Symantec Management Platform global policy distribution

Symantec Management Platform global policy distribution

Legal Notice

Contents

Chapter 1

Understanding global policy distribution

This chapter includes the following topics:

About global policy distribution

Global policy distrubution uses a hierarchy to let you create and control global policies from a parent Notification Server computer. Hierarchy gives you some global management capabilities but still preserves regional Notification Server autonomy. Policies, jobs, and tasks, are managed at each child Notification Server, while global policies are managed centrally from the parent Notification Server.

The majority of your day-to-day management work should be performed from each Notification Server computer using the Web-based console. However; you can control some policies that apply to all endpoints from the single global

Notification Server. These global policies can be forced to run on every child Notification Server in the hierarchy.

At the global Notification Server computer, you can create global reports. However; to make these reports contain the data you need, you may need to specify the data for replication that is required to populate them.

A global administrator can distribute policies to regional Notification Servers where the local administrator may make changes and apply the policy. These distributed policies can be made either editable or non-editable.

A non-editable policy is used to force consistent policy behavior across all Notification Servers. Regional administrators cannot override these rights without you specifying the properties of the policy that they may edit. An editable policy lets regional administrators modify a common policy to apply to specific targets and schedules.

A non-editable policy can be cloned. All properties of the cloned policies can then be edited. Whether or not a policy may be cloned is controlled through role-based security rights.

See "About hierarchy editable properties" on page 14.

What you can do with global policy distribution

Global policy distribution provids limited centralized management opportunities.

See "About global policy distribution" on page 5.

Global policy distribution lets you do the following:

- Create and distribute central policies
- Replicated packages
- Forward inventory for limited centralized reporting
- Manage security role's centrally

How global policy distribution works with hierarchy

The purpose of hierarchy is to combine multiple Notification Server computers into a single Symantec Management Platform to let you manage some policies from a single Symantec Management Console. However, hierarchy does not increase the number of endpoints that each Notification Server computer can independently support.

For example, you can replicate a software delivery policy. Replicating a policy also replicates the associated data such as a software package so that the software

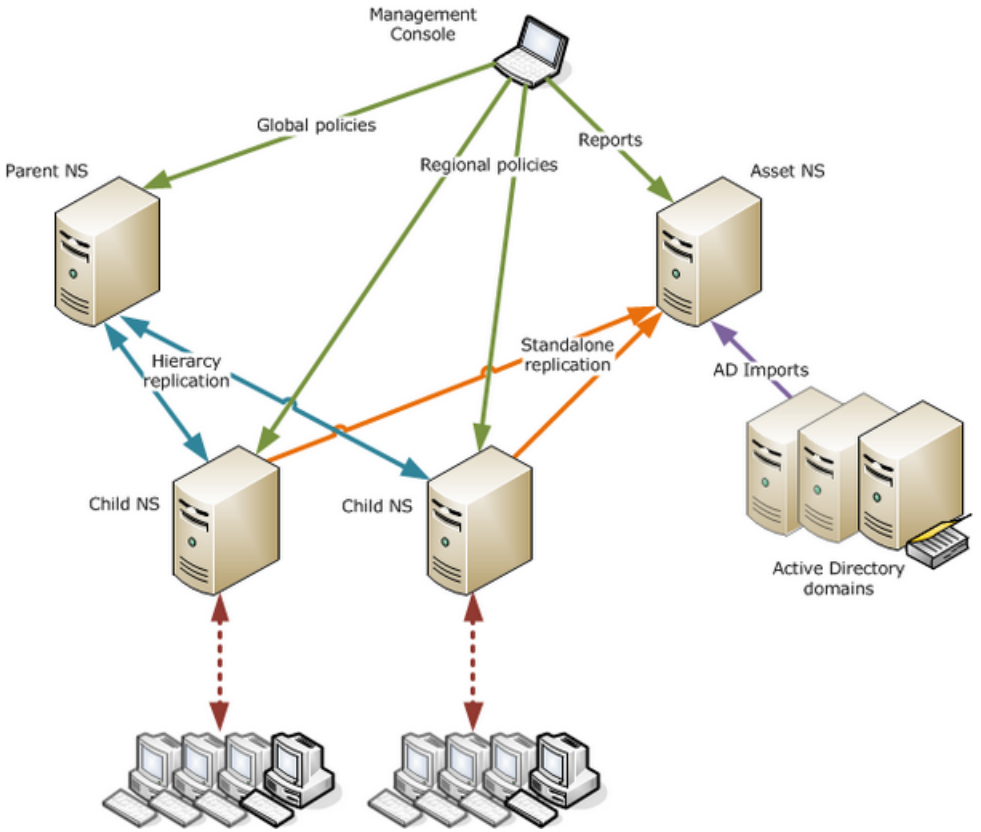
can be delivered to the applicable client computers of the child Notification Server computers.

See "About global policy distribution" on page 5.

