiceNow instance.

Label	Names	Description
Instance proxy enable	<code>mid.instance.use_proxy</code> or <code>mid.proxy.use_proxy</code>	<p>If your MID Server must go through a web proxy to access the ServiceNow instance, set this parameter to true to instruct the MID Server to use the proxy. You must also set the proxy server's host and port, and perhaps the user name and password as well.</p> <ul style="list-style-type: none"> • Type: true false • Default value: false
Instance proxy host	<code>mid.proxy.host</code>	<p>If your MID Server must go through a web proxy to access the ServiceNow instance, set this parameter to define the proxy's host.</p> <ul style="list-style-type: none"> • Type: string • Default value: none
Instance proxy password	<code>mid.proxy.password</code>	<p>If your MID Server must go through a web proxy to access the ServiceNow instance, and your proxy requires a password, set this parameter to define that password.</p> <ul style="list-style-type: none"> • Type: string • Default value: none
Instance proxy port	<code>mid.proxy.port</code>	<p>If your MID Server must go through a web proxy to access the ServiceNow instance, set this parameter to define the proxy's port.</p> <ul style="list-style-type: none"> • Type: integer (0-65535) • Default value: 80
Instance proxy user name	<code>mid.proxy.username</code>	<p>If the MID Server must go through a web proxy to access the ServiceNow instance, and the proxy requires a user name, set this parameter to define that user name.</p> <ul style="list-style-type: none"> • Type: string • Default value: none

Shazzam Parameters

Label	Names	Description
Port probe packet interval	<code>mid.shazzam.regulator.interval_ms</code>	<p>Sets the interval, in milliseconds, in which Shazzam can launch packets. This parameter works with the <code>mid.shazzam.regulator.packets_per_interval</code> parameter to set the number of packets allowed in this interval. By default, Shazzam launches one packet each millisecond.</p> <ul style="list-style-type: none"> • Type: integer • Default value: 1
Port probe packets launched per regulator interval	<code>mid.shazzam.regulator.packets_per_interval</code>	<p>Sets the number of packets that Shazzam can launch in the configured time interval. This parameter works with the <code>mid.shazzam.regulator.interval_ms</code> parameter, which sets that interval. By default, Shazzam launches one packet each millisecond.</p> <ul style="list-style-type: none"> • Type: integer • Default value: 1
Shazzam chunk size	<code>mid.shazzam.chunk_size</code>	<p>Specifies the maximum number of IP addresses that Shazzam scans in parallel. This parameter primarily controls outbound port consumption.</p> <ul style="list-style-type: none"> • Type: integer • Default value: 100

SNMP Discovery Parameters

Label	Names	Description
Enable automatic inclusion of SNMP public community string	mid.snmp.enable_auto_public	Specifies whether to enable the SNMP public community string ^[5] . <ul style="list-style-type: none"> • Type: true false • Default value: true
Timeout to wait for a response for each OID request (ms)	mid.snmp.request.timeout	Specifies the timeout value for each SNMP OID ^[6] request. The default is 1.5 seconds. <ul style="list-style-type: none"> • Type: integer • Default value: 1500 milliseconds
Inactivity timeout for an established session - after the first response is received (ms)	mid.snmp.session.timeout	Specifies the timeout value for existing SNMP connections. The default is 0.5 seconds. <ul style="list-style-type: none"> • Type: integer • Default value: 500 milliseconds

SSH Discovery Parameters

Label	Names	Description
MID Server connection cache	mid.connection_cache	Specifies whether to cache connections. Set to false to disable connection caching. This parameter applies to SSH connections only. <ul style="list-style-type: none"> • Type: true false • Default value: true
Decide if the PATH environment variable should be set for SSH commands	mid.ssh.set_path	Specifies whether to set the PATH environment variable for SSH commands. <ul style="list-style-type: none"> • Type: true false • Default value: true
Process commands against localhost via SSH rather than console	mid.ssh.local	Specifies whether to execute commands for the MID Server host machine (localhost) via SSH rather than from a console. This allows long-running commands to execute properly. This parameter applies to the legacy SSH client only. <ul style="list-style-type: none"> • Type: true false • Default value: false
MID Server SSH connection per host	mid.ssh.connections_per_host	Controls the number of concurrent probes the MID Server can run against a given host. Lowering the number of concurrent connections can slow Discovery. <ul style="list-style-type: none"> • Type: integer • Default value: <ul style="list-style-type: none"> • 7 for the ServiceNow client • 3 for the legacy SSH client
Enable (or disable) sudo to preserve environment (-E) for SSH	mid.ssh.sudo_preserve_environment	Specifies whether to use sudo ^[7] to preserve the environment for SSH. <ul style="list-style-type: none"> • Type: true false • Default value: false

Set the PATH environment paths for SSH commands	mid.ssh.path_override	<p>Overrides the default paths set before executing a command. Enter one or more override paths delimited by a colon (:). The default path is <code>/usr/sbin: /usr/bin: /bin: /sbin</code>.</p> <p>The ServiceNow SSH client accepts the following prefixes in front of the <code>path_override</code> value.</p> <ul style="list-style-type: none"> • append: Appends the override path to the end of the host's path. This is the default behavior. • replace: Replaces the host path with the <code>path_override</code> value. • prepend: Appends the override path to the front of the host path. • Type: string (a colon-separated list of directories) • Default value: None
Enable ServiceNow SSH Client	mid.ssh.use_snc	<p>Enables the ServiceNow SSH client (SNCSSH), which is a ServiceNow implementation of an SSH client. SNCSSH is active by default on new instances starting with the Eureka release. Customers upgrading to Eureka or a later release can manually switch to the ServiceNow SSH client with this parameter. Enabling the ServiceNow SSH client disables the legacy SSH client. This parameter is available starting with the Eureka release.</p> <ul style="list-style-type: none"> • Type: true false • Default value: false
The maximum number of times to retry an SSH operation after a timeout	mid.ssh.max_retries	<p>Specifies the maximum amount of times to retry an SSH operation after a time-out. The system sleeps two seconds between each connection attempt. By default, the MID Server retries once only. Set the parameter to 0 to disable retries.</p> <ul style="list-style-type: none"> • Type: integer • Default value: 1
Sets a different remove file command to replace the default <code>/bin/rm -f</code>	mid.ssh.alt_rm	<p>Sets a different SSH remove file command.</p> <ul style="list-style-type: none"> • Type: string • Default value: none
Delay sending any SSH commands to a server after connecting	mid.ssh.initial_delay_ms	<p>Delays sending any SSH probe commands to a server after connecting to the target for the time specified, in milliseconds. This parameter is available starting with the Calgary release. This parameter applies to the legacy SSH client only.</p> <ul style="list-style-type: none"> • Type: integer (milliseconds) • Default value: 0
Suppress history file generation for SSH	mid.ssh.suppress_history	<p>Suppresses the generation of the SSH history file. This parameter applies to the legacy SSH client only.</p> <ul style="list-style-type: none"> • Type: true false • Default value: false
Timeout in ms for SSH socket read	mid.ssh.socket_timeout	<p>Specifies the timeout value for the SSH socket to prevent issues created by a socket timeout. Some devices, such as systems with embedded controllers like UPSs and PDUs, that have SSH enabled require more time to respond to an authentication request. The default value of 2 minutes ensures such requests do not timeout prematurely.</p> <p>In versions prior to Fuji, the default value is 60000 (1 minute).</p> <ul style="list-style-type: none"> • Type: integer (milliseconds) • Default value: 120000 (2 minutes)
Timeout in ms for SSH channel activity	mid.ssh.channel_timeout	<p>Specifies the amount of time that the MID Server waits for activity on the SSH socket before closing the connection. If there has been no activity on the SSH socket for the specified timeout value, the MID Server closes the connection. Some devices, such as systems with embedded controllers like UPSs and PDUs, that have SSH enabled may require more time to respond to an authentication request. This parameter is available starting with the Eureka release.</p> <ul style="list-style-type: none"> • Type: integer (milliseconds) • Default value: 120000 (2 minutes)

Timeout in ms for SSH socket read	mid.ssh.session_timeout	<p>Specifies the amount of time that a cached session remains in memory after last use. Excessively small values tend to decrease performance. This parameter applies to the ServiceNow SSH client only.</p> <ul style="list-style-type: none"> • Type: integer (milliseconds) • Default value: 300000 (5 minutes)
Timeout for SSH command execution (ms)	mid.ssh.command_timeout_ms	<p>The timeout duration, in milliseconds, for the execution of an SSH command.</p> <ul style="list-style-type: none"> • Type: integer (milliseconds) • Default value: 300000 (5 minutes)
Use keyboard interactive authentication for SSH	mid.ssh.use_keyboard_interactive	<p>Uses the <i>keyboard interactive</i> authentication mode ^[8] in SSH daemons on which it is activated.</p> <ul style="list-style-type: none"> • Type: true false • Default value: false
Min size of DH group in bits	mid.ssh.dh_group_length_min	<p>Specifies the minimum group length in bits used for generating a "shared secret" key in Diffie-Hillman key exchange ^[9]. The larger the key the more secure the SSH connection is but at the cost of performance. This parameter is available starting with the Eureka release.</p> <ul style="list-style-type: none"> • Type: integer (bits) • Default value: 1024
Max size of DH group in bits	mid.ssh.dh_group_length_max	<p>Specifies the maximum group length in bits used for generating a "shared secret" key in Diffie-Hillman key exchange ^[9]. The larger the key the more secure the SSH connection is but at the cost of performance. This parameter is available starting with the Eureka release.</p> <ul style="list-style-type: none"> • Type: integer (bits) • Default value: 2048

Default Paths for SSH Commands

By default, the MID Server is configured to search for SSH commands in the following paths and the logged-on user's default paths:

- /usr/sbin
- /usr/bin
- /bin
- /sbin


Upgrade Parameters

Label	Names	Description
Fixed MID Server version	mid.pinned.version	<p>Name of the version to which this MID Server is pinned.</p> <ul style="list-style-type: none"> • Type: string • Default value: build timestamp
Upgrade branch	glide.mid.autoupgrade.branch <i>or</i> mid.upgrade.branch	<p>Defines a <i>branch</i> (a directory on the distribution server) the MID Server should download its upgrades from. This might be set if you had a special MID Server version for some reason. Consult with ServiceNow <i>before</i> adding this parameter to your configuration.</p> <ul style="list-style-type: none"> • Type: string (path) • Default value: none

