pool, which balances the monitoring load of your management group as new management servers are added, and provides automatic failover for monitoring. The impact of failure of a management server in a distributed environment is minimized, but it increases the workload on additional management servers in the management group until the failed management server is restored. See [Distributed Deployment of Operations Manager](#ze9b6f0678f3e465e9a0ff3ae46859bd6) in the Deployment Guide for complete details.

You should always keep a backup of your operational database and data warehouse databases. For information about scheduling regular backups of the Operations Manager databases, see [How to Schedule Backups of System Center 2012 - Operations Manager Databases](#z301b7af3369541b5b91ce1a672bce591).

You must keep SDK services running on all management servers.

See Also

[Operations Manager Sizing Helper](http://go.microsoft.com/fwlink/?LinkId=231853)

Deploying System Center 2012 - Operations Manager

All System Center 2012 – Operations Manager individual management group deployments will either be an "all-in-one" installation, where all features are loaded on a single server, or the deployment will be a distributed installation, where Operations Manager features are distributed across servers. Any number of these can then be combined together to form an overall Operations Manager infrastructure that consists of multiple management groups. These management groups can then relate to each other in a hierarchical fashion as your business needs dictate.

This section of the Deployment Guide describes an individual management group deployment, where you have one management group, but the features of Operations Manager are either installed on a single server or distributed over several servers.

 [Single-Server Deployment of Operations Manager](#z6a3bd68b89564703baddf93170c23054)

 [Distributed Deployment of Operations Manager](#ze9b6f0678f3e465e9a0ff3ae46859bd6)

For information about connecting management groups, see [Connecting Management Groups in Operations Manager](http://go.microsoft.com/fwlink/p/?LinkID=207755).

Before You Begin

Before you begin your deployment, you should read the release notes, and ensure that your server meets the minimum system requirements for Operations Manager. For more information, see:

 [Release Notes for System Center 2012 - Operations Manager](http://go.microsoft.com/fwlink/p/?LinkId=246973)

 [System Requirements for System Center 2012 – Operations Manager](http://go.microsoft.com/fwlink/p/?LinkID=219650)

Operations Manager Administrators Role Assignment

Operations Manager handles assignment of the Operations Manager Administrators role differently than previous versions. In System Center 2012 – Operations Manager, Setup automatically assigns the Administrators group on the local computer to the Operations Manager Administrators role. You must be logged on with an account that has local Administrator rights to run Setup on the first management server that you install; this ensures that you can open the Operations console after Setup is completed. When you install additional management servers, you must use a Domain account of which you are a member.

Required Accounts

During setup, you are prompted for two accounts, the management server action account and the System Center Configuration service and System Center Data Access service account. In Operations Manager, you can use the same account for both services.

If you install Reporting, you are prompted for two additional accounts, the Data Warehouse Write account and the Data Reader account. These accounts are created as domain user accounts and added to the local Administrators group on the target server.

Note

If you create a specific account for installation, this account must be a member of the sysadmin server role for Microsoft SQL Server, but also have access to the master database.

Note

If you install multiple management servers, you are prompted for a management server action account and a System Center Configuration service and System Center Data Access service account each time you add a management server. You must provide the same accounts for each installation.

|  |  |  |
| --- | --- | --- |
| Account | Description | Permissions |
| Management server action account | This account is used to carry out actions on monitored computers across a network connection. | To save time, specify a domain-based account. We recommend that you create an account for this purpose that has local administrative credentials. You should not use an account that has domain administrative credentials. |
| System Center Configuration service and System Center Data Access service account | This account is one set of credentials that is used to update and read information in the operational database. Operations Manager ensures that the credentials used for the System Center Data Access service and System Center Configuration service account are assigned to the sdk\_user role in the operational database. | This account can be configured as either Local System or as a domain account. The account must have local administrative credentials. For cases where the operational database is hosted on a remote computer that is not a management server, a domain account must be used. For better security, we recommend that you use an account different from the one used for the management server action account. |
| Data Warehouse Write account | The Data Warehouse Write account writes data from the management server to the Reporting data warehouse and reads data from the operational database. | This account is assigned write permissions on the Data Warehouse database and read permissions on the operational database.  Note  Ensure that the account you plan to use for the Data Warehouse Write account has SQL Server Logon rights and has logon rights for the computers hosting both the operational database and the reporting data warehouse. Otherwise, Setup fails, and all changes are rolled back. This might leave SQL Server Reporting Services in an inoperable state. |
| Data Reader account | The Data Reader account is used to define which account credentials SQL Server Reporting Services uses to run queries against the Operations Manager reporting data warehouse. | The account should be configured as a domain account.  Note  Ensure that the account you plan to use for the Data Reader account has SQL Server logon rights and Management Server logon rights. |

SQL Server Requirements

System Center 2012 – Operations Manager requires access to an instance of a server running Microsoft SQL Server 2008 SP1, SQL Server 2008 R2, or SQL Server 2008 R2 SP1. This instance can be located on a separate computer from the management servers in a distributed installation or on the first management server in the management group. In either case, the instance of Microsoft SQL Server 2008 SP1, SQL Server 2008 R2, or SQL Server 2008 R2 SP1 must already exist and be accessible before you start your first management server installation. The SQL Server Collation setting must be a supported value, and SQL Full Text Search must be enabled.