In a hierarchy you can manage from both the parent Notification Server computer and the child Notification Server computers. Management from the parent server applies to all child servers. Management at a child server only applies to its endpoints. This lets you combine both global management practices and regional management practices into a single platform. For example, a global policy can be distributed from the parent Notification Server computer to all managed endpoints, but regional administrators can also create policies that apply to their specific region.

See "About hierarchy" on page 11.

The following diagram shows how hierarchy can distribute policies down and use inventory forwarding to provide specific reporting data.



Configuring global policy distribution with local accountability

A global administrator can distribute policies to regional Notification Servers where the local administrator may make changes and apply the policy.

See "How global policy distribution works with hierarchy" on page 6.

To configuring global policy distribution with local accountability, you do the following:

- Scenario Global administrator defines policies for a large organization.
- Policies and their packages are sent to regional notification servers.
- Regional administrators customize and apply the policies to their endpoints.
- Preconfigured data is sent up to the global notification server
- The data is available for reporting.

Limitations of global policy distribution in a hierarchy

Global policy distribution in a hiearchy topology does not replace regional management needs. It is important to understand some limitations and considerations before you create a global policy distribution plan.

See "Global policy distribution implementation considerations" on page 9.

See "What you can do with global policy distribution" on page 6.

Global policy distribution has the following limitations:

- Hierarchy does not provide a central view of all report data in an environment. In a hierarchy, administrators must manage and report at the child and parent Notification Servers in order to view all data.
- Setting up a hierarchy will not increase the ability to scale.
- Hierarchy is not a replacement for organizational views and groups. It is not an efficient method to provide scope-based management in an environment.
- Hierarchy is not a data replication strategy for Notification Server fail-over.

Global policy distribution implementation considerations

Global policy distribution in a hiearchy topology does not replace regional management needs. It is important to understand some limitations and considerations before you create a global policy distribution plan.

See "Limitations of global policy distribution in a hierarchy" on page 8.

See "What you can do with global policy distribution" on page 6.

See "Global policy distribution implementation considerations when using with Patch Management Solution" on page 9.

See "Global policy distribution implementation considerations when using with Software Management Solution" on page 10.

When considering implementing global policy distribution, do the following:

- Plan for replication server load and delay when using a hierarchy. The default replication schedule is 24 hours.
- Use a flat two tier hierarchy to simplify hardware requirements and minimize replication delays.
- Carefully consider the amount of data to be replicated before configuring replication rules.
- Implement inventory forwarding if central reporting is the primary objective. This feature does not require a hierarchy to use.
- For distributed sites, use site servers instead of an additional Notification Server.

Global policy distribution implementation considerations when using with Patch Management Solution

There are some specific considerations about Patch Managment Solution to be aware of before you implement a global policy distribution plan.

See "Global policy distribution implementation considerations" on page 9.

The following are implementation considerations with Patch Management Solution:

- Use patch management in a hierarchy to replicate software updates down the hierarchy for distribution and receive vulnerability reports at the top of the hierarchy.
- In a hierarchy, patches must be imported at the parent notification server.
- To minimize distribution times, replication schedules must account for the following order of operations: PMImport schedule; PMImport replication rule; site server download; agent update interval.
- Without aligning schedules, patch distribution will typically take more than 48 hours.
- A compliance summary is all that's available at the parent NS. Full vulnerability analysis reports drill down to each child notification server.

Global policy distribution implementation considerations when using with Software Management Solution

There are some specific considerations about Software Managment Solution to be aware of before you implement a global policy distribution plan.

See "Global policy distribution implementation considerations" on page 9.

The following are implementation considerations with Software Management Solution:

- Hierarchy replication will replicate software delivery policies and packages to child notification servers for distribution.
- Policies, filters, and packages will be replicated automatically down the hierarchy.
- Software delivery will typically take more than 48 hours.
- Replication rules will need to be customized to include the Software inventory details needed for reporting.
-

Chapter 2

Understanding hierarchical relationships

This chapter includes the following topics:

About hierarchy

Hierarchy is a topology that lets you perform global policy distribution. Global policy distribution is a method to centrally manage policies when multiple Notification Servers are required.

A hierarchy uses parent-to-child relationships to define how information flows across multiple Notification Server computers. These relationships are called your hierarchy topology.

See "How global policy distribution works with hierarchy" on page 6.

Hierarchy requirements

To share or receive common configuration settings and data with multiple Notification Servers, you must first add the Notification Server computer to a hierarchy. Because Notification Servers can be managed locally, each Notification Server must be added or removed from a hierarchy individually with the appropriate access credentials. Typically, the Symantec Administrator managing the topology design accesses the Notification Server computers in other sites remotely to add them to a hierarchy.