Upgrade proxy enable	mid.upgrade.use_proxy	<p>If your MID Server must go through a web proxy to access the upgrade URL, set this parameter to true to instruct the MID Server to use the proxy. You must also set the proxy server's host and port. If the instance proxy user name and password are set, they are used for the upgrade proxy as well.</p> <ul style="list-style-type: none"> • Type: true false • Default value: false
Upgrade proxy host	glide.mid.autoupgrade.proxy_host <i>or</i> glide.gldesopap.proxy_host	<p>If your MID Server must go through a web proxy to access the upgrade URL, define the proxy's host here. You must restart the instance after changing this property to apply the change in versions prior to Calgary Patch 6.</p> <ul style="list-style-type: none"> • Type: string (URL) • Default value: none
Upgrade proxy port	glide.mid.autoupgrade.proxy_port <i>or</i> glide.gldesopap.proxy_port	<p>If your MID Server must go through a web proxy to access the upgrade URL, define the proxy's port here. You must restart the instance after changing this property to apply the change in versions prior to Calgary Patch 6.</p> <ul style="list-style-type: none"> • Type: integer (0-65535) • Default value: 80
Upgrade proxy user	glide.mid.autoupgrade.proxy_user	<p>If your MID Server must go through a web proxy to access the upgrade URL, define the proxy's user name here.</p> <ul style="list-style-type: none"> • Type: string (URL) • Default value: none
Upgrade proxy password	glide.mid.autoupgrade.proxy_password	<p>If your MID Server must go through a web proxy to access the upgrade URL, define the proxy's password here.</p> <ul style="list-style-type: none"> • Type: string • Default value: none
Upgrade URL	glide.mid.autoupgrade.host	<p>Controls where the MID Server downloads its upgrades from. Normally, you should not set this parameter.</p> <ul style="list-style-type: none"> • Type: string (URL) • Default value: [10]

Windows Discovery Parameters

Label	Names	Description
Enable or Disable the enforcement of UTF-8 for command output	mid.powershell.enforce_utf8	<p>Enable this parameter to force commands on a target Windows system to return UTF-8 encoded output. Disabling it allows the target system to use its default encoding. This parameter is only valid when PowerShell is enabled. Setting this value to false may result in incorrect values in the CMDB when non-ASCII characters are returned by a probe.</p> <ul style="list-style-type: none"> • Type: true false • Default value: true
Enable PowerShell for Discovery	mid.use_powershell	<p>Specifies whether to enable PowerShell for Discovery. The MID Server requires PowerShell version 2 to operate. If the MID Server cannot find the correct version of PowerShell, it uses WMIRunner instead.</p> <ul style="list-style-type: none"> • Type: true false • Default value: true

Enable/Disable automatically falling back to the MID Server service user credential if all other credentials fail	mid.powershell.local_mid_service_credential_fallback	<p>Specifies the login credentials the MID Server uses if all other credentials fail. This parameter is available starting with the Calgary release.</p> <ul style="list-style-type: none"> • Type: true false • Default value: true
Timeout for Windows probes	mid.windows.probe_timeout	<p>Specifies the timeout value for the Windows probe, in seconds. The default value is 5 minutes.</p> <ul style="list-style-type: none"> • Type: integer • Default value: 300 seconds
MSSQL credentials for PowerShell	mid.powershell.use_mssqlauth	<p>Determines whether PowerShell should use Integrated Windows Authentication ^[11], also known as Windows Integrated Security, or SQL authentication when attempting to log into the MSSQL instance. PowerShell uses Windows Integrated Security by default.</p> <p>Note: This parameter is obsolete starting with the Calgary release and has been removed from the platform. Microsoft SQL Server discoveries use the PowerShell probe, which uses the MID Server's credentials. The Calgary upgrade removes any MSSQL credentials from the Credentials [discovery_credentials] table.</p>  <ul style="list-style-type: none"> • Type: true false • Default value: false
Powershell use credentials table	mid.powershell.use_credentials	<p>Specifies whether PowerShell Discovery should use the Windows credentials from the credentials table. To use PowerShell Discovery on a single domain, set this parameter to false, and then restart the MID Server. In this case, the MID Server runs the probes with the credentials of the user for the MID Server process.</p> <ul style="list-style-type: none"> • Type: true false • Default value: true
Path to Powershell executable	mid.powershell.path	<p>Enables an administrator to point to a specific PowerShell on a MID Server in cases where more than one PowerShell is installed. Supply the path to the directory containing the PowerShell executable, for example, <i>C:\mypowershell</i> or <i>C:\mypowershell\</i>. ServiceNow automatically appends the string <i>powershell.exe</i> to the path.</p> <p>This parameter might be necessary when both 32-bit and 64-bit PowerShells are active on the same MID Server, and it becomes necessary to launch the correct PowerShell for the context. Note that 64-bit Windows employs file system redirection and the MID Server runs as a 32-bit application. If the path is in <i>%WinDir%\System32</i>, Windows automatically redirects to <i>%WinDir%\SysWOW64</i>. To avoid redirection, specify the path as <i>%WinDir%\Sysnative</i>. An example would be to specify <i>C:\WINDOWS\sysnative\WindowsPowerShell\v1.0\</i> instead of <i>C:\WINDOWS\system32\WindowsPowerShell\v1.0\</i>.</p>



Note: *On a 64-bit version of Windows Server 2003 or Windows XP, a Microsoft hotfix^[12] may be required to enable this capability.*

To discover applications running on a 64-bit Windows machine in the Calgary release, the MID Server must be running on a 64-bit Windows host machine. For MID Servers installed on 32-bit hosts to discover 64-bit Windows applications, you must add the `mid.powershell.path` parameter to the MID Server and define the `C:\WINDOWS\system32\WindowsPowerShell\1.0\` path.

- **Type:** string (path)
- **Default value:** none

Timeout for all
Windows probes
on a MID Server

`windows_probe_timeout`

Sets the timeout interval for all Windows probes on a specific MID Server. This value is overridden by the values configured for individual probes with the `wmi_timeout` probe parameter.

- **Type:** integer
- **Default value:** none

References

- [1] https://docs.servicenow.com/bundle/jakarta-it-operations-management/page/product/mid-server/concept/c_MIDServerConfiguration.html
- [2] <http://docs.oracle.com/javase/1.3/docs/tooldocs/win32/keytool.html>
- [3] <http://java.sun.com/j2se/1.4.2/docs/api/java/text/SimpleDateFormat.html>
- [4] <http://en.wikipedia.org/wiki/Subnetwork>
- [5] http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol#Security_implications
- [6] http://en.wikipedia.org/wiki/Object_identifier
- [7] <http://en.wikipedia.org/wiki/Sudo>
- [8] http://en.wikipedia.org/wiki/Secure_Shell#Architecture
- [9] http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
- [10] <http://install.service-now.com/glide/distribution/builds/mid/>
- [11] [http://msdn.microsoft.com/en-us/library/aa292114\(VS.71\).aspx](http://msdn.microsoft.com/en-us/library/aa292114(VS.71).aspx)
- [12] <http://support.microsoft.com/kb/942589>

MID Server Clusters



Note: This article applies to Fuji. For more current information, see *MID Server Cluster Configuration* ^[1] at <http://docs.servicenow.com>. The ServiceNow Wiki is no longer being updated. Please refer to <http://docs.servicenow.com> for the latest product documentation.

Overview

MID Server clusters enable multiple MID Servers with the appropriate **capabilities** to be grouped together for *load balancing* and *fail-over protection*. A MID Server can be added to both a load balancing cluster and a fail-over cluster for more flexibility.

MID Server clusters are available for Discovery and for use with products integrating with the ServiceNow platform.

For performance and reliability reasons, these data sources should not be used with MID Server clusters:

- LDAP
- Export sets
- JDBC data sources

These external data sources should only be used with dedicated MID Servers.

MID Server Cluster Event

The following event is triggered when the platform cannot find a MID Server with the appropriate capabilities to replace a MID Server in a fail-over cluster. Use this event to create an email to notify appropriate users that the cluster has failed.

Event	Table	Description	Business Rule
mid_server.cluster.down	MID Server Cluster [ecc_agent_cluster]	A MID server cluster has failed	MID Server Cluster Management

How Clusters Work

MID Servers in clusters must be able to connect to all the devices with which they are expected to communicate. Make sure all the MID Servers are added to any Access Control List (ACL) in use. MID Server clusters are managed by a business rule called **MID Server Cluster Management**, which checks to see if the MID Server assigned to a job in the **ECC Queue** belongs to a cluster.

Load Balancing

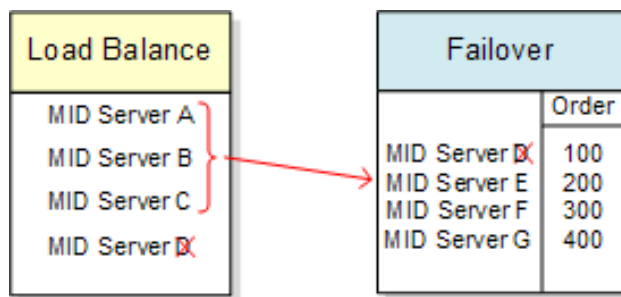
If the cluster business rule determines that a MID Server is part of a load balancing cluster, the application using the MID Server automatically balances the work between the MID Servers in that cluster. It is best practice to put MID Servers with the same capabilities in a load balancing cluster.

Fail-Over Protection

MID Servers in a *fail-over* cluster each have a configured order that the platform uses to determine which MID Server to use next in case of failure. MID Servers in a fail-over cluster work independently and do not load balance with other MID Servers in that cluster (although they might also be members of load balancing clusters). When a MID Server fails, the **MID Server Cluster Management** business rule selects the highest available MID Server in the order to take over the work. The selected MID Server checks the ECC Queue and starts with jobs that are either **Processing** or **Ready**. It is best practice to configure a fail-over MID Server with at least the same capabilities as the MID Server it is intended to relieve.

Combining Clusters

A MID Server can be added to both types of clusters at the same time. This diagram shows a scenario in which a MID Server from a load balancing cluster (MID Server D) is also present in a failover cluster. If MID Server D fails, MID Server E in the failover cluster is available to the load balancing cluster to perform the tasks previously assigned to MID Server D.



Configuring a Cluster

1. Navigate to **MID Server > Clusters**.
2. Click **New**.
3. Name the cluster and select the cluster type: **Failover** or **Load Balance**.
4. Right click in the header bar and select **Save** from the context menu.
5. Click **Edit** in the **Includes MID Servers** Related List.
6. Select appropriate MID Servers for this cluster from the slushbucket.