System Center 2012 Service Pack 1 (SP1), Operations Manager requires access to an instance of a server running Microsoft SQL Server 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1. This instance can be located on a separate computer from the management servers in a distributed installation or on the first management server in the management group. In either case, the instance of Microsoft SQL Server 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1 must already exist and be accessible before you start your first management server installation. The SQL Server Collation setting must be a supported value, and SQL Full Text Search must be enabled.

During setup, you are prompted for the following:

 The SQL Server database server name and instance name. If you have installed SQL Server by using the default instance, you only have to specify the SQL Server name.

You can accept the default values for or set:

 SQL Server Port number. By default, 1433.

 A new operational database (for first management server installation in the management group) or an existing operational database (for installing additional management servers in an existing management group).

 The database name. By default, OperationsManager.

 The starting database size. By default, 1000 MB.

 The Data file and Log folder locations. By default, these are C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Data or C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\Log as appropriate to the SQL Server defaults.

Important

If TCP/IP is disabled on a remote server that is hosting the SQL Server database, Setup will not be able to connect to the SQL Server database. To resolve this issue, enable TCP/IP on the remote server.

Ensure that SQL Server Reporting Services has been correctly installed and configured. For more information about how to install and configure SQL Server 2012 Reporting Services, see [SQL Server Installation (SQL Server 2008 R2)](http://go.microsoft.com/fwlink/p/?LinkId=146943).

See Also

[Deploying System Center 2012 - Operations Manager](#z969a31d65ef241279cfe0af66c981b6c)

Environmental Prerequisites for Operations Manager

This section covers the infrastructure that you need to have in place and other factors to consider before you run the Setup for System Center 2012 – Operations Manager or System Center 2012 Service Pack 1 (SP1), Operations Manager.

There are two sets of prerequisites that must be satisfied prior to installing any of the Operations Manager features. One set consists of those items that the Prerequisite checker identifies during Setup. The Prerequisite checker is targeted at the server that Setup is running on and determines if the server has the necessary configuration to host whatever role you have chosen.

The other set consists of those items that are outside the scope of the Prerequisite checker, such as the Active Directory domain or forest functional level, or the availability of a certification authority (CA) to issue the certificates that are necessary for deploying agents and gateway servers across trust boundaries. This section addresses this second set of prerequisites, which are much broader in scope, because they apply to the whole environment that Operations Manager will be functioning in, rather than those that are verified by the Prerequisite checker during Setup. To ensure that Operations Manager deploys smoothly and functions as expected, the environment that it will run in must be properly prepared. Because environmental changes affect more than Operations Manager, ensure that you exercise due caution before making sweeping changes. The prerequisites are presented in a unified format with scenario-specific items called out.

For more information about design and environmental decisions, see [Planning the System Center 2012 - Operations Manager Deployment](#zd6edb9b45db840c2be00a32445732d50). For more information about supported configurations for System Center 2012 – Operations Manager, see [System Requirements for System Center 2012 – Operations Manager](http://go.microsoft.com/fwlink/p/?LinkID=219650).

In This Section

[Supporting Infrastructure](#z9c9c8c720fa546ff8abe67dca0b27ee5)

|  |
| --- |
| Describes prerequisites and issues that you need to be aware of before you install System Center 2012 – Operations Manager. |

[Security Considerations](#z9c0f4ce08cfc499497e45e0e29c1b6c5)

|  |
| --- |
| Describes high-level security factors that need to be addressed. |

[Agent and Agentless Monitoring](#z504958dff85349f2b27a795948234220)

|  |
| --- |
| Describes the environmental prerequisites for deploying agents to monitor devices and for deploying agentless monitoring. |

Supporting Infrastructure

This section addresses prerequisites and issues involving Active Directory Domain Services (AD DS) and Domain Name System (DNS) that you need to be aware of before initiating your System Center 2012 – Operations Manager installation.

Active Directory Domain Services

System Center 2012 – Operations Manager relies on AD DS for a number of services, including definition of security principles, rights assignment, authentication, and authorization. Operations Manager queries AD DS when performing computer and service discovery and can use AD DS for storing and distributing agent configuration information. For Operations Manager to function properly, AD DS and its supporting service, DNS, need to be healthy and at certain minimum configuration levels. In addition, certain domain naming conventions must be followed.

Domain Space Naming

An Operations Manager management group cannot be installed into a root Active Directory domain that has a flat DNS namespace. However, you can install the management group into child domains of the root domain. For example, you have a root domain that has a DNS name of "Woodgrove". Because this root domain has a flat DNS namespace, you cannot install an Operations Manager management group into the Woodgrove domain. But, if the Woodgrove domain has a child domain with a DNS name of "National", the fully qualified domain name of the child domain would be national.woodgrove. For more information about configuring Windows for domains with single-label DNS names, see [Information about configuring Active Directory domains by using single-label DNS names](http://go.microsoft.com/fwlink/p/?LinkID=160783).