The requirements for configuring hierarchy are as follows:

- Network traffic must be routable between adjoining Notification Servers within the hierarchy.
- HTTP/HTTPS traffic must be permitted between adjoining Notification Servers within the hierarchy.
- Trust relationships must exist between adjoining Notification Servers within the hierarchy, or credentials for the privileged accounts that facilitate trust must be known.
- Each Notification Server must be able to resolve the name and the network address of any adjoining Notification Servers within the hierarchy.
- There must be sufficient bandwidth between Notification Server sites to support package and data replication.
  Bandwidth and the hardware that is required depend on the size of your Hierarchy topology and the data replicated.
- A site must exist for each Notification Server, and must include the subnet that contains Notification Server. The site must also contain a package server (a site server that is running the package service) that serves the Notification Server computer .

Limitations of hierarchy

Hierarchy can simplify the management of multiple Notification Server computers. However, having multiple Notification Server computers does not necessarily indicate that you should implement a hierarchy. Even if a hierarchy simplifies your administration, it increases your Notification Server computer infrastructure overhead.

Consider the following limitations before you implement a hierarchy:

- Three-tier hierarchies are supported, but two-tier hierarchies are recommended to minimize the overhead and to increase the replication speed.

- Typically you can have between one and 12 child Notification Server computers in a hierarchy. This number depends on the hardware capabilities of each server and your IT management requirements. For example, the frequency and amount of inventory that you gather affects the number of clients each Notification Server computer can support. In a highly complex hierarchy scenario, you should contact Symantec Consulting Services to analyze your requirements and fine-tune the platform architecture to meet your needs.
- Hierarchy adds the cost of a very robust Notification Server computer to act as the parent server.
- Replication has some affect on the performance of all the Notification Server computers. This additional load on the child Notification Server computer may influence its maximum supported client count.
- Replicating information is subject to a time-delay of replicating information.
- Network traffic must be routable between parent and child Notification Server computers.
- HTTP/HTTPS traffic must be permitted between parent and child Notification Server computers.
- Trust relationships must exist between the parent server and the child server, or your administrators must know the credentials for privileged accounts.
- Parent and child Notification Server computers must be able to resolve the computer name and the network address of each other.
- There must be sufficient bandwidth between Notification Server computers to support package and data replication.
- Replicating more than once a day can have negative consequences.
- Not all solutions in the Symantec Management Platform support hierarchy replication.
- All Notification Server computers must have the same version of the Symantec Management Platform and Solutions installed. To determine the version you can open the Symantec Installation Manager locally on each Notification Server computer and record them. To perform Symantec Management Platform updates, hierarchy replication must be disabled first to avoid conflicts between dissimilar versions. You can easily enable or disable hierarchy replication on specific Notification Server computers with a single step. To perform Solution updates, use Symantec Installation Manager locally on each Notification Server computer.
- You cannot get real-time data with hierarchy replication. When data is moved through the hierarchy there is a time delay. For example, if you use the default replication schedule for software distribution, then you require up to 24 hours

for each tier in the hierarchy to deliver the software. You can force individual items to replicate by using the replicate now option instead of waiting for the schedule.

- If clients are configured with SSL (HTTP or HTTPS), then their Notification Server computer must also be configured for it. Mixed SSL and non-SSL environments should not be supported. If one Notification Server computer has SSL, then all of them must have it configured.

About hierarchy editable properties

Hierarchy editable properties let you control rights to your globally-defined policies. Regional administrators cannot override these rights without you specifying the properties of the policy that they may edit.

You can define whether or not a regional administrator has rights to do the following:

- Turn on and off a global policy
- Change the schedule of a global policy
- Modify the targets of global policy.

About creating and managing hierarchical relationships

You can add your Notification Server (the one that you are logged into, which may be a remote logon) to a hierarchy as a child of an existing remote Notification Server, or as its parent. To create a hierarchical relationship, you require a Symantec Administrator account (or an account with equivalent privileges) on both computers. To add or remove Notification Servers from a hierarchy, you need the following security privileges: Manage Hierarchy Topology on both computers, and Manage Hierarchy Replication on the local computer.

See "Hierarchy requirements" on page 12.

You can view and configure the Notification Server computer hierarchy using the Symantec Management Console. If you are the Hierarchy administrator, you can see only the parent and children (down to all levels) of your Notification Server.

Note that all actions that you take are based on your Notification Server. Right-clicking a Notification Server does not perform a remote logon to any remote Notification Servers. It opens a context menu containing the actions that you can perform on that server, which is different for local and remote computers. A full set of actions is available for the local server, but only a limited set is available

for remote servers. Actions such as extracting reports are performed on the appropriate database.

The actions that you can perform on the hierarchy are relative to your Notification Server, which is the computer that you are logged on to. If you have the Manage Hierarchy privilege on a remote Notification Server, you can perform a remote logon to that computer. You can then open the Symantec Management Console, and perform hierarchy configuration relative to that computer.

When you remove a Notification Server from a hierarchy, its child Notification Servers are also removed from the Hierarchy. If any of those servers has its own child servers, it automatically becomes the top-level node of its own hierarchy structure. If you remove the Notification Server computer at the top of a hierarchy structure, all its child servers become parent servers of their own hierarchy structures.