***Note:** All MID Servers in a cluster must have **capabilities** defined. Ensure that each MID Server has the appropriate capabilities for the job. A MID Server in a failover cluster must have the same capabilities (or expanded capabilities) as the MID Server it is expected to replace.*

MID Server Cluster [Update] [Delete]

Name:

Type:

[Update] [Delete]

Includes MID Servers [Edit...] Go to: [Q]

MID Server Cluster = SNC_domain02

MID server	Status	Host OS	Version	Order
<input type="checkbox"/> MID_Prod01	Up	Windows	01-03-2011_1602	100
<input type="checkbox"/> MID_ProdSSH01	Up	Windows	01-03-2011_1602	100

[Actions on selected rows...]

References

[1] <https://docs.servicenow.com/bundle/jakarta-it-operations-management/page/product/mid-server/reference/mid-server-clusters.html>

Autofinder

Discovery

Orchestration

Related Topics

- Cloud Provisioning
- Help the Help Desk
- Help the Help Desk Login Script
- ECC Queue
- Useful Related Lists in CI Forms
- Creating a Workflow
- Using Workflow Activities

Get the Book



Discovery



Data Collected by Discovery



Orchestration for VMWare

Overview

MID Servers are associated with IP address ranges, enabling Orchestration to select the correct MID Server to use for an Orchestration activity based on the IP address of the target machine. This functionality ensures that a MID Server with proper privileges is available wherever Orchestration probes need to operate in a network. Autofinder also enables administrators to define specific **capabilities** for each MID Server within an IP address range.

Mapping IP Addresses to DNS Names

If the MID Server manages resources within defined IP ranges, all host servers must have their DNS names mapped to an IP address. This ensures that the appropriate MID Server is selected based on the IP Address range configuration. If this is not done, Orchestration reverts to the default MID Server. If Discovery cannot discover the server and resolve the DNS name to an IP address, you must perform this task manually.

1. Enter **cmdb_ci_dns_name.list** in the navigation filter.

A list of DNS names appears.

2. Check the list for your host server.

If it does not appear in the list, continue with this procedure to create the relationship between the DNS name and the IP address manually.

3. Click **New**.
 4. Enter the fully-qualified domain name (FQDN) of the host server in the **Name** field.
 5. Right-click in the form header and select **Save** from the context menu.
 6. In the **IP Address** related list, click **New**.
 7. In the **IP Address** field, enter the IP address of your host server.
-

- 8. In the **Nic** field, select **eth0** or your preferred network interface controller.
- 9. Leave the **Netmask** field blank.
- 10. Click **Submit**.

Configuring a MID Server for an IP Address Range

- 1. Navigate to **MID Server > IP Ranges**.
- 2. Click **New**.
- 3. Type a unique name for this MID Server Autofinder IP address range.

This name is for reference only and is not used in any processing.
- 4. Define the IP addresses for this range, using one or more of the following formats in a comma-delimited list.
 - IP Address Ranges
 - IP Networks
 - IP Address Lists

For additional details about these formats, see **Configuring IP Addresses**.
- 5. In the **Type** field, select whether to **Include** or **Exclude** these addresses.

MID Server IP Range

Submit

Name:

SDSales

Range:

10.10.11.8/24,10.10.10.0-10.10.10.255,10.10.8.45,10.10.8.68

Type:

Include

Submit

- 6. Click **Submit**.
- 7. Reopen the form and click **Edit** in the **MID Servers** Related List.
- 8. Select one or more MID Servers to use for this IP address range.

MID Server IP Range

UpdateDelete

Name:

SDSales

Range:

10.10.11.8/24,10.10.10.0-10.10.10.255,10.10.8.45,10.10.8.68

Type:

Include

UpdateDelete

MID Servers

NewEdit...

Go to MID Server

IP Range = SDSales

MID Server

Surfpilot-MID1

Actions on selected rows...

1 to 1 of 1

The IP address ranges defined here also appear in a Related List in the MID Server's record (*Orchestration > MIDServers*).

MID Server Capabilities

MID Server *capabilities* define the specific functions of a MID Server within an IP address range. At least one capability is required for each MID Server used by Orchestration. The base functionality enables an administrator to select specific capabilities for the probes launched by each MID Server. You can assign multiple MID Servers to the same IP address range and give them different capabilities, or assign a MID Server with specific capabilities to more than one IP address range. When Orchestration initiates a Workflow activity, Orchestration uses the IP address of the target machine to locate the MID Server assigned to that network segment that has the necessary capabilities to execute the activity.

The following capabilities are available for Orchestration:

- SSH
- SNMP
- VMware
- PowerShell
- WMI
- SOAP
- REST
- Resolve DNS

Values

Capabilities provided in the base system do not have a defined **Value** string. A MID Server configured to use a capability that has no **Value** can locate any device using that capability's protocol. If a capability has a defined value, the MID Server using that capability finds only those devices using that protocol that match the value string *exactly*. The exception to this is the **Resolve DNS** capability, which is configured to resolve any DNS name into an IP address using a partial string match.

Scripted Value Matching

A module called Capability Value Tests, enables administrators to create capabilities that find devices using values that do not require exact string matching. Action on these values is controlled by a user-defined script. The Resolve DNS capability is provided in the base system and is configured to resolve DNS names into IP addresses for devices whose names *end* with a specified domain name. The capability **Value** entered is automatically prefaced with a dot during processing to match domain syntax. This value can contain one or more sub-domains, but must include the end of the domain string. Matching devices must end with the identical syntax. The script for the Resolve DNS capability determines if a device name matches the criteria defined by **Value**. If a match exists, the platform performs the address resolution automatically. For example, if the value for the Resolve DNS capability is **service-now.com**, the MID Server with this capability finds *lnxlab01.sandiego.service-now.com* and *dbsrv101.sanjose.service-now.com*. If the value is changed to **sandiego.service-now.com**, then the MID Server finds only *lnxlab01*.



Note: If **Value** in the Resolve DNS capability is blank, then all domains match.

To view the script for evaluating this capability, navigate to *MID Server > Capability Value Tests* and select **Resolve DNS** from the list.

The screenshot shows the 'MID Server Capability Value Test' configuration window. The 'Capability' dropdown is set to 'Resolve DNS' and the 'Active' checkbox is checked. The 'Value test script' field contains the following JavaScript code:

```

1 function(capability_value, requested_value) {
2   if (JSUtil.nil(capability_value)) {
3     return true;
4   }
5   var i = requested_value.lastIndexOf(capability_value);
6   if (i < 0) {
7     return false;
8   }
9   if (i == 0) {
10    return true;
11  }
12  if (requested_value.length != i + capability_value.length) {
13    return false;
14  }
15  return (requested_value.charAt(i - 1) == '.') && (i > 1);
16 }

```

At the bottom of the window are 'Update' and 'Delete' buttons.

Configuring Capabilities

1. Navigate to **MID Server > Capabilities**.
2. Select an existing capability or click **New** to create one.

NOTE: At least one capability is required for each MID Server. Ensure that each IP address range has MID Servers with the necessary capabilities to complete the *Orchestration* activities on that network segment.

3. Configure the value for a custom capability.

An example is a capability for **DOMAIN**, with a value of **service-now**.

4. Click **Submit**.
5. Reopen the record and click **Edit** in the MID Servers Related List.
6. Select one or more MID Servers for this capability from the slushbucket.

← MID Server Capability

Capability:

DOMAIN

Value:

service-now

Update

Delete

MID Servers

New

Edit...

Go to

MID Server

► Capability = DOMAIN

MID Server

☐

Surfpilot

☐

Actions on selected rows...

The capability defined here also appears in the primary record for this MID Server.

← MID Server

Update

Delete

Name:

Surfpilot

Host name:

sandb01.service-now.com

Status:

Up

IP address:

10.10.10.3

Version:

11-07-2010_2100

Router:

10.10.10.1

Last refreshed:

2010-11-15 14:14:18

Network:

10.10.10.0/23

Started:

2010-11-11 09:11:14

Host OS:

Windows

Stopped:

Windows domain:

SERVICE-NOW

Update

Delete

Related Links

[Grab MID Logs](#)

[MID Stats](#)

[Refresh SNMP MIBs](#)

[Restart MID](#)

[Upgrade MID](#)

[Configuration help](#)

Configuration Parameters (6)

IP Ranges

Capabilities (1)

Logs (7)

Threads (14)

Properties

Capabilities

New

Edit...

Go to

Capability

► MID Server = Surfpilot

Capability

Value

☐

DOMAIN

service-now

☐

Actions on selected rows...

1

to 1 of 1

MID Server Selection Criteria

If Orchestration finds multiple MID Servers in the target IP range with appropriate capabilities, it selects one of these at random. If no MID Servers are found with the necessary capabilities, Orchestration uses the MID Server defined in Orchestration MID Server properties. For this reason, it is very important to define a default MID Server in the properties that can fulfill this function.

To set the default Orchestration MID Server, navigate to **Orchestration > MID Server Properties** and type the name of the MID Server into the **Default MID Server to use for Orchestration Activities** property field.


MID Server

Default MID Server to use for Orchestration Activities

DevDoc1

With the Dublin release, the instance does not select a MID Server at random if no default is specified. The first MID Server to connect to the instance becomes the default MID Server.

You can set a MID Server as the default by clicking the **Set as default** related link on the MID Server form.

 MID Server

Name:	<input type="text" value="lsh30"/>	Host name
Status:	<input type="text" value="Up"/>	IP address
Version:	<input type="text" value="2013-10-08-2230"/>	Router:
Last refreshed:	<input type="text" value="2013-10-09 16:34:07"/>	Network:
Started:	<input type="text" value="2013-10-09 15:21:27"/>	Host OS:
Stopped:	<input type="text" value="2013-10-09 10:18:38"/>	Windows d

Related Links

[Grab MID logs](#)

[Set as default](#)

[MID Statistics](#)

[Restart MID](#)

[Upgrade MID](#)

Approvals and Provisioning

Approving and Provisioning VMware Requests - Versions Prior to Calgary

Overview

Some service catalog requests for virtual servers that are not using task automation must be approved and then provisioned by members of designated approval and provisioning groups. Upon approval of the request, Orchestration automatically creates the virtual server and powers it up on the network, using one of the IP addresses supplied. When Orchestration fulfills a virtual server request and creates a VMware configuration item (CI), ServiceNow creates a new asset in Asset Management. This new asset appears in the requesters My Assets portal.

Workflow

The approval and provisioning process for each virtual server request in the base system is controlled by a workflow (**Workflow > Workflow Editor**) called **Virtual Server**. This workflow performs the following tasks:

- Creates approval tasks for the approval group.
- Collects the provisioning information when the request is approved. (If the request is rejected, the workflow ends.) The workflow determines if the request is for a Windows or Linux virtual machine.
- Creates a catalog task to select the proper virtual server template and supply it with the necessary requirements, including the appropriate ESX resource pool.
- Sets the variables and provisions the virtual server. Using the template selected, Orchestration clones the virtual server, attaches the IP address to the new virtual machine if guest customization is configured.
- Powers up the virtual server.
- Notifies the requester that the virtual machine has been created successfully.