Domain Functional Level

Windows Server Active Directory can operate at different functional levels. These levels are distinguished by the version of the Windows Server operating system that is permitted on the domain controllers present in the domain. System Center 2012 – Operations Manager requires that the domain functional level be Windows 2000 native, Windows Server 2003 interim, Windows Server 2003, or Windows Server 2008. The domain functional level of Windows Server 2008 R2 is also supported (for the SP1 version of System Center 2012 – Operations Manager, Windows Server 2008 R2 SP1 and Windows Server 2012 are supported). For System Center 2012 – Operations Manager to function properly, you must check the domain functional level and raise it to the appropriate version. To do this, see [Raise the Domain Functional Level](http://go.microsoft.com/fwlink/p/?LinkId=232554).

Note

Ensure that you exercise due caution prior to raising a domain's functional level because it cannot be reversed, and if there are any down-level domain controllers, their function will be impacted.

Forest Functional Level

The forest functional level is similar to the domain functional level in that it sets a minimum domain controller operating system level across the whole forest. After it is set, domain controllers with down-level operating systems from lower functional levels cannot be introduced into the forest. Operations Manager does not have a forest functional level requirement; however, if the forest functional level is left at the default Windows 2000 level, there may be domains in your forest that won't meet the minimum domain functional level requirement.

DNS

DNS must be installed and in a healthy state to support AD DS. Beyond the reliance of Operations Manager on AD DS, there are no specific DNS requirements.

See Also

[Environmental Prerequisites for Operations Manager](#z95d59f735aa94616b98c30680406959a)

Security Considerations

Most of the work in preparing the environment for System Center 2012 – Operations Manager goes into security-related tasks. This section covers those tasks at a cursory level. For more information, see the [Index to Security-related Information for Operations Manager](http://go.microsoft.com/fwlink/p/?LinkId=244660).

Preparing the security-related tasks involves the following:

 Understanding, planning, and preparing for monitoring across trust boundaries.

 Understanding, planning, and preparing for monitoring UNIX or Linux computers.

 Planning and preparing the service accounts, user accounts, and security groups that you will need.

 Understanding and preparing the network ports as required by your design.

Trust Boundaries

Active Directory domains form the basic unit of a Kerberos trust boundary as seen by Operations Manager. This boundary is automatically expanded to other domains in the same name space (the same Active Directory tree), and between domains that are in different Active Directory trees but still in the same Active Directory forest via transitive trusts. The trust boundary can be further expanded between domains in different Active Directory forests through the use of across forest trusts.

Kerberos

The Kerberos authentication protocol, which is supported by Windows 2000 domain controllers and above, can only occur within a trust boundary. Kerberos authentication is the mechanism used to perform the Operations Manager agent/server mutual authentication. Agent/server mutual authentication is mandated in Operations Manager Shell for all agent/server communication.

An Operations Manager management group does have the ability to perform discovery and monitoring outside of the Kerberos trust boundary that it is in. However, because the default authentication protocol for Windows-based computers that are not joined to an Active Directory domain is NTLM, another mechanism must be used to support mutual authentication. This is done through the exchange of certificates between agents and servers.

Certificates

When Operations Manager communication needs to occur across trust boundaries, such as when a server that you want to monitor lies in a different, untrusted, Active Directory domain than the management group that is performing the monitoring, certificates can be used to satisfy the mutual authentication requirement. Through manual configuration, certificates can be obtained and associated with the computers and the Operations Manager services running on them. When a service that needs to communicate with a service on a different computer starts and attempts to authenticate, the certificates will be exchanged and mutual authentication completed.

Important

The certificates used for this purpose must ultimately trust the same root certification authority (CA).

For more information about how to obtain and make use of certificates for mutual authentication, see [Deploying a Gateway Server](#zb890d6e81363423dbf2b7c7cf6d6ce5b).

Certification Authority

To get the necessary certificates, you will need access to a certification authority (CA). This can be either Microsoft Certificate Services or a third-party certification service such as VeriSign.

Microsoft Certificate Services

There are four types of Microsoft CAs:

 Enterprise root

 Enterprise subordinate

 Stand-alone root

 Stand-alone subordinate

 Both enterprise types of CAs require Active Directory Domain Services; stand-alone CAs do not. Either type of CA can issue the necessary certificates for agent/server mutual authentication across trust boundaries.

Customarily, a CA infrastructure consists of a root CA that signs its own certificates and certifies itself and one or more subordinate CAs, which are certified by the root. The subordinate CA servers are the ones that a service certificate requests, while the root is taken offline and held for safekeeping. For more information about designing certificates, see [Infrastructure Planning and Design](http://go.microsoft.com/fwlink/p/?LinkId=86400) and [Authentication and Data Encryption for Windows Computers](#z8ee895a97bac427480b8092475a83c67).