You can enable or disable Hierarchy replication on specific Notification Servers at any time. For example, you can use this facility to temporarily disable Hierarchy replication during maintenance tasks such as solution installation, upgrades or uninstallation. Disabling replication on one Notification Server does not affect the replication schedule on the other Notification Servers in the hierarchy. However, no data is passed through the disabled computer, so replication down stops at the parent, and replication up stops at the children.

A colored symbol on the Hierarchy Management page indicates any hierarchy alerts. The colors that you might see, and the corresponding alert status are as follows:

Yellow	Low alert status
Orange	Medium alert status
Red	Critical alert status. For example, if you attempt to replicate the same data both up and down the hierarchy from the same Notification Server a critical alert is raised. Data should be replicated one way only. If the parent or the child Notification Server has the same hierarchy replication rules implemented, or you could set up a data clash.

About hierarchy topology

The hierarchy topology is a set of one-to-one parent-to-child relationships between two or more Notification Server computers. Each Notification Server computer in the hierarchy can have multiple children servers, but each child server may only connect to a single parent server. Each Notification Server computer is only

aware of its immediate parent and its immediate children. The servers are unaware of peer members in the hierarchy.

You can manage from both the parent and the child Notification Server computers. If management is done from a parent server, it can apply to all of the child servers and their managed computers. If management is done from a child server, the task only applies to the child server's managed computers.

When you set up the relationships of your hierarchy topology, you must add them two at a time. You must have administrative rights on both Notification Server computers. The relationships can be established from either the child server or the parent server.

There is a dedicated security role in the Symantec Management Platform for manipulating hierarchy topology settings like establishing relationships, editing schedules and configuring replication rules. Your administrators can force hierarchy to replicate individual items without being assigned this security role.

Setting up a hierarchical relationship between two Notification Servers

You can set up a hierarchical relationship (either Parent of or Child of) between your Notification Server and a remote Notification Server. You need to specify the name, URL, and access details of the remote Notification Server and provide the access details of your local Notification Server. By default, the hierarchy replication schedule staggers the replication between each pair of Notification Servers. You can change the replication schedule to suit your requirements, but you should ensure that replication staggering is maintained.

See "Hierarchy requirements" on page 12.

See "About creating and managing hierarchical relationships" on page 14.

Both Notification Servers must have a package server available within their respective sites. The package server is required for performance reasons. You cannot create a hierarchical relationship between two Notification Servers if either one does not have a package server available.

Notification Server application credentials should be stable and not be changed regularly like some user account passwords. If the Notification Server computer application account password becomes invalid, a message is displayed in the console. The message prompts you to use the ASConfig command-line tool to make the necessary updates.

To set up a hierarchical relationship between two Notification Servers

1. In the Symantec Management Console, in the **Settings** menu, click **Notification Server Management > Hierarchy**.
2. On the Hierarchy Management page, on the **Topology** tab, right-click your Notification Server, and then click the appropriate option:
   - **Add > Parent**
   - **Add > Child**
   - **Edit > Parent**
   - **Edit > Child**
3. In the Add Hierarchy Node Wizard, on the first page, enter the name and URL of the remote Notification Server.
4. Supply the appropriate access credentials.

   The access credentials must be a Symantec Administrator account or equivalent account on the remote Notification Server.
5. Click **Advanced**.
6. In the **Advanced** dialog, specify the Symantec Administrator (or equivalent) account that the remote Notification Server uses to communicate with the local Notification Server.
7. Click **OK** to close the Advanced dialog.
8. Click **Next**.
9. On the Replication Schedules page, set up the differential and the complete replication schedules, and enable those that you want to use on the Notification Server computer.

   By default only the differential replication schedule is enabled. Complete replication is rarely used because it puts a heavy load on the Notification Server computer, but you can enable it when necessary. You should schedule the replication at the times that do not clash with replication schedules on other Notification Servers in the Hierarchy.

10 Click **Next**.

11 On the Confirm Settings page, verify that the settings are correct, and then click **Finish**.

The local Notification Server uses the specified information to locate and verify the remote Notification Server and set up the appropriate hierarchical relationship with it.

If the remote Notification Server does not have a package server available within its site, the verification fails and the hierarchical relationship cannot be established.

Replication types in the Symantec Management Platform

There are two types of replication that are used in a Symantec Management Platform.

These include the following types:

- Hierarchy replication. Copies information between multiple Notification Server computers. It defines which items are replicated, the direction that each item type flows, and when the replication occurs on each server in the platform. You can use replication to copy policies and tasks, and reporting information to other Notification Server computers.
- Peer-based replication. Requires you to specifically define the items to replicate and the direction that they replicate. You must configure the rules very selectively because there is no automatic conflict prevention in peer-based replication. You can use both hierarchy replication and peer-based replication concurrently within a single Symantec Management Platform environment. This method of replication was called "inventory forwarding" in previous releases.