Approving VMware Requests

Requests for virtual servers in the base system can be approved or rejected by one member in either of the following approval groups:

- VMware approvers
- Virtual Provisioning Cloud Administrators

When a virtual server is requested through the service catalog, the workflow creates an approval task in each group member's Service Desk approval queue.

To approve or reject a VMware request:

1. Navigate to **Service Desk > My Approvals**.
2. Open the approval request.
3. Change the state of the request to **Approved** or **Rejected**.

After any member of the approval group approves the request, the workflow creates the provisioning task. The approval request is updated in the queues of other approval group members.

- Click the arrow by virtual machine in the **Description** list to display the feature summary.

Approval

Approver: Alene Rabeck

State: Requested

Approval for: RITM0010006

Comments:

Summary of Item being approved:

Description	Price	Quantity	Total
Request a new virtual Windows or Linux server	\$1,460.00	1	\$1,460.00

Business purpose: Test machine for Winter release
 Start: 2013-01-25 13:28:57
 End: 2013-03-19 13:28:57
 Business service: ITSM
 Application: ServiceNow
 Used for: Test
 Datacenter: -- None --
 Offering: Linux
 Use predefined size: No
 Size: -- None --
 CPUs: 2
 Memory: 4 GB
 Additional disk: 20 GB

Activity >>

2013-01-18 13:31:51 System Administrator - Changed: Approver, State
 Approver: Alene Rabeck
 State: Requested

Update Approve Reject Delete

Provisioning Virtual Servers

The provisioning task is assigned to a user who is a member of the VMware Operators group.

To complete the provisioning task:

- Navigate to **Service Desk > My Groups Work**.
- Open the provisioning task.
- Provide the appropriate information (see table).

Some information is pre-populated from the catalog request.

- Click **Close Task**.

Options	Description
Template	Select an operating system template to be cloned for this virtual machine.
Destination folder	Each template belongs to a vCenter <i>datacenter</i> , which contains <i>folders</i> of virtual machines. Select a folder from the datacenter that contains the provisioned virtual machine. If no folder is selected, the resulting cloned instance is placed in the folder containing the template that was used to create the clone.
Clone name	Provide the name of the virtual machine as it should appear in VMware vCenter. This name must be unique on the ESX Server (or the cluster) on which it is being provisioned.
Cluster	Clusters appearing in the list are those from the datacenter in which the selected destination folder resides. If the virtual machine is not being attached to a cluster, choose None . In this case, make sure to select a non-clustered Host .
ESX Host	Select the ESX Server on which to deploy the virtual machine. If you selected None in the Cluster field, only those hosts that are not part of a cluster are available. If you did select a cluster for this virtual server, then the available hosts all belong to the selected cluster.
Resource pool	Select the ESX resource pool to use for this virtual machine. If a cluster was chosen, the available resource pools belong to that cluster. If a host was selected (and no cluster), the available resource pools belong to the selected host. Resource pools define the maximum amount of resources that templates using that pool can consume. An ESX Server property enables resource pools to expand when necessary if the ESX Server has additional resources to spare. If you select the Resources pool, the ESX Server creates a virtual machine for use under a normal load.
Datastore	Select the datastore on which to provision the virtual server and any data disks. To put the virtual server on the datastore where the template is located, select None . The available datastores are for the selected host.

Network Select the network that the virtual server will use. Available networks are those from the datacenter in which the selected destination folder resides.

Guest customizations If guest customizations are configured for this virtual server, select one of the following:

- **VM's host name:** [Required] Name of the server hosting the virtual machine being provisioned. Check the **Notes** in the request form for the name designated by the requester.
- **Windows/Linux configuration:** [Required] Specifics for Windows or Linux virtual machines configured in **VMware > Customization Specifications**. Configuration information includes DNS for Linux and the product key and domain credentials for Windows.
- **Network configuration:** [Required] Select the network and the network configuration for the virtual server. The IP address allocated to the virtual server is selected from a list of available addresses configured in the network record.

If you choose not to apply guest customizations to the virtual server, Orchestration provisions the server directly from the template, using only the configuration available to that template.

The screenshot shows the 'Catalog Task' form in the VMware vSphere interface. The form is divided into several sections:

- Task Information:** Includes fields for Number (TASK0010002), Request (REQ0010002), Request Item (RITM0010002), Requested for (David Loo), Due date (2013-03-05 12:41:20), Configuration item, Approval (Not Yet Requested), State (Open), Assignment group (VMware Operators), Assigned to, and Work notes list.
- Variables:** A section for defining variables.
- VM provisioning details:** Includes Business purpose (Test machine for exchange server migration) and More information.
- VMware provisioning information:** Includes Used for (QA), More information, Template (Prod-Server2012-Template | ServiceNow vCenter), Clone name (qaeschttest02), Datacenter (Seattle Staging Data Center), Destination folder (None), VMware configuration (Staging Cluster), ESX host (stage-esx), Resource pool (Resources | Staging Cluster), Datastore (stage datastore | 251.0 | 158.7890625), and Network (Stage Network).
- Guest configuration:** Includes Guest customization (No).
- Notes:** A section for adding notes, with a note titled 'Name this server qaeschttest02'.
- Short description:** Select how this virtual server will be provisioned in vSphere.
- Description:** A text area for additional details.
- Work notes:** A large text area for work notes.

Provisioning Rules

Provisioning rules enable an administrator to select which vCenter resources (datacenter, network, and folder) are used to provision virtual machines for a specific virtual machine category (such as Dev, QA, or Prod) or for *any* category if the **Category** field in the rule is left empty.

Rule Order

Each rule has an **Order** field that defines the sequence for evaluating the rules. The rules are evaluated by the Select Datacenter, Network, and Folder activity. When that activity runs, it finds all the provisioning rules that apply to a particular vCenter instance and category (rules with a blank category match *any* category), and then uses the provisioning rule with the lowest order value. By carefully choosing order values for provisioning rules, you can ensure that rules for specific categories are evaluated *before* (low order values) provisioning rules for *any* category (high order values).

Weight

You might want more than one datacenter, network, or folder to be used for virtual machines on a particular vCenter instance and category. For example, you have a vCenter containing two datacenters, and you'd like to provision 75% of the virtual machines to one datacenter, and 25% to the other. You can do this by creating two provisioning rules for the particular vCenter and category with the same order value for each. Multiple rules with the same **vCenter**, **Category**, and **Order** values trigger this special behavior. Give each provisioning rule a **Weight** value proportional to the percentage of the time you want the rule to be used. For this example, you might choose **Weight** values of 300 and 100. Any other numbers in the same proportion would also work, like 3 and 1. To check the percentage for any given rule, calculate the **Weight** value of that rule divided by the sum of the **Weight** values for all the rules with the same vCenter, category, and order value. In the example, the calculations would be $300 / (300 + 100) = 75\%$, and $100 / (300 + 100) = 25\%$, which meets the goal.

Creating a Provisioning Rule

1. Navigate to **VMware > Rules > Provisioning Rules**.
2. Click **New**.
3. Create a unique **Name** for this rule.
4. Select a **Category**.

If you do not select a category, the rule applies to any category.

5. Select the **vCenter** to use for this category.

The **Datacenter** field appears.

6. Select a datacenter from the list of datacenters available for this vCenter.

The **Network** and **Folder** fields appear.

7. Select an appropriate network and a folder.
8. Enter an **Order** value to establish the order in which this rule is evaluated.
9. If you create multiple rules with the same **Category**, **vCenter**, and **Order**, select an appropriate **Weight** to determine which virtual machines, by proportion, are provisioned with this rule.
10. Click **Submit**.

The screenshot shows the 'VM Provisioning Rule' configuration form. It includes fields for Name, Category, vCenter, Order, Weight, Datacenter, Network, and Folder. The 'Name' field is 'Business Critical1', 'Category' is 'Dev', 'vCenter' is 'vCenter@server2008', 'Order' is '100', and 'Weight' is '200'. The 'Datacenter' field is 'San Diego Dev Data Cent', 'Network' is 'Dev VM Network', and 'Folder' is 'Dev Instances'. There are 'Update' and 'Delete' buttons at the bottom left and top right.

VM Provisioning Rule		= Required field		Update Delete	
Name:	Business Critical1	Datacenter:	San Diego Dev Data Cent		
Category:	Dev	Network:	Dev VM Network		
vCenter:	vCenter@server2008	Folder:	Dev Instances		
Order:	100				
Weight:	200				
Update Delete					

Reference

VMware Component Relationships

Discovery

Orchestration

Related Topics

- Cloud Provisioning
- Help the Help Desk
- Help the Help Desk Login Script
- ECC Queue
- Useful Related Lists in CI Forms
- Creating a Workflow
- Using Workflow Activities

Get the Book



Discovery



Data Collected by Discovery



Orchestration for VMWare



Note: The latest release this documentation applies to is Fuji. For the Geneva release, see Discovery^[1]. Documentation for later releases is also on docs.servicenow.com^[2].

Overview

ServiceNow supports the use of virtual machines generated by the VMware application, installed on Windows, Linux, or ESX Servers. The ServiceNow Discovery product can extract information from VMware configuration items (CI), including their relationships. Discovery is configured to work with the Orchestration VMware Support Plugin, which enables the automatic cloning of virtual machines by an ESX Server managed by vCenter. For information about data collected by Discovery on vCenter, see Discovery for VMware vCenter.

VMware Architecture

ServiceNow supports two basic types of VMware deployment using the VMware application:

- VMware installed on an ESX Server, managed by vCenter.
- VMware installed on a Windows or Linux host machine, not managed by vCenter.