Monitoring UNIX and Linux computers

System Center 2012 – Operations Manager can monitor UNIX and Linux computers. Because the UNIX and Linux computers are not participating in the Active Directory domain that the management group is in a variation of the certificate method of mutual authentication, discussed before, is used.

Establishing Mutual Authentication with UNIX and Linux computers

You will use the Discovery wizard to find UNIX and Linux computers and add them to the management group as managed objects. During the Discovery wizard process, Operations Manager has the discovered UNIX and Linux computer generate a self-signed certificate which is used for mutual authentication with the management server. The certificate generation, signing and exchange process works like this when SSH discovery is enabled:

1. The Discovery Wizard process on the management server has the discovered UNIX or Linux computer generate a self-signed certificate.

2. The discovering management server issues a get certificate request to the UNIX or Linux computer.

3. The UNIX or Linux computer returns the certificate to the management server

4. The discovering management server creates a key pair and a self-signed certificate of its own. The management server only generates a key pair and a self-signed certificate when it discovers its first UNIX or Linux computer. The management server then imports its own certificate into its trusted certificate store. The discovering management server then signs the UNIX or Linux certificate with its private key. Any subsequent signing of UNIX or Linux computer certificates by the management server will reuse the management server’s private key that was generated on the first signing.

5. The discovering management server then issues a put certificate request which puts the now management server-signed certificate back onto the UNIX or Linux computer that initially generated it. The UNIX or Linux computer WSMAN communication layer is then restarted to make the new UNIX\Linux computer generated certificate active.

6. Now when the management server requests that the UNIX or Linux computer authenticate itself, the UNIX or Linux computer will provide the trusted certificate to the management server and the management server will read the signature on the certificate that it is presented with, see that it trusts this signature (because the signature is its own private key that is stored in its own trusted certificate store) and accept this certificate as proof that the UNIX OR LINUX computer is who the management server thinks it is.

7. The discovering management server will use UNIX or Linux credentials as configured in the appropriate Run As Profile to authenticate itself with the UNIX or Linux computer. See the [Planning for UNIX or Linux Run As Profiles](#z52) section for more details.

Important

The preceding order of operations is for the low security version of UNIX or Linux discovery.

Planning for UNIX or Linux Run As Profiles

After the UNIX or Linux computer is being managed by the discovering management server, the management pack discoveries and workflows begin to run. These workflows require the use of credentials to complete successfully. These credentials, what objects, classes or group they will be applied to and the computers that they will be distributed to are contained in Run As Profiles. There are two Run As Profiles that are imported when the UNIX management packs are imported into your management group; they are:

 Unix Action Account profile – This Run As profile and its associated UNIX or Linux credentials are used for low security activities on the designated UNIX or Linux computers.

 Unix Privileged Account profile – This Run As profile and its associated UNIX or Linux credentials are used for activities that are protected by a higher level of security and therefore require an account that has higher privileges on the UNIX or Linux computer. This can be (but does not have to be) the root account.

You will need to configure these profiles with the appropriate UNIX or Linux computer credentials for the management pack workflows that use them to function correctly.

Accounts and Groups

Over the lifetime of your Operations Manager deployment, you will potentially need many accounts and security groups. During Operations Manager Setup, you are only prompted for four. You need to consider additional accounts when planning out role-based security assignments, notifications, and alternate credentials to run processes. For guidance on planning role-based security assignments, see [Planning the System Center 2012 - Operations Manager Deployment](#zd6edb9b45db840c2be00a32445732d50).

Role-Based Security Accounts and Groups

Operations Manager controls access to monitored groups, tasks, views, and administrative functions through the assignment of user accounts to roles. A role in Operations Manager is the combination of a profile type (operator, advanced operator, administrator) and a scope (what data the role has access to). Typically, Active Directory security groups are assigned to roles, and then individual accounts are assigned to those groups. Prior to deploying, plan out Active Directory security groups that can be added to these and any custom-created roles so that you can then add individual user accounts to the security groups.

Operations Manager provides the following role definitions out-of-the-box.

You can add Active Directory security groups or individual accounts to any of these predefined roles. If you do, those individuals will be able to exercise the given role privileges across the scoped objects.

Note

The predefined roles are globally scoped, giving them access to all groups, views, and tasks (except for Report Security Administrator).

Operations Manager also allows you to create custom roles based on the Operator, Read-Only Operator, Author, and Advanced Operator profiles. When you create the role, you can further narrow the scope of groups, tasks, and views that the role can access. For example, you can create a role entitled "Exchange Operator" and narrow the scope to only Exchange-related groups, views, and tasks. User accounts assigned to this role will only be able to run Operator-level actions on Exchange-related objects.

Notification Accounts and Groups

Individuals in your company that will interact with Operations Manager frequently, such as an Exchange administrator who has been assigned to the Exchange Operator role, need a way to discover new alerts. This can be done by either watching the Operations console for new alerts or by Operations Manager informing them about the alert via supported communications channels. Operations Manager supports notifications through e-mail, instant messaging, Short Message Service, or pager messages. Notifications on what the role needs to know go out to recipients that you specify in Operations Manager. An Operations Manager recipient is merely an object that has a valid address to receive the notification, such as an SMTP address for e-mail notifications.