Chapter 3

Understanding hierarchy replication

This chapter includes the following topics:

About hierarchy replication

Hierarchy replication specifies what is replicated in the hierarchy. It has no effect on the stand-alone replication that you can set up between any two Notification Servers. Any data that is replicated down from a parent Notification Server has priority, and overwrites the corresponding data on its child servers.

See "About creating and managing hierarchical relationships" on page 14.

See "Setting up a hierarchical relationship between two Notification Servers" on page 16.

See "Configuring hierarchy replication" on page 25.

See "Configuring hierarchy replication rules" on page 26.

The replicated configuration and management items received from a parent server are usually read-only so they cannot be modified. The read-only setting ensures that it is replicated unchanged down the hierarchy. If you want to allow additions to replicated items on child servers, you need to unlock the relevant items on the Notification Server computer on which they were created. For example, you may want to allow policies to be enabled and disabled on the child Notification Servers.

Hierarchy replication does not let you replicate the same data up and down the hierarchy. If you set up two rules that have the same resource type being replicated in both directions, a critical alert is raised and the replication rules are not executed.

Hierarchy has two modes of replication:

Differential	Replicates the objects and the data that have changed since the last replication. This mode is enabled by default and reduces the load and the bandwidth that hierarchy uses.
Complete	Replicates all objects and data. This mode is disabled by default.

To minimize the load on the network and to prevent data collisions, you should schedule hierarchy replication at a different time for each Notification Server in your hierarchy.

Hierarchy replication synchronizes different types of objects in the following ways:

Security objects	Security objects, such as roles and privileges, always use complete replication. Differential replication is not an option for read-only objects such as these.
Items	Items use differential replication, which is handled by hashing each item to check for changes and replicating those that have changed.
Resources	Resources use differential replication. Differential replication is based on the "last changed" timestamp on the source data. Any data that has changed since the last replication is replicated to the destination server. The data on the destination is then verified, if data verification has been enabled in the appropriate replication rule. Data verification imposes significant processing load on Notification Server. To reduce this load, you can verify a specified percentage of data on the destination server with each replication. For example, if you verify 10% of the data for each replication, that ensures that all data has been verified after 10 replications.

Understanding hierarchy replication

Hierarchy replication copies information between multiple Notification Server computers. It defines which items are replicated, the direction that each item type flows, and when the replication occurs on each server in the platform.

Objects and data are constrained to only replicate in known directions to avoid conflicts. The data from the source server is always given priority and overwrites

older versions of the data on the target server. The replicated data is read-only on the target server. This also applies for the items that are replicated up the hierarchy. Although the items are replicated as read-only by default, the policies can have the hierarchy editable properties (HEPs) that allow some settings to be edited at the child Notification Server computer. The HEPs must be configured on the parent Notification Server computer. The HEP that is currently implemented is “enable/disable the policy. To change this setting, the administrator must edit the hierarchy properties on each policy, one at a time.

Each unique child server replicates with its immediate parent according to its own schedule. By default, the hierarchy replication schedule is every 24 hours. You should stagger the hierarchy replication schedule for each server to balance the load on the parent server. To estimate how long each replication takes, you can check the event logs to see how long the regular replication events take and add a buffer. It is recommended to do this estimation after the initial replication, because the initial replication is a complete replication whereas the subsequent replication will be mostly differential.

Hierarchy replication does not affect any peer-based replication that you set up between two Notification Server computers independently of the hierarchy topology. The difference between peer-based replication and hierarchy based replication is that servers in a hierarchy topology have predefined definitions of the direction that each type of data flows.

How hierarchy replication works

Hierarchy replication copies selected data from the parent server to its child server and from the child server to its parent server. It is neither realistic nor necessary to replicate all of the data in the entire platform. The default rules of hierarchy replication are unique for each solution. Only some items are enabled for hierarchy replication by default. Parent and child Notification Server computers are not mirror replicas of one another because replicated data is limited to only what is necessary for management and reporting.

The limitations of how much data you can replicate are evident with upstream replication. There are large amounts of data available that the Symantec Management Platform can gather. For example, the level of detail that Inventory Solution can be configured to collect can overload the parent Notification Server computer. Hierarchy replication rules define if an item is replicated. The Symantec Management Platform includes several rules by default . You can modify these existing hierarchy replication rules or create your own. To do this you must identify the data classes and resources in the CMDB that you want to replicate.

When you select which data to replicate, you do not need to specify the direction that the data replicates. Each data type only flows in one direction. For example,

policies, tasks, packages, and configuration settings flow downstream from the parent server to the child servers. The data classes that are needed for reporting flow upstream from the child servers to the parent server.

Replication can be initiated in two ways. Individual items, such as policies, can be replicated by right-clicking on the item and choosing “replicate now.” If the option does not appear in the right-click menu, then the item does not support replication. You can also initiate replication through a schedule. Replication rules define items that replicate through the hierarchy according to the schedule. The default replication schedule is to replicate every 24 hours.