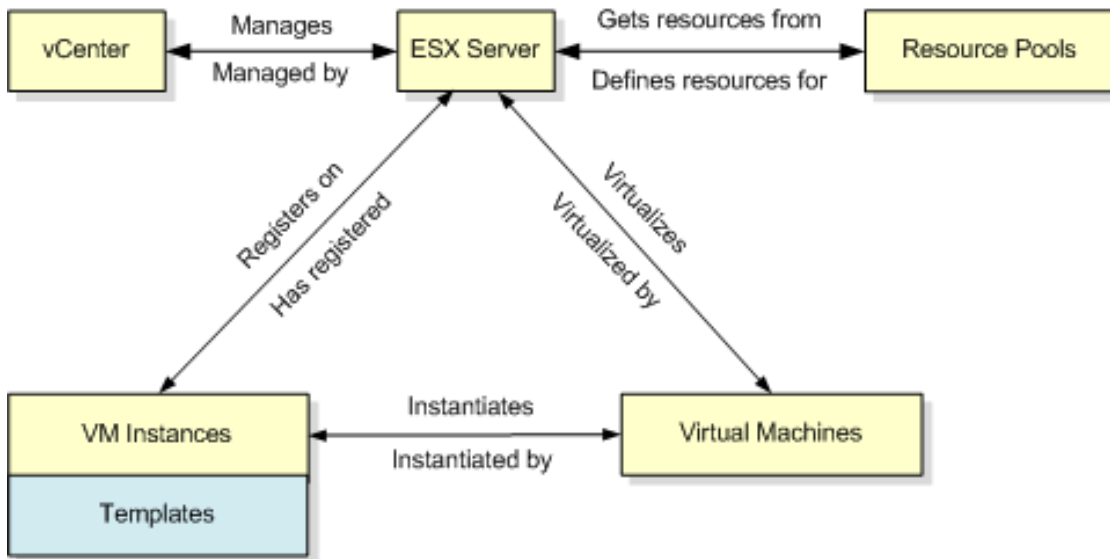
ServiceNow Discovery can extract information from all the components in a VMware system, including vCenter. Discovery creates records in the CMDB for vCenter, the host machine and all the virtual machines running on that server. Discovery finds the stored templates and maps all the relationships between components. In networks that use Orchestration to create and manage virtual servers, Discovery populates records automatically and detects changes in the network. Without Discovery, all the records for Orchestration VMware Support must be created and updated

manually, including the relationships between VMware components.

vCenter Cloning

The vCenter management console can control multiple ESX Server machines, each of which is capable of hosting multiple virtual servers cloned from stored templates. The relationships between VMware components for this type of installation are shown in the following diagram:

VMWare Relationships with ESX Server



Relationships

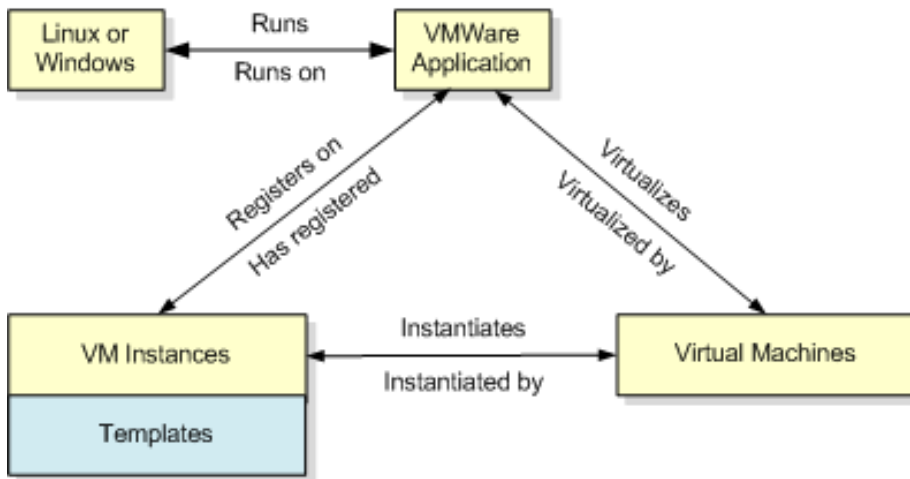
The components in a system managed by vCenter have the following relationships:

- VCenter: **Manages** one or more ESX Servers
- ESX Server:
 - **Managed by** vCenter
 - **Gets resources from** the Resource Pool
 - **Has registered** VMware instances
 - **Virtualizes** virtual machines.
- Resource Pool: **Defines resources for** the ESX Server. See Resource Pools for more information.
- VM Instances (including images and templates):
 - **Registers on** the ESX Server
 - **Instantiates** individual virtual machines.
- Virtual machines:
 - **Instantiated by** VM instances (images and templates)
 - **Virtualized by** ESX Server

VMware Running on a Host Machine

In the basic VMware system, the VMware application runs on a Windows or Linux host machine. This system can clone instances from templates, but cannot be automated. The relationships between VMware components for this type of installation are shown in the following diagram:

VMWare Relationships Without ESX Server



Relationships

The components in a VMware system installed on a Windows or Linux host have the following relationships:

- Windows or Linux Server: **Runs** the VMware application
- VMware application:
 - **Runs on** a Windows or Linux host machine
 - **Has registered** VM instances
 - **Virtualizes** virtual machines.
- VM Instances (including images and templates):
 - **Registers on** the VMware application
 - **Instantiates** individual virtual machines.
- Virtual machines:
 - **Instantiated by** VM instances
 - **Virtualized by** VMware application

References

- [1] https://docs.servicenow.com/bundle/geneva-it-operations-management/page/product/discovery/concept/c_Discovery.html
- [2] <http://docs.servicenow.com>

VMware Workflow Activities

Discovery

Orchestration

Related Topics

- Cloud Provisioning
- Help the Help Desk
- Help the Help Desk Login Script
- ECC Queue
- Useful Related Lists in CI Forms
- Creating a Workflow
- Using Workflow Activities

Get the Book



Discovery



Data Collected by Discovery



Orchestration for VMWare

Overview

Orchestration - VMware Support adds these activities for use in workflows. Your ServiceNow instance must have access to a MID Server configured to use VMware to run these activities. For the list of all Orchestration activities, see Orchestration Activities.

Determining VMware Activity Result Values

VMware activities communicate with vCenter through a MID Server. When a VMware activity sends a request, the MID Server sends a response to the ECC Queue. All VMware activities set their `activity.result` value based on the payload of the response from the MID Server. If this payload contains an error, the activity result value is **failure**. If the the payload contains no error, the activity result value is **success**. Some activities, such as **Delete Snapshot**, specify additional result values. For more information about `activity.result`, see Using the Activity Result Value.

Managed Object Reference ID

A managed object reference (MOR) ID uniquely identifies a VMware virtual machine. ServiceNow uses MOR ID values in several VMware activities to select specific virtual machines to act on. VMware provides additional documentation on obtaining the MOR ID ^[1] for a virtual machine.

Virtual Machine UUID

The VMware universal unique identifier (UUID) required by VMware activities (**VM uuid** input variable) must be in the following format: 4210c162-e31e-70e6-4a03-b46abbe17b4f. If you are writing a workflow and not using an automated workflow from ServiceNow, you must provide a properly formatted UUID. A UUID from another source might be in the wrong format. For example the UUID from the VMX file (**uuid.bios** field) on the

virtual machine appears in this format, 42 10 c1 62 e3 1e 70 e6-4a 03 b4 6a bb e1 7b 4f, and produces an error. If the UUID you have for a virtual machine is not in the correct format, use one of these methods to obtain the correct value.

Managed Object Browser

The Managed Object Browser (MOB) is a vCenter utility that allows users to view detailed information about vCenter objects, such as images and virtual machines. To find the UUID of a virtual machine using the MOB:

1. Navigate to **https://<vCenter IP>/mob** to log into the MOB.
2. Browse to **content**, **rootFolder**, and down the **childEntity** list into the appropriate datacenter, datastore, and finally down to the actual virtual machine.
3. In the virtual machine, click **config** and find the **uuid** field.

Copy this value into the **VM uuid** activity input variable.

Conversion Function

A function called `turnCorrelationIdToUuid` in the *VMUtils* script include converts a UUID to the proper format automatically. Use this function to convert a UUID to the proper format within the workflow:

```
javascript:VMUtils.turnCorrelationIdToUuid(<uuid from another source>)
```

For example, you can enter `javascript:VMUtils.turnCorrelationIdToUuid('42 10 c1 62 e3 1e 70 e6-4a 03 b4 6a bb e1 7b 4f')` directly in the **VM uuid** activity input variable.

Another method is to use the function to create a scratchpad variable that is available to all the activities in the workflow. For example, you might add a **Run Script** activity to the beginning of the workflow in which you create the following variable:

```
workflow.scratchpad.uuid=VMUtils.turnCorrelationIdToUuid('42 10 c1 62  
e3 1e 70 e6-4a 03 b4 6a bb e1 7b 4f')
```

You can then access this variable from any activity by entering `${workflow.scratchpad.uuid}` in the **VM uuid** activity input variable.

Add Disk

The **Add Disk** activity creates a new disk on a virtual machine. This activity selects a datastore for the new hard disk automatically if you do not specify one.

Input Variables

These variables determine the behavior of the activity.

Field	Description
vCenter	IP address of the vCenter server that manages the virtual machine to operate.
Datastore MOR id	The ID of the datastore on which to put this disk. If this variable is blank, Orchestration searches all the datastores associated with the virtual machine to find one with sufficient space for the disk being added.
VM uuid	The VMware universal unique identifier assigned to this virtual machine. If you are creating your own workflow, see Virtual Machine UUID for instructions on properly formatting the unique identifier.
Disk size (MB)	The size of the new disk to create, in megabytes. This activity provisions all the necessary space for the new disk immediately (thick mode).

Change Network

The **Change Network** activity changes the network that a virtual machine is configured to use.

Input Variables

These variables determine the behavior of the activity.

Field	Description
vCenter	IP address of the vCenter server that manages the virtual machine to operate.
VM uuid	The VMware universal unique identifier assigned to this virtual machine. If you are creating your own workflow, see Virtual Machine UUID for instructions on properly formatting the unique identifier.
Network	Name of the network. For example, Production Network . A virtual machine can only access a network in the same datacenter.

Change State

The **Change State** activity sends commands to vCenter to control the power state of a given VMware virtual machine, such as powering on and powering off the VM. If the VM is already in the state to which it is being changed, the workflow takes no action.

Input Variables

These variables determine the behavior of the activity.

Field	Description
vCenter	IP address to the vCenter server that manages the virtual machine to operate.
Action	Select the new state for the virtual machine: <ul style="list-style-type: none"> • Power On: turns on a virtual machine that is powered off or suspended and does nothing if the virtual machine is already on. • Power Off: turns off a virtual machine that is powered on or suspended and does nothing if the virtual machine is already off. This variable returns an error if the virtual machine is suspended. • Suspend: suspends a virtual machine that is powered on and does nothing if the virtual machine is already suspended. This variable returns an error if the virtual machine is off. • Reset: resets a virtual machine that is powered on. This variable returns an error if the virtual machine is off or suspended.
VM uuid	The VMware universal unique identifier assigned to this virtual machine. If you are creating your own workflow, see Virtual Machine UUID for instructions on properly formatting the unique identifier.