Therefore, it is logical to combine role assignment with notification group membership via an e-mail-enabled security group. For example, create an Exchange Administrators security group and populate it with individuals that have the knowledge and permissions to fix things in Exchange. Assign this security group to a custom-created Exchange Administrator role so they have access to the data and are e-mail-enabled. Then, create a recipient by using the SMTP address of the e-mail-enabled security group.

Service Accounts

At the time of deployment, you need to have the following service accounts ready. If you use domain accounts and your domain Group Policy object (GPO) has the default password expiration policy set as required, you will either have to change the passwords on the service accounts according to the schedule, or use low maintenance system accounts, or configure the accounts so that the passwords never expire.

Service Principal Names

When you deploy Operations Manager, you may need to register a Service Principal Name (SPN) in some configurations. SPNs are used by Kerberos authentication for the client to mutually authenticate with the server. For more information, see [What Are Service Publication and Service Principal Names?](http://go.microsoft.com/fwlink/p/?linkID=245905).

When you install Operations Manager, you select an account for the System Center Configuration service and System Center Data Access service. For more information, see [Deploying System Center 2012 - Operations Manager](#zd81818d2534e475c98e165496357d5a5).

Caution

Do not modify the default Active Directory permissions to allow an account to do unrestricted modifications of its own SPN.

If you select the Local System as the System Center Data Access service account, the account can create the appropriate SPN. No additional configuration is necessary.

If you use a domain account, you must register an SPN for each management server. Use the SETSPN command line tool. For more information about running that tool, see [Setspn Overview](http://go.microsoft.com/fwlink/p/?linkID=154899).

Register both the netbios name and fully qualified domain name of the management server, using the following syntax:

setspn –a MSOMSdkSvc/<netbios name><DAS account domain>\<DAS account name>

setspn –a MSOMSdkSvc/<fqdn><DAS account domain>\<DAS account name>

Tip

You can list the SPNs registered to user account or computer with the following syntax:

setspn –l <DAS account name>

setspn –l <fqdn>

If you are using Network Load Balancing or using a hardware load balancer, the System Center Data Access service must run under a domain account. In addition to the setup already described, you must also register the load balanced name, using the following syntax:

setspn –a MSOMSdkSvc/<load balanced name><DAS account domain>\<DAS account name>

Note

All of the System Center Data Access services running behind the load balancer must be running with the same domain account.

Run As Accounts

Agents on monitored computers can run tasks, modules, and monitors on demand as well as in response to predefined conditions. By default, all tasks run by using the Agent Action account credentials. In some cases, the Agent Action account may have insufficient rights and privileges to run a given action on the computer. Operations Manager supports the running of tasks by agents in the context of an alternate set of credentials called a Run As Account. A Run As Account is an object that is created in Operations Manager, just like a recipient is, and maps to an Active Directory user account. A Run As Profile is then used that maps the Run As Account to a specific computer. When a rule, task, or monitor that has been associated with a Run As Profile at the development time of a management pack needs to run on the targeted computer, it does so by using the specified Run As Account.

Out-of-the-box, Operations Manager provides a number of Run As Accounts and Run As Profiles, and you can create additional ones as necessary. You may also choose to modify the Active Directory credentials that a Run As Account is associated with. This will require planning, creating, and maintaining additional Active Directory credentials for this purpose. You should treat these accounts as service accounts with respect to password expiration, Active Directory Domain Services, location, and security.

You will need to work with management pack authors as they develop requests for Run As Accounts. For more information, see the [Index to Security-related Information for Operations Manager](http://go.microsoft.com/fwlink/p/?LinkId=244660).

See Also

[Environmental Prerequisites for Operations Manager](#z95d59f735aa94616b98c30680406959a)

Agent and Agentless Monitoring

This section covers the environmental prerequisites for devices that will have agents installed and devices that will be monitored in an agentless fashion.

Clients with Agents Installed

The three main activities involved with agent administration are discovery of target devices, deployment or installation of agents to those devices, and ongoing management of the agents. Agents that lie outside a trust boundary require a few more prerequisites than agents that lie inside a trust boundary.

Agents Inside a Trust Boundary

Discovery

Discovery requires that the TCP 135 (RPC), RPC range, and TCP 445 (SMB) ports remain open and that the SMB service is enabled. For UNIX\Linux computers, default discovery and management occurs over TCP 1270, troubleshooting, and diagnostics discovery occur over SSH, TCP 22. Discovery and deployment over SSH, default TCP 22, can also be enabled to allow Operations Manager to install the WSMAN communication layer on the discovered UNIX/Linux computer.

Installation

After a target device has been discovered, an agent can be deployed to it. Agent installation requires the following:

 Opening Remote procedure call (RPC) ports beginning with endpoint mapper TCP 135 and the Server Message Block (SMB) port TCP/UDP 445.