The following are commonly replicated objects and the direction that the data flows:

- Configuration and Management Items
  Policies, tasks, filters, and reports are replicated as read-only items down a hierarchy.
- Security
  Security roles, privileges, and permissions are replicated down a hierarchy.
- Resources
  Resource information, such as computers, users, sites, and their associated data classes, are replicated up or down a hierarchy.
- Events
  Event data-classes, such as software delivery execution, are replicated up or down a hierarchy. There are no events that are replicated by default. To avoid overwhelming the parent server, event replication should only be done on a limited and temporary basis.

About hierarchy replication rules

Hierarchy replication relies on replication rules. These rules define the data that will replicate to other Notification Server computers. Many items are configured to replicate by default. However, there are practical constraints, particularly on the number of items that can replicate up the hierarchy. For example, many inventory data classes are not enabled to replicate up the hierarchy by default. Without those data classes, some reports will not function at the parent Notification Server computer. You should be selective in choosing which data classes to replicate up. You can disable a replication rule at any time and enable it again later; it is not deleted.

Events are another item that can overwhelm a parent Notification Server computer when replicated. By default, no events are enabled to replicate. These should be replicated only with great caution and for limited time periods. Note that because

replication does not occur real-time, raw event data cannot be used for alerting at the parent Notification Server computer.

Chapter 4

Setting up and using hierarchy replication

This chapter includes the following topics:

Configuring hierarchy replication

When you add a Notification Server to a hierarchy you can specify what to replicate to the parent Notification Server and to any child Notification Servers. By default, everything is replicated (full replication), which may consume excessive bandwidth. We recommend that you configure hierarchy replication on each Notification Server to best suit the requirements of your organization.

See "About hierarchy replication" on page 19.

See "Configuring hierarchy replication rules" on page 26.

Anything that is published on a child Notification Server is read-only and cannot be overwritten by the data that is replicated down from its parent.

Hierarchy replication of resources and events is configured using replication rules. These rules define the data that you want to replicate to other Notification Servers. You need to create all the rules that you require, and then enable those

that you want to use. You can disable a replication rule at any time—it is not deleted—and enable it again later.

Hierarchy replication rules are replicated down the hierarchy. You can set up your replication rules at the root level Notification Server and then replicate them to all child levels. You may want to do the same for security roles and privileges. Lower-level Notification Servers cannot change the replicated security items or replication rules, but they can add new ones when necessary. Any new security items or replication rules would apply only to the local Notification Server, but they can be replicated down to its children. You need the Manage Hierarchy Replication privilege to make any changes to replication rules.

You can also manually replicate selected data directly from a Notification Server to all its child Notification Servers without including it in a replication rule. Manual replication is a once-off replication that takes place immediately. You need the Replicate Now privilege to perform manual replication.

See "Replicating selected data manually" on page 31.

See "About replication" on page 33.

To configure hierarchy replication

1. In the Symantec Management Console, in the **Settings** menu, click **Notification Server > Hierarchy**.
2. On the Hierarchy Management page, select the Replication tab.
3. Configure hierarchy replication by selecting the appropriate options, and setting up and enabling the appropriate rules.
4. To save the configuration settings, click **Apply**.
5. If you want to set up custom hierarchy replication for configuration and managements items, make the appropriate settings.

   The context menu option to enable hierarchy replication on specific items is not available until the Custom option has been confirmed.
6. Click **Apply** to confirm the custom hierarchy replication settings.

Configuring hierarchy replication rules

You can set up replication rules for the resource types or resource targets, specific data classes, and event types that you want to replicate within the hierarchy. Each rule replicates the specified data in one direction only, up to the parent Notification Server or down to the child Notification Servers.

See "Configuring hierarchy replication" on page 25.

See "Hierarchy replication rule settings" on page 28.

You may include resource targets in a resource replication rule. Resource scoping applies to the contents (resources) of the targets that are replicated. Therefore, the resources that are replicated depends on the owner of the resource target. The Notification Server administrator can choose to replicate resource targets in their current state (owned by somebody else, with the corresponding scope). Alternatively, they can take ownership of the targets, save them with the administrator's scope (which usually contains more resources) and replicate them in that state. All the current members of a resource target are replicated. The actual resource target item is replicated in the background as a dependent item.

The replication rules that are provided with Notification Server and the installed solutions cannot be deleted, and you should not normally need to modify them. However, you can enable and disable rules when necessary, and you can edit the rule name and description.

To configure hierarchy replication rules

1. In the Symantec Management Console, in the **Settings** menu, click **Notification Server Management > Hierarchy**.
2. On the Hierarchy Management page, click the Replication tab.
3. Do any of the following:

To create a new hierarchy replication rule	Click **Add**.
To modify an existing hierarchy replication rule	Select the appropriate rule, and then click **Edit**.
To enable a hierarchy replication rule	Check **Enabled** beside the replication rule name. If you want to disable the replication rule, uncheck **Enabled**.
To delete a hierarchy replication rule	Select the appropriate rule, and then click **Delete**.