Check VM Alive

The **Check VM Alive** activity uses the VMware API to determine if a newly configured virtual machine is alive. The virtual machine is alive if its state is **powered on** and it uses the same IP address it was configured to use.

Input Variables

These variables determine the behavior of the activity.

Field	Description
vCenter	IP address of the vCenter server that manages the virtual machine to check.
IP Address	The IP address that the virtual machine with the VM uuid parameter should have to be declared alive.
VM uuid	The VMware universal unique identifier assigned to this virtual machine. If you are creating your own workflow, see Virtual Machine UUID for instructions on properly formatting the unique identifier.

Clone

The **Clone** activity sends commands to vCenter to clone a given VMware virtual machine or virtual machine template. Several input variables require a *MOR ID*. ServiceNow stores MOR data in the **Object ID** field of configuration item records.

Input Variables

These variables determine the behavior of the activity.

Field	Description
vCenter	IP address of the vCenter server that manages the virtual machine to clone and also will manage the clone.
VM uuid	The VMware universal unique identifier assigned to the machine you are cloning. If you are creating your own workflow, see Virtual Machine UUID for instructions on properly formatting the unique identifier.
Clone name	The name to assign to the newly cloned virtual machine.
Folder MOR id	The managed object reference ID for the folder in which the cloned virtual machine resides. This variable is optional. If this field is blank, Orchestration places the cloned virtual machine in the same folder as the source virtual machine.
Datastore MOR id	The managed object reference ID for the datastore the new virtual machine belongs to. This variable is optional. If this field is blank, Orchestration places the cloned virtual machine in the same datastore as the source virtual machine.
Host MOR id	The managed object reference ID for the host the new virtual machine is assigned to. This variable is optional. If this field is blank, Orchestration assigns the cloned virtual machine to the same host as the source virtual machine.
Resource pool MOR id	The managed object reference ID for the resource pool the new virtual machine is assigned to. This variable is optional when cloning a virtual machine. If this field is blank, Orchestration assigns the cloned virtual machine to the same resource pool as the source virtual machine.
Resource Pool Owner	Owner of the resource pool as seen by vCenter. For example, the owner might be something like labesx01.service-now.com or an IP address. The owner should point to the ESX box on which the original VM and clone are located (whatever vCenter's representation of that ESX name is).

Configure Linux

The **Configure Linux** activity sends commands to vCenter to set the identity and network information on a given VMware virtual Linux machine. This activity also enables guest customization for the Linux machine. This activity fails if run against a single virtual machine more than once.

Input Variables

These variables determine the behavior of the activity.

Field	Description
vCenter	IP address of the vCenter server that manages the Linux virtual machine being configured.
VM uuid	The VMware universal unique identifier assigned to this virtual machine. If you are creating your own workflow, see Virtual Machine UUID for instructions on properly formatting the unique identifier.
Hostname	The operating system name assigned to the Linux virtual machine.
Domain	The domain the Linux virtual machine is assigned to.
IP Address	The IP address assigned to the Linux virtual machine.
Netmask	The netmask for the network the Linux virtual machine's IP address belongs to.
Gateway	The gateway address for the network the Linux virtual machine's IP address belongs to.
DNS	The DNS server for the network the Linux virtual machine's IP address belongs to.

Configure Windows

The **Configure Windows** activity sends commands to vCenter to set the identity and network information on a given VMware virtual Windows machine. This activity also enables guest customization for the Windows machine. This activity fails if run against a single virtual machine more than once.

Input Variables

These variables determine the behavior of the activity.

Field	Description
vCenter	IP address of the vCenter server that manages the Windows virtual machine being configured.
VM uuid	The VMware universal unique identifier assigned to this virtual machine. If you are creating your own workflow, see Virtual Machine UUID for instructions on properly formatting the unique identifier.
Gateway	The gateway address for the network the Windows virtual machine's IP address belongs to.
Administrator Password	The password assigned to the Administrator user for this operating system.
Domain Administrator Password	The password for the domain user with the proper credentials to move a machine onto the given domain.
Domain Administrator	A user who has the credentials to get this Windows machine onto the domain.
DNS	The DNS server for the network the Windows virtual machine's IP address belongs to.
Hostname	The computer name of the Windows virtual machine.
IP Address	The IP address assigned to the Windows virtual machine.
Netmask	The netmask for the network the Windows virtual machine's IP address belongs to.

Organization	The organization of the registered user for the OS installed on this virtual machine. This value appears in the Properties box of My Computer.
Time Zone	The time zone <i>value</i> . For example, the value for the US/Pacific time zone is 4 .
Domain	The domain the Windows virtual machine is assigned to.
Product Key	The Microsoft product key for the Windows operating system installed on the virtual machine.
Registered User	The registered user for the operating system installed on the virtual machine. This user appears in the Properties box of My Computer.
Run once	A set of Windows commands that run on the specified Windows machine when this activity initializes.
License mode	The type of license the Windows operating system uses, either Per server or Per seat . See Microsoft Licensing ^[2] for more information.
Concurrent connections	When using a Per server license mode, the Concurrent connections value specifies how many users can access the Windows machine at a time.

Delete Snapshot

The **Delete Snapshot** activity deletes a saved virtual machine snapshot from a vCenter server. This activity is available starting with the Eureka release.

Results

- **Success:** the snapshot was successfully deleted.
- **Failure:** an error occurred while attempting to delete the snapshot. Additional details may be available in the workflow log.
- **Not Found:** the specified snapshot was not found on the vCenter server.

Input Variables

These variables determine the behavior of the activity.

Field	Description
vCenter	IP address of the vCenter server that stores the snapshot to delete.
VM uuid	The VMware universal unique identifier assigned to the virtual machine storing the snapshot to delete. If you are creating your own workflow, see Virtual Machine UUID for instructions on properly formatting the unique identifier.
Snapshot MOR id	The managed object reference ID of the snapshot to delete.

Destroy

The **Destroy** activity sends a command to vCenter to destroy the named VMware virtual machine. This activity deletes the virtual machine and removes it from the disk.

Input Variables

These variables determine the behavior of the activity.

Field	Description
vCenter	IP address of the vCenter server that manages the virtual machine to destroy.
VM uuid	The VMware universal unique identifier assigned to this virtual machine. If you are creating your own workflow, see Virtual Machine UUID for instructions on properly formatting the unique identifier.

Get VM Events

The **Get VM Events** activity retrieves the most recent events for a virtual machine. This activity stores the retrieved event information in the `events` sensor script variable as an array of JavaScript objects. Each object in this array contains these fields:

- **classname:** The class of the event generated by the vCenter.
- **message:** The event text.
- **time:** The timestamp when the event occurred.

This activity is available starting with the Eureka release.

Input Variables

These variables determine the behavior of the activity.

Field	Description
vCenter	IP address of the vCenter server that manages the virtual machine from which you want to retrieve events.
VM uuid	The VMware universal unique identifier assigned to this virtual machine. If you are creating your own workflow, see Virtual Machine UUID for instructions on properly formatting the unique identifier.
Max events	The maximum number of events to retrieve from the virtual machine. The activity returns at most 15 events if you do not specify a value.

Get VM Guest Info

The **Get VM Guest Info** activity retrieves the guest customization information for a virtual machine. This activity stores the returned information in these sensor script variables:

- **hostname:** The host name of the virtual machine.
- **state:** The power state of the virtual machine.
- **ip:** An array of strings that lists the IPv6 and IPv4 addresses of the virtual machine.

This activity is available starting with the Eureka release.

Input Variables

These variables determine the behavior of the activity.

Field	Description
vCenter	IP address of the vCenter server that manages the virtual machine from which you want to retrieve guest customization information.
VM uuid	The VMware universal unique identifier assigned to this virtual machine. If you are creating your own workflow, see Virtual Machine UUID for instructions on properly formatting the unique identifier.

Reconfigure

The **Reconfigure** activity updates the number of CPUs and the amount of memory assigned to a virtual machine.

Input Variables

These variables determine the behavior of the activity.

Field	Description
vCenter	IP address of the vCenter server that manages the virtual machine to operate.
VM uuid	The VMware universal unique identifier assigned to this virtual machine. If you are creating your own workflow, see Virtual Machine UUID for instructions on properly formatting the unique identifier.
Number of CPUs	The number of CPUs to allocate to the virtual machine. If this field is blank, you must reconfigure the memory for this virtual machine.
Memory (MB)	The amount of memory, in megabytes, to allocate to the virtual machine. If this field is blank, you must reconfigure the number of CPUs for this virtual machine. This value must be divisible by 4. If the amount is not divisible by 4, the activity succeeds but the virtual machine cannot start.

Revert to Snapshot

The **Revert to Snapshot** activity reverts a virtual machine to the state captured in a given snapshot.

Input Variables

These variables determine the behavior of the activity.

Field	Description
vCenter	IP address of the vCenter server that manages the virtual machine for which the snapshot was created.
VM uuid	The VMware universal unique identifier assigned to the virtual machine from which the snapshot was created. If you are creating your own workflow, see Virtual Machine UUID for instructions on properly formatting the unique identifier.
Snapshot name	Unique name of the snapshot.
Snapshot MOR id	Reverts the virtual machine to the snapshot with this ManagedObjectReference ID. If this variable is present, the workflow ignores the Snapshot name .

Snapshot

The **Snapshot** activity creates a snapshot of a virtual machine. A snapshot stores the current state of a virtual machine, but is not a full backup.

Input Variables

These variables determine the behavior of the activity.

Field	Description
vCenter	IP address of the vCenter server that manages the virtual machine for which you want to create a snapshot.
VM uuid	The VMware universal unique identifier assigned to the virtual machine from which the snapshot is created. If you are creating your own workflow, see Virtual Machine UUID for instructions on properly formatting the unique identifier.
Snapshot name	Unique name of the snapshot.
Snapshot description	Description that distinguishes this snapshot from other snapshots of the same virtual machine.
Scratchpad variable	The scratchpad variable to store the returned snapshot ID. You can use this snapshot ID in the Snapshot MOR id variable for the Revert to Snapshot and Delete Snapshot activities. This variable is available starting with the Eureka release.

Select Datacenter, Network, and Folder

The **Select Datacenter, Network, and Folder** activity is deprecated starting with the Eureka release. Datacenter, network, and folder selection is handled by extension points.

Versions Prior to the Eureka Release

Click the plus to expand previous version information

The **Select Datacenter, Network, and Folder** activity selects a vCenter datacenter, network, and folder for a virtual machine (VM) being provisioned. The activity makes these selections by applying virtual machine *provisioning rules* to the vCenter instance (inferred from the VMware template selected by the requester) and the VM category (selected by the requester).