 Enabling the File and Printer Sharing for Microsoft Networks and the Client for Microsoft Networks services (this ensures that the SMB port is active).

 If enabled, Windows Firewall Group Policy settings for Allow remote administration exception and Allow file and printer sharing exception must be set to Allow unsolicited incoming messages from: to the IP address and subnets for the primary and secondary management servers for the agent.

 An account that has local administrator rights on the target computer.

 Windows Installer 3.1. To install, see [Windows Installer 3.1](http://go.microsoft.com/fwlink/p/?LinkId=86322) (article 893803) in the Microsoft Knowledge Base.

 Microsoft Core XML services (MSXML) 6 on the Operations Manager product installation media in the \msxml subdirectory.

Note

Push agent installation will install MSXML 6 on the targeted device if it is not there.

Ongoing Management

Ongoing management of an agent requires that the TCP 135 (RPC), RPC range, and TCP 445 (SMB) ports remain open and that the SMB service remains enabled.

Agents Outside a Trust Boundary

For agents that lie outside the trust boundary of the management servers, the environmental prerequisites are the same as for those that lie inside a trust boundary, plus some additions.

Because the device is going to have an installed agent, the software, service, and port requirements remain the same. However, because there is no underlying infrastructure to support Kerberos authentication, certificates must be used on both sides of the connection.

To simplify the cross trust boundary configuration, you can install an Operations Manager gateway server in the same trust boundary as the devices that you will monitor. The gateway server acts as a proxy so that all communication between the management server and agents is routed through the gateway server. This communication is done over a single port, TCP 5723, and requires certificates on the management server and the gateway server. In addition, the gateway server performs discovery and installation, and relays ongoing administration traffic on behalf of the management server to the agents. The use of gateway servers also reduces the volume of network traffic and is therefore useful in low bandwidth conditions

Gateway servers can also discover and manage UNIX/Linux computers; this is done over TCP ports 1270 and as needed SSH TCP 22, this port is configurable.

For more information about gateway server configuration, see [Deploying a Gateway Server](#zb890d6e81363423dbf2b7c7cf6d6ce5b).

Manually Installed Agents

Discovery is not performed for manually installed agents, so there are fewer requirements.

Agentless Monitoring

Agentless monitoring of devices is performed by either a management server or by another device that does have an agent, called a proxy agent. An agentless managed device must not be separated from its management server or proxy agent by a firewall because monitoring is performed over RPC. The action account of the agent that is performing the monitoring must have local administrative rights on the device that is being monitored.

See Also

[Environmental Prerequisites for Operations Manager](#z95d59f735aa94616b98c30680406959a)

Single-Server Deployment of Operations Manager

The single-server management group scenario combines all the management group roles that can coexist onto a single instance of the Windows Server 2008 R2 SP1, or Windows Server 2012 operating system running as a member server in an Active Directory domain. This instance can be on dedicated hardware or on a virtual computer. The Operations console can be deployed to computers other than the single server, and the web console is accessed via a browser. Agents are then typically deployed to a limited number of devices depending on the capacity of the server that System Center 2012 – Operations Manager is deployed on.

You deploy Operations Manager in a single-server management group when you want to use it for evaluation, testing, and management pack development, usually in nonproduction or preproduction environments.

Operations Manager Services

The single-server management group configuration supports the following services:

1. Monitoring and alerting

2. Reporting (available in the Operations console but not in the web console)

3. Audit collection

4. Agentless exception management

5. Data (accessed by using the web console and the Operations console)

Operations Manager Features

The single-server management group configuration combines these features:

 Audit Collection Services (ACS) collector

 ACS database

 ACS forwarder

 Operational database

 Operations console

 Reporting data warehouse database

 Reporting database

 Reporting server

 Web console server

 Command Shell

Restrictions

The single-server management group configuration is the easiest to deploy, but there are limitations to its capabilities and therefore limitations to what it is commonly used for.

Gateway Server

This configuration does not include the gateway server role. Because of this, all monitored devices must be in the same Active Directory forest as the management server or you must use certificates on both the managed computer and the management server to provide for mutual authentication.

High Availability and Redundancy

The single server, single management group resides on a single set of hardware. This configuration supports only one instance of each server role and therefore cannot support agent failover between management servers.

Common Uses

This configuration is most commonly used for evaluation, testing, and management pack development purposes, usually in nonproduction or preproduction environments. Single-server management group configurations generally lack the robustness and performance to support anything but the smallest production loads.

Ports Used

In this configuration, you need to make sure that network ports are opened for communication between the agents and the management server, between the Operations console and the management server, and between the web console and the management server. All other inter-service communication occurs on the management server itself. The ports are as follows:

 Operations console to management server: TCP 5724

 Operations console to Reporting server: TCP 80

 Web console to web console server: selected web site port

 Agent to management server: TCP 5723

 ACS forwarder to ACS collector: TCP 51909

 Agentless management: occurs over remote procedure call

 Management server to UNIX\Linux computer: TCP 1270

 Management server to UNIX\Linux computer for special discovery and troubleshooting: TCP 22

For a complete listing of ports used, the direction of the communication, and if the ports can be configured, see [Supported Configurations for System Center 2012 – Operations Manager](http://go.microsoft.com/fwlink/p/?LinkID=219650).