4. If you want to create or modify a rule, in the **Replication Rule** window, specify the appropriate settings.

   See "Hierarchy replication rule settings" on page 28.
5. Click **Save Changes**.

   The modified hierarchy replication rule is added to the table.
6. On the **Replication** tab, click **Apply**.

Hierarchy replication rule settings

You can set up replication rules for the resource types or resource targets, specific data classes, and event types that you want to replicate within the hierarchy. Each rule replicates the specified data in one direction only, up to the parent Notification Server or down to the child Notification Servers. Some settings apply only to a particular rule type.

See "About hierarchy replication" on page 19.

See "Configuring hierarchy replication" on page 25.

See "Configuring hierarchy replication rules" on page 26.

Table 4-1 Hierarchy replication rule settings

Setting	Description
Rule name and description	The first line of the page heading is the name of the replication rule. The second line of the page heading is its description. To change these, you can click the text to make it editable, and then type the rule name or description.
Rule status symbol	The current status of the replication rule: ■ On (Green light) – The rule is active. ■ Off (Red light) – The rule is idle. You can click the symbol to toggle the status to its alternative setting.
Resource Types **Resource Targets**	Applies to resource replication rules and event replication rules. The resources that you want to replicate. These two options are alternatives. You can click the appropriate option to activate the one that you want: ■ **Resource Types** Replicates the selected resource types. Click **Resource Types** and then, in the **Select Resource Type** window, select the resource types that you want to include. ■ **Resource Targets** Replicates the selected resource targets. Click **Resource Targets** and then, in the **Resource Target** window, select the resource targets that you want to include. If you want to create new resource targets, click **Build Target** and, in the **Select a Group** window, specify the appropriate resource target.

Table 4-1 Hierarchy replication rule settings *(continued)*

Setting	Description
Data Classes	Applies to resource replication rules only. If you want to specify particular data classes to include, you can click **Data Classes**. In the **Inventory Data Classes** window, select the classes that you want.
Event Classes	Applies to event replication rules only. The event classes to include. To select these, you can click **Event Classes** and, in the **Event Classes** window, select the classes that you want.
Direction	The direction of replication: ■ Up the Hierarchy ■ Down the Hierarchy.
Maximum Rows	Applies to event replication rules only. You can specify the maximum number of table rows to replicate.
Resend events that have been sent previously	Applies to event replication rules only. You should use this option if a destination server has recently purged its event classes. You could also use this option if you have experienced network problems between servers in the hierarchy. Resending events is a once-off operation and you should disable this option after the rule has been run. **Note:** Enabling this option may cause duplicate event data at the destination Notification Server because event data does not support merging.
Use Standard Replication Schedule	Use the default replication schedule for this Notification Server. This schedule is the replication schedule that is defined when you add the Notification Server computer to the hierarchy. See "Setting up a hierarchical relationship between two Notification Servers" on page 16.
Use this schedule	Overrides the default replication schedule and use another schedule for this rule. You can select the schedule that you want to use. If you select Custom Schedule, you need to click **Define Custom Schedule** and, in the Schedule Editor, specify the schedule parameters.
Enable Data Verification	Applies to resource replication rules only. Data verification imposes a significant load on the server, so should be used only for critical business processes.

Table 4-1 Hierarchy replication rule settings *(continued)*

Setting	Description
Verify maximum of nn% of data during each replication	Applies to resource replication rules only. To reduce the load that is imposed on the server, you can verify small amounts of resource data on every replication. You can specify a verification percentage in the replication rule. For example, if you verify 10% of the data for each replication, that ensures that all data has been verified after 10 replications.

Overriding the hierarchy differential replication schedule

The Notification Server computers in a hierarchy are normally synchronized according to the replication schedule that is set up in the replication rules. If necessary, you can manually override the differential replication schedule for your Notification Server and trigger all the hierarchy replication rules immediately. You can manually replicate data to your Notification Server from a remote parent or child Notification Server only.

You cannot manually override replication to a remote Notification Server. You can only perform an operation that affects your Notification Server. You can log on to a remote Notification Server to make it your Notification Server, and manually override the differential replication schedules on its parent or its child Notification Servers.

See "About hierarchy replication" on page 19.

See "Configuring hierarchy replication" on page 25.

To override the hierarchy differential replication schedule

1. In the Symantec Management Console, in the **Settings** menu, click **Notification Server > Hierarchy**.
2. On the Hierarchy Management page, on the Topology tab, right-click the Notification Server computer from which you want to replicate data.
3. Click **Hierarchy > Replicate To...**.

   This option triggers the hierarchy replication rules that point to the local (currently logged on) Notification Server. You cannot replicate data from the remote Notification Server to any other remote servers.
4. In the confirmation dialog box, click **OK**.

Replicating selected data manually

You can override the replication rules for your Notification Server by performing a manual hierarchy replication of a particular folder or item. Manual replication replicates the selected data to the child Notification Servers immediately. The data is replicated regardless of the replication schedules or whether the data is included in the replication rules.