Configure the provisioning rules before allowing any workflow that uses this activity to run. See Provisioning Rules for a detailed explanation of this process. The activity must read and process the provisioning rules to configure the correct datacenter, network, and folder.

Input Variables

These variables determine the behavior of the activity.

Name	Description
vCenter	The sys_id of the vCenter to use.
Category	The sys_id of the category to use.

Scratchpad Entries

The activity writes this data to the workflow scratchpad:

Property Name	Contents
selections.datacenter	The sys_id of the vCenter datacenter selected.
selections.network	The sys_id of the vCenter network selected.
selections.folder	The sys_id of the vCenter folder selected.
error	A human-readable error message describing exactly what went wrong. This property is set only when this activity fails for any reason.

Select ESX Host and Datastore

The **Select ESX Host and Datastore** activity is deprecated starting with the Eureka release. ESX host and datastore selection is handled by extension points.

Versions Prior to the Eureka Release

Click the plus to expand previous version information

The **Select ESX Host and Datastore** activity selects a specific ESX host and a vCenter datastore for a virtual machine (VM) being provisioned. The algorithm selects the combination of ESX host and datastore that can host the virtual machine with the least possible impact to the virtual hosting infrastructure.

Input Variables

These variables determine the behavior of the activity.

Name	Description
Template	The sys_id of the template to be provisioned.

Scratchpad Entries

The activity requires this scratchpad data to run:

Property Name	Contents
selections	A JavaScript object.
selections.vCenter	The sys_id of the vCenter from which to select an ESX host and datastore. This value is generally inferred from the template by the <i>Select Datacenter, Network, and Folder</i> activity described in this page.
selections.datacenter	The sys_id of the vCenter datacenter from which to select an ESX host and datastore. This value is generally set by the <i>Select Datacenter, Network, and Folder</i> activity.

The activity writes this data to the workflow scratchpad:

Property Name	Contents
selections.esx	The sys_id of the vCenter ESX host selected.
selections.datastore	The sys_id of the vCenter datastore selected.
selections.cluster	The sys_id of the selected vCenter cluster of which the selected ESX host is a member, or <i>null</i> if the selected ESX host is not a member of any cluster.
error	A value is set in this property only when this activity fails for any reason. It displays a human-readable error message describing exactly what went wrong.

Selection Algorithm

The ESX host and datastore selection algorithm makes use of *normalized metrics*, sometimes called figures of merit [3]. For each object being measured, the result is expressed as a number between 0 and 1 (that's the *normalized* part). Anything expressed as a percentage is a normalized metric. A glass that's half full of milk is 50% full, as is a 10,000 liter fuel storage tank containing 5,000 liters of fuel. Even though they are vastly different in capacity, the *fullness* of those two vessels has been normalized as 50% full. This selection algorithm makes use of similar normalized metrics.

For each possible combination of ESX host and vCenter datastore, the algorithm computes three normalized metrics:

- **Storage metric:** If the sum of all the storage configured for all virtual machines on a datastore, plus the storage needed for the virtual machine being provisioned, is less than the capacity of the datastore, then this metric has a value of **1**. Often the possible storage consumption on all virtual machines configured on a datastore is greater than the actual capacity of the datastore. This occurs because the virtual hosting environment administrators take advantage of the fact that most virtual machines do not use the storage capacity for which they are configured. The selection algorithm detects this case and computes a metric value that is closer to **0** for datastores that are more over-allocated, and closer to **1** for datastores that are less over-allocated.
- **Compute metric:** Generally, the sum of the CPUs allocated for all virtual machines running on an ESX host exceeds (sometimes *greatly* exceeds) the number of cores physically present on the ESX host. This occurs because virtual hosting environment administrators take advantage of the fact that most virtual machines spend most of their time idling. This algorithm computes a CPU metric that is closer to **0** for ESX hosts that are more over-allocated for CPUs, and closer to **1** for ESX hosts that are less over-allocated.
- **Memory metric:** Generally, the sum of the memory (RAM) allocated for all virtual machines running on an ESX host exceeds (sometimes *greatly* exceeds) the amount of memory physically present on the ESX host. This occurs because virtual hosting environment administrators take advantage of the fact that most virtual machines use less memory than is allocated for them. This algorithm computes a memory metric that is closer to **0** for ESX hosts that are more over-allocated for memory, and closer to **1** for ESX hosts that are less over-allocated.

Each of these metrics is then adjusted by a *weighting factor*, which can be any number greater than or equal to zero. By default, the weighting factor is **1**, which means that all three normalized metrics (storage, compute, and memory) are treated as equally important. You can adjust these weighting factors in any fashion to make a particular metric either more or less important in the overall ESX host and datastore selection process. The closer a weighting factor is to **0**, the *more* important that particular metric will be in the selection. Conversely, the more a weighting factor is greater than **1**, the less important that particular metric will be in the selection. From a purely mathematical perspective, the raw metric is raised to the power of the weighting factor to obtain the weighted metric. Since the raw metric is a number in the interval [0,1], the result (for any positive power) is also in the interval [0,1].

These weighting factors are controlled by three properties:

Weighting Factor	Property Name
Storage	<code>glide.vmware.provisioning.storage_weight</code>
Compute	<code>glide.vmware.provisioning.compute_weight</code>
Memory	<code>glide.vmware.provisioning.memory_weight</code>

When each of these metrics is calculated for the possible combinations of ESX host and vCenter datastore, the metrics are multiplied together to get an overall normalized metric for that particular ESX host and datastore combination. The result of this multiplication is always a number between **0** and **1** (inclusive, in the interval [0,1]). The ESX host and the datastore combination with the largest overall normalized metric are the ones selected by this activity.

Select IP Address

The **Select IP Address** activity is deprecated starting with the Eureka release. IP address selection is handled by extension points.

Versions Prior to the Eureka Release

Click the plus to expand previous version information

The **Select IP Address** activity selects an IP address for a virtual machine (VM) being provisioned. The selection is made by finding the IP pool available to the selected vCenter network that has the most unused IP addresses remaining, and then randomly selecting and allocating an unused IP address from that IP pool. IP pools must be assigned before this activity runs in a workflow.

Scratchpad Entries

The activity requires this scratchpad data to run:

Property Name	Contents
<code>selections</code>	A JavaScript object.
<code>selections.network</code>	The <code>sys_id</code> of the vCenter network selected. Generally, this is set by the Select Datacenter, Network, and Folder activity.

The activity writes these properties to the workflow scratchpad:

Property Name	Contents
<code>selections.ip</code>	The IP address selected, in dotted-decimal form such as 10.54.228.62 .
<code>selections.netmask</code>	The netmask of the selected IP address.
<code>selections.dns</code>	The IP Address of the DNS server associated with the selected IP address.
<code>selections.gateway</code>	The gateway used by the selected IP address.
<code>selections.pool_id</code>	The <code>sys_id</code> value of the IP pool that contains the selected IP address.
<code>error</code>	A value is set in this property only when this activity fails for any reason. The property then contains a human-readable error message describing exactly what went wrong.

Select Name

The **Select Name** activity is deprecated starting with the Eureka release. Name selection is handled by extension points.

Versions Prior to the Eureka Release

Click the plus to expand previous version information

The **Select Name** activity selects a name for a virtual machine (VM) being provisioned. This one name is used for both the host name and the DNS name. The following algorithm determines the selection:

- If a preferred name is supplied, and if that name is available (not already a host name, DNS name, or VMware image name), then the preferred name is selected and this activity finishes.
- If a preferred name is supplied but is not available, the activity appends a hyphen (-) and the requester's initials to the original preferred name. If that modified preferred name is available, then the activity uses the modified preferred name and finishes. For example, if the preferred name supplied was **Dev**, and the user making the request was Athena Fontanilla, then you would use **Dev-af** as the modified preferred name. This activity uses the `current.opened_by` variable to identify the user who made the service catalog request that caused the workflow containing this activity to run.
- If no preferred name was supplied, or if neither the preferred name nor the modified preferred name is available, the activity uses the base name specified in the VM template, the requester's initials, and a sequence number, each separated by hyphens (-). These are combined with increasing sequence numbers until an available name is found. When an available name is found, the activity selects that name and finishes. For example, if the base name in the VM template was **Test**, and the user making the request was John Smith, then the very first name tried might be **Test-js-4**. If that name was not available, the next name checked would be **Test-js-5**. This process continues until an available name is found. If the VM template does not have a base name configured, the activity uses the name **global**.

You can replace the default algorithm, by using the VM template to configure a different script include to use instead of the default VMnamer script include. This alternative script include must have an `initialize` method and a `process` method with the same arguments and return values as the VMnamer script include. However, the replacement script can use any algorithm desired to generate the names.



Note: Developers might find it convenient to use the script include VMnumbers to generate sequence numbers for arbitrary base names. You may also find it convenient to extend VMnamer to override the `process` method, to use the other methods defined there in your own script include.

Input Variables

These variables determine the behavior of the activity.

Name	Description
Template	The sys_id of the template to be provisioned.
Preferred Name	An optional name that is preferred by the requester. If the preferred name is supplied and available, that name or a variant is selected. See the algorithm description, above.

Scratchpad Entries

The activity writes this data to the workflow scratchpad.

Property Name	Contents
selections.name	The name selected for the VM being provisioned.
error	A value is set in this property only when this activity fails for any reason. The property then contains a human-readable error message describing exactly what went wrong.