To deploy Operations Manager in a single-server management group, see [Walkthrough: Installing Operations Manager on a Single Server](#z894677121c2c49cc97ddb6af36d5c51a).

See Also

[Deploying System Center 2012 - Operations Manager](#zd81818d2534e475c98e165496357d5a5)

[Distributed Deployment of Operations Manager](#ze9b6f0678f3e465e9a0ff3ae46859bd6)

Walkthrough: Installing Operations Manager on a Single Server

This walkthrough guides you through an installation of System Center 2012 – Operations Manager or System Center 2012 Service Pack 1 (SP1), Operations Manager on a single server. The features installed include the following:

 Management server

 Operations console

 Web console

 Reporting server

Prerequisites

You must ensure that your server meets the minimum supported configurations for Operations Manager. For more information, see [System Requirements for System Center 2012 – Operations Manager](http://go.microsoft.com/fwlink/p/?LinkID=219650).

Important

Before you follow these procedures, read the [Before You Begin](#z51) section of [Deploying System Center 2012 - Operations Manager](#zd81818d2534e475c98e165496357d5a5).

To install the single server management group configuration

|  |
| --- |
| 1. Log on to the server by using an account that has local administrative credentials.  2. On the Operations Manager installation media, run Setup.exe, and then click Install.  3. On the Getting Started, Select features to install page select the Management server, Operations console, Web console, and Reporting server features. To read more about each feature and its requirements, click Expand all, or expand the buttons next to each feature. Then click Next.  4. On the Getting Started, Select installation location page, accept the default value of C:\Program Files\System Center 2012\Operations Manager or type in a new location or browse to one. Then click Next.  5. On the Prerequisites page, review and resolve any warnings or errors, and then click Verify Prerequisites Again to recheck the system.  Note  Installation of the web console requires that ISAPI and CGI Restrictions in IIS be enabled for ASP.NET 4. To enable this, select the web server in IIS Manager, and then double-click ISAPI and CGI Restrictions. Select ASP.NET v4.0.30319, and then click Allow.  Important  You must install IIS before installing .NET Framework 4. If you installed IIS after installing .NET Framework 4, you must register ASP.NET 4.0 with IIS. Open a Command prompt window by using the Run As Administrator option and then run the following command:  %WINDIR%\Microsoft.NET\Framework64\v4.0.30319\aspnet\_regiis.exe -r  6. If the Prerequisites checker does not return any warnings or errors, the Prerequisites, Proceed with Setup page appears. Click Next.  7. On the Configuration, Specify an installation option page, select Create the first Management server in a new management group, type in a name for your management group and then click Next.  Note  After the management group name is set, it cannot be changed. The Management Group name cannot contain the following characters:, ( ) ^ ~ : ; . ! ? " , ' ` @ # % \ / \* + = $ | & [ ] <>{}, and it cannot have a leading or trailing space. It is recommended that the Management Group name be unique within your organization if you plan to connect several management groups together.  8. On the Configuration, Please read the license terms page, review the Microsoft Software License Terms, select I have read, understood, and agree with the license terms, and then click Next.  9. When the Configuration, Configure the operational database page opens, in the Server name and instance name box, type the name of the server and the name of the SQL Server instance for the database server that will host the operational database. If you installed SQL Server by using the default instance, you only have to enter the server name. If you changed the default SQL Server port, you must type in the new port number in the SQL Server port box.  If you type an invalid SQL Server and instance name, you see a red circle with a white X in it appear to the left of the Server name and instance name and SQL Server port boxes.  The white X appears under the following circumstances:   You entered an instance of SQL Server or a SQL Server port value that is not valid or that does not exist.   The instance of SQL Server that you specified does not have the required configuration or features.   You entered a value that is out-of-range (for example, port 999999).   You entered an illegal character for that box (for example, server\instance%)  You can hover the cursor over the Server name and instance text box to view additional information about the error.  10. After you type the correct value for the SQL Server database server name, click the SQL Server port box so that Setup will attempt to validate the values you typed for the SQL Server name and for the port number.  11. In the Database name, Database size (MB)Data file folder, and Log file folder box, we recommend that you accept the default values. Click Next  Note  These paths do not change if you connect to a different instance of SQL Server.  Important  You might receive a message about having the wrong version of SQL Server, or you might encounter a problem with the SQL Server Windows Management Instrumentation (WMI) provider. To resolve this problem, open a Command Prompt window, select Run as administrator, and then run the following command. In the command, replace the <path> placeholder with the location of SQL Server:  mofcomp.exe “<path>\Microsoft SQL Server\100\Shared\sqlmgmproviderxpsp2up.mof”  Note  The SQL Server model database size must not be greater than 100 MB. If it is, you might encounter an error in Setup regarding the inability to create a database on SQL due to user permissions. To resolve the issue, you must reduce the size of the model database.  12. When the Configuration, Configure the data warehouse database page opens, in the Server name and instance name box, type the server name and the name of the instance of SQL Server for the database server that will host the data warehouse database.  13. Because this is a single-server installation, accept the default value of Create a new data warehouse database.  14. In the Database name, Database size (MB)Data file folder, and Log file folder boxes, we recommend that you accept the default values. Click Next.  Important  You might receive a message about having the wrong version of SQL Server, or you might encounter a problem with the SQL Server Windows Management Instrumentation (WMI) provider. To resolve this problem, open a Command Prompt window, select Run as administrator, and then run the following command. In the command, replace the <path> placeholder with the location of SQL Server:  mofcomp.exe “<path>\Microsoft SQL Server\100\Shared\sqlmgmproviderxpsp2up.mof”.  Note  These paths do not change if you connect to a different instance of SQL Server.  15. On the Configuration, SQL Server instance for reporting services page, select the SQL Server database instance from the drop-down list. This drop-down list contains the SQL Server database instance name that was created when you installed SQL Server 2008 R2, SQL Server 2008 R2 SP1, SQL Server 2008 R2 SP2, SQL Server 2012, or SQL Server 2012 SP1 and should be the name of the server on which you are installing Operations Manager. Click Next.  16. On the Configuration, Specify a web site for use with the Web console page, select Default Web Site or the name of an existing website. Select the option Enable SSL only if the website has been configured to use SSL, and then click Next.  17. On the Configuration, Select an authentication mode for use with the Web console page, select your option, and then click Next.  18. On the Configuration, Configure Operations Manager accounts page, we recommend that you use Domain Account option for the Management Server Action Account, System Center Configuration service and System Center Data Access service, the Data Reader account, and the Data Writer account.  Enter the credentials for a domain account in each field. The error icon will disappear after account validation. Click Next.  19. On the Configuration, Help improve System Center 2012 - Operations Manager page, select your options and click Next.  20. If Windows Update is not activated on the computer, the Configuration, Microsoft Update page appears. Select your options, and then click Next.  21. Review the options on the Configuration, Installation Summary page, and click Install. Setup continues.  22. When Setup is finished, the Setup is complete page appears. Click Close and the Operations console will open. |