See "About hierarchy replication" on page 19.

To manually replicate selected data from your Notification Server

1. In the Symantec Management Console, in the left pane, right-click the folder or item that you want to replicate.

   If you select a folder, the replication includes all of its content (all levels of subfolders and items that it contains). Any parent folders (but not their contents) are also replicated to preserve the folder paths within the structure.
2. Click **Hierarchy > Replicate Now...**.
3. In the confirmation dialog box, click **OK**.

Running a hierarchy report

Some hierarchy reports are supplied with Notification Server, and solutions may provide additional reports. You can run a report on any Notification Server in the hierarchy to extract data from its CMDB.

Some installed solutions may supply hierarchy federated reports. These reports summarize the relevant data across the hierarchy, and the results contain a single line for each Notification Server. You can run the full report on a particular Notification Server by double-clicking on the appropriate line.

To run a hierarchy report

1. In the Symantec Management Console, in the **Settings** menu, click **Notification Server > Hierarchy**.
2. On the Hierarchy Management page, on the **Topology** tab, right-click the Notification Server computer on which you want to run a report.
3. Click **Reports** and click the appropriate report.
4. In the report page, specify any parameters that you want to use, and refresh the report.

Chapter 5

Understanding standalone replication

This chapter includes the following topics:

About replication

Replication is the one-way transfer of data between two Notification Servers.

See "Replication requirements" on page 34.

See "About configuring replication" on page 37.

Replication lets you replicate the following between Notification Servers:

- Configuration and management items, such as reports, resource targets, policies, and tasks
- Resources, such as computers, users, and packages
  When you replicate resources you can verify the data that is replicated by entering a Data Verification percentage in the rule.
- Events, such as software delivery execution
- Security settings, such as roles, privileges, and permissions

---

Note: Replication replaces Inventory Forwarding and Package Replication Solution in Notification Server 7.0.

The stand-alone replication functionality that is described here is different from hierarchy replication. Stand-alone replication defines the information flow between

two Notification Servers. Hierarchy replication provides reliable and scalable data synchronization between multiple Notification Servers.

Replication can be configured to replicate data outside the hierarchy structure. For example, by sending data to an external server that collates particular information for reports.

The following replication types are supported:

Differential	Replicates the objects and the data that have changed since the last replication. This method is the recommended method because it reduces the network load and bandwidth consumption when data is replicated.
Complete	Replicates all objects and data. This method is commonly used for hierarchy replication. A complete replication is typically performed monthly to ensure full replication.

Another difference between hierarchy replication and replication is that within a hierarchy, the replicated data is secured and (by default) read-only. Ownership applies so that child Notification Servers cannot automatically overwrite the data that has been replicated down from the parent Notification Servers. Some data includes the settings that enable it to be editable on the destination, and these can be configured as appropriate. Replication has no such ownership, so all replicated data can be edited on the destination Notification Servers.

Replication requirements

The requirements for configuring replication in your Notification System must be satisfied before you configure any replication.

The requirements are as follows:

- Network traffic must be routable between Notification Servers.
- HTTP/HTTPS traffic must be permitted between Notification Servers.
- Trust relationships must exist between Notification Servers, or credentials for the privileged accounts that facilitate trust must be known.
- Each Notification Server must be able to resolve the name and the network address of any Notification Server with which it replicates data.
- There must be sufficient bandwidth between Notification Servers to support package and data replication.
  Required bandwidth and hardware depends on the size of your infrastructure topology and the data replicated.

- Each Notification Server must have a site server that is running the package service available. The package service must serve the Notification Server computer.

See "About replication" on page 33.

See "About configuring replication" on page 37.

Chapter 6

Setting up and using standalone replication

This chapter includes the following topics:

About configuring replication

Before you start replicating data from one Notification Server to another, you need to plan your replication. This is to ensure that similar data is not passed in both directions. If any of your servers are part of a hierarchy, you need to ensure that the replication does not conflict with the hierarchy replication process. Notification Server does not check to ensure that your replication configuration is consistent with the hierarchy. A poorly planned implementation may create data clashes or overwrites in the affected CMDBs.

See "About replication" on page 33.

See "Replication requirements" on page 34.

See "Configuring replication rules" on page 38.

To configure replication, you need to set up the appropriate replication rules on each Notification Server. Each rule specifies the data to replicate from that server (the source server) to one or more specified destination servers and the schedule to use. You should use different replication schedules for each Notification Server.

For example, stagger the times to ensure that each runs at a different time. Replicating to and from multiple Notification Servers at the same time can cause problems in the CMDB.

The rule must be enabled for the specified replication to take place. You can enable and disable replication rules at any time, according to the needs of your organization. For each rule that is enabled, the specified data is replicated according to the defined schedule.

You can replicate data at any time by running the appropriate replication rules. Running a replication rule overrides its schedule and