References

- [1] <http://blogs.vmware.com/vsphere/2012/02/uniquely-identifying-virtual-machines-in-vsphere-and-vcloud-part-1-overview.html>
- [2] <http://www.microsoft.com/licensing/>
- [3] http://en.wikipedia.org/wiki/Figure_of_merit

Article Sources and Contributors

Orchestration VMware Support Plugin *Source:* <http://wiki.servicenow.com/index.php?oldid=191570> *Contributors:* Cheryl.dolan, David.Bailey, Joseph.messerschmidt, Roy.lagemann, Steven.wood

Requesting a Virtual Server - Versions Prior to Calgary *Source:* <http://wiki.servicenow.com/index.php?oldid=191549> *Contributors:* Cheryl.dolan, Davida.hughes, Joseph.messerschmidt, Steven.wood

Configuring VMware - Versions Prior to Calgary *Source:* <http://wiki.servicenow.com/index.php?oldid=232479> *Contributors:* Cheryl.dolan, David.Bailey, George.rawlins, Joseph.messerschmidt, Steven.wood

Accessing the vCenter API - Versions Prior to Calgary *Source:* <http://wiki.servicenow.com/index.php?oldid=191627> *Contributors:* Cheryl.dolan, Joseph.messerschmidt, Neola, Steven.wood

ESX Resource Pools - Versions Prior to Calgary *Source:* <http://wiki.servicenow.com/index.php?oldid=245664> *Contributors:* Cheryl.dolan, Joseph.messerschmidt, Steven.wood

VMware Templates - Versions Prior to Calgary *Source:* <http://wiki.servicenow.com/index.php?oldid=233740> *Contributors:* Cheryl.dolan, David.Bailey, Joseph.messerschmidt, Steven.wood

MID Server Plugin *Source:* <http://wiki.servicenow.com/index.php?oldid=89866> *Contributors:* Aburruss, Bow, CapaJC, Cheryl.dolan, Christen.mitchell, Chuck.tomasi, Dan.sherwin, David Loo, David.Bailey, Dawn.bunting, Doogiesd, Fuji.publishing.user, G.yedwab, Guy.yedwab, Jeremiah.hall, John.andersen, John.ramos, John.roberts, Joseph.messerschmidt, Mark.odonnell, Neola, Phillip.salzman, Publishing.user, Rob.woodbyrne, Steven.wood, Tom.dilatush, Vaughn.romero, Vhearne

Requirements *Source:* <http://wiki.servicenow.com/index.php?oldid=250733> *Contributors:* Bow, CapaJC, David Loo, Dawn.bunting, Doogiesd, Fuji.publishing.user, Gadi.yedwab, Guy.yedwab, John.ramos, Joseph.messerschmidt, Phillip.salzman, Rob.woodbyrne, Steven.wood, Valor, Vaughn.romero, Vhearne, Virginia.kelley

Installation *Source:* <http://wiki.servicenow.com/index.php?oldid=250732> *Contributors:* John.ramos, Joseph.messerschmidt, Katharine.sohler, Mary.stromberg, Phillip.salzman, Publishing.user, Rachel.sienko, Steven.wood, Vaughn.romero, Virginia.kelley

Configuration *Source:* <http://wiki.servicenow.com/index.php?oldid=250729> *Contributors:* Aleck.lin, Bow, Cheryl.dolan, David.Bailey, Dawn.bunting, Emily.partridge, Fuji.publishing.user, Guy.yedwab, Jim.holthaus, John.ramos, Joseph.messerschmidt, Phillip.salzman, Publishing.user, Steven.wood, Tom.dilatush, Vaughn.romero, Vhearne, Virginia.kelley, Voytek.blonski

MID Server Clusters *Source:* <http://wiki.servicenow.com/index.php?oldid=250328> *Contributors:* Anat.kerry, Dawn.bunting, Fuji.publishing.user, John.ramos, Joseph.messerschmidt, Phillip.salzman, Steven.wood

Autofinder *Source:* <http://wiki.servicenow.com/index.php?oldid=248932> *Contributors:* Joseph.messerschmidt, Steven.wood

Approving and Provisioning VMware Requests - Versions Prior to Calgary *Source:* <http://wiki.servicenow.com/index.php?oldid=232376> *Contributors:* Cheryl.dolan, David.Bailey, Fuji.publishing.user, Jennifer.ball, Joseph.messerschmidt, Steven.wood

VMware Component Relationships *Source:* <http://wiki.servicenow.com/index.php?oldid=249549> *Contributors:* Aleck.lin, Joseph.messerschmidt, Phillip.salzman, Steven.wood

VMware Workflow Activities *Source:* <http://wiki.servicenow.com/index.php?oldid=191773> *Contributors:* Cheryl.dolan, David.Bailey, Emily.partridge, George.rawlins, Jimmy.yuan, Joe.Westrich, Joseph.messerschmidt, Steven.wood, Vaughn.romero

Image Sources, Licenses and Contributors

Image:Warning.gif *Source:* <http://wiki.servicenow.com/index.php?title=File:Warning.gif> *License:* unknown *Contributors:* CapaJC

Image:VM_Service_Catalog1.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Service_Catalog1.png *License:* unknown *Contributors:* Steven.wood

Image:VM_Service_Catalog2.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Service_Catalog2.png *License:* unknown *Contributors:* Steven.wood

Image:VM_Service_Catalog3.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Service_Catalog3.png *License:* unknown *Contributors:* Steven.wood

Image:VM_Service_Catalog4.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Service_Catalog4.png *License:* unknown *Contributors:* Steven.wood

Image:VM_Service_Catalog5.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Service_Catalog5.png *License:* unknown *Contributors:* Steven.wood

Image:VM_ESX_Server_Calgary.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_ESX_Server_Calgary.png *License:* unknown *Contributors:* Steven.wood

Image:VM_vCenter_Calgary.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_vCenter_Calgary.png *License:* unknown *Contributors:* Steven.wood

Image:cp_vm_ip_pool_config.png *Source:* http://wiki.servicenow.com/index.php?title=File:Cp_vm_ip_pool_config.png *License:* unknown *Contributors:* George.rawlins

Image:cp_ip_pool_allocation2.png *Source:* http://wiki.servicenow.com/index.php?title=File:Cp_ip_pool_allocation2.png *License:* unknown *Contributors:* George.rawlins

Image:VM_IP_Pool2.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_IP_Pool2.png *License:* unknown *Contributors:* Steven.wood

Image:VM_Config_Windows_Eur.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Config_Windows_Eur.png *License:* unknown *Contributors:* George.rawlins

Image:VM_Config_Windows_Calgary.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Config_Windows_Calgary.png *License:* unknown *Contributors:* Joseph.messerschmidt, Steven.wood

Image:VM_Config_Linux_Eur.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Config_Linux_Eur.png *License:* unknown *Contributors:* George.rawlins

Image:VM_Approval_Group_Calgary.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Approval_Group_Calgary.png *License:* unknown *Contributors:* Steven.wood

Image:VM_Size_Definition.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Size_Definition.png *License:* unknown *Contributors:* Steven.wood

File:VM_Price.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Price.png *License:* unknown *Contributors:* Steven.wood

Image:VM_CPU_Select_Calgary.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_CPU_Select_Calgary.png *License:* unknown *Contributors:* Steven.wood

Image:VM_Memory_Select_Calgary.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Memory_Select_Calgary.png *License:* unknown *Contributors:* Steven.wood

Image:VM_Disk_Size_Select_Calgary.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Disk_Size_Select_Calgary.png *License:* unknown *Contributors:* Steven.wood

File:Lease_Duration_Diagram.png *Source:* http://wiki.servicenow.com/index.php?title=File:Lease_Duration_Diagram.png *License:* unknown *Contributors:* Steven.wood

File:VM_Lease_End_Workflow.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Lease_End_Workflow.png *License:* unknown *Contributors:* Steven.wood

Image:cp_datastores_eur.png *Source:* http://wiki.servicenow.com/index.php?title=File:Cp_datastores_eur.png *License:* unknown *Contributors:* George.rawlins

Image:Knowledge.gif *Source:* <http://wiki.servicenow.com/index.php?title=File:Knowledge.gif> *License:* unknown *Contributors:* G.yedwab, Joseph.messerschmidt, Publishing.user

Image:RBA_VMWare_Privileges1.png *Source:* http://wiki.servicenow.com/index.php?title=File:RBA_VMWare_Privileges1.png *License:* unknown *Contributors:* Steven.wood

Image:RBA_VMWare_Privileges2.png *Source:* http://wiki.servicenow.com/index.php?title=File:RBA_VMWare_Privileges2.png *License:* unknown *Contributors:* Steven.wood

Image:RBA_VMWare_Privileges3.png *Source:* http://wiki.servicenow.com/index.php?title=File:RBA_VMWare_Privileges3.png *License:* unknown *Contributors:* Steven.wood

Image:RBA_VMWare_Privileges4.png *Source:* http://wiki.servicenow.com/index.php?title=File:RBA_VMWare_Privileges4.png *License:* unknown *Contributors:* Steven.wood

Image:VM_ESX_Resource_Pool.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_ESX_Resource_Pool.png *License:* unknown *Contributors:* Steven.wood

Image:VM_Template_Record_Calgary.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Template_Record_Calgary.png *License:* unknown *Contributors:* Steven.wood

Image:JAR_File_Sync.png *Source:* http://wiki.servicenow.com/index.php?title=File:JAR_File_Sync.png *License:* unknown *Contributors:* Steven.wood

Image:mid_server_menu.png *Source:* http://wiki.servicenow.com/index.php?title=File:Mid_server_menu.png *License:* unknown *Contributors:* Vaughn.romero

Image:MID_Server_Download_Dublin.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Download_Dublin.png *License:* unknown *Contributors:* Vaughn.romero

Image:MID_config.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_config.png *License:* unknown *Contributors:* Steven.wood, Tom.dilatush

Image:MID_config.xml.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_config.xml.png *License:* unknown *Contributors:* Tom.dilatush

Image:MID_Server_Script_File_Sync.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Script_File_Sync.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_Script_File_Sync2.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Script_File_Sync2.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_Unblock_Config.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Unblock_Config.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_Clusters_Diagram.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Clusters_Diagram.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_Cluster1.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Cluster1.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_IP_Range1.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_IP_Range1.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_IP_Range2.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_IP_Range2.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_IP_Range3.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_IP_Range3.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_Resolve_DNS.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Resolve_DNS.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_Capability2.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Capability2.png *License:* unknown *Contributors:* Steven.wood

Image:MID_Server_Capability3.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_Server_Capability3.png *License:* unknown *Contributors:* Steven.wood

Image:RBA_MID_Server_Property.png *Source:* http://wiki.servicenow.com/index.php?title=File:RBA_MID_Server_Property.png *License:* unknown *Contributors:* Joseph.messerschmidt, Steven.wood

Image:MID_SetDefault.png *Source:* http://wiki.servicenow.com/index.php?title=File:MID_SetDefault.png *License:* unknown *Contributors:* Joseph.messerschmidt

Image:VM_Approvals3.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Approvals3.png *License:* unknown *Contributors:* Steven.wood

File:VMware_Catalog_Task.png *Source:* http://wiki.servicenow.com/index.php?title=File:VMware_Catalog_Task.png *License:* unknown *Contributors:* Steven.wood

File:VM_Provisioning_Rule.png *Source:* http://wiki.servicenow.com/index.php?title=File:VM_Provisioning_Rule.png *License:* unknown *Contributors:* Neil.narvaez, Steven.wood

Image:VMWare_VCenter_Diagram.png *Source:* http://wiki.servicenow.com/index.php?title=File:VMWare_VCenter_Diagram.png *License:* unknown *Contributors:* Steven.wood

Image:VMWare_No_VCenter_Diagram.png *Source:* http://wiki.servicenow.com/index.php?title=File:VMWare_No_VCenter_Diagram.png *License:* unknown *Contributors:* Steven.wood