To install the System Center 2012 - Operations Manager single server management group configuration by using the Command Prompt window

|  |
| --- |
| 1. Log on to the server by using an account that has local administrative credentials.  2. Open the Command Prompt window by using the Run as Administrator option.  Note  Setup.exe requires administrator privileges because the Setup process requires access to system processes that can only be used by a local administrator.  3. Change the path to where the Operations Manager setup.exe file is located, and run the following command.  Important  Use the /WebConsoleUseSSL parameter only if your website has Secure Sockets Layer (SSL) activated.  For a default web installation, specify Default Web Site for the /WebSiteName parameter.  Important  The following command assumes that you specified the Local System for the Management server action account (/UseLocalSystemActionAccount) and Data Access service (/UseLocalSystemDASAccount). To specify a domain\user name for these accounts, you must provide the following parameters instead.  /ActionAccountUser: <domain\username> /ActionAccountPassword: <password>  /DASAccountUser: <domain\username> /DASAccountPassword: <password>  setup.exe /silent /install  /components:OMServer,OMConsole,OMWebConsole,OMReporting  /ManagementGroupName: "<ManagementGroupName>"  /SqlServerInstance: <server\instance>  /DatabaseName: <OperationalDatabaseName>  /DWSqlServerInstance: <server\instance>  /DWDatabaseName: <DWDatabaseName>  /UseLocalSystemActionAccount /UseLocalSystemDASAccount  /DatareaderUser: <domain\username>  /DatareaderPassword: <password>  /DataWriterUser: <domain\username>  /DataWriterPassword: <password>  /AcceptEndUserLicenseAgreement  /WebSiteName: "<WebSiteName>" [/WebConsoleUseSSL]  /WebConsoleAuthorizationMode: [Mixed|Network]  /SRSInstance: <server\instance>  /SendODRReports: [0|1]  /EnableErrorReporting: [Never|Queued|Always]  /SendCEIPReports: [0|1]  /UseMicrosoftUpdate: [0|1] |

Verifying the Installation

To confirm the health of the management server

|  |
| --- |
| 1. In the Operations console, select the Administration workspace.  2. In Device Management select Management Servers. In the results pane, you should see the management server that you just installed with a green check mark in the Health State column. |

To confirm the health of operations manager reports

|  |
| --- |
| 1. In the Operations console, in the navigation pane, click the Reporting button.  Note  After initial deployment, it can take up to 30 minutes for reports to appear.  2. Click Microsoft ODR Report Library, and then double-click any of the reports listed. The selected report is generated and displays in a new window.  By default, you should see the following reports:   Alerts Per Day   Instance Space   Management Group   Management Packs   Most Common Alerts  Note  Selecting the management packs report is particularly useful at this point because it provides you with a full inventory of the management packs that have been installed on your server.  3. Close the report window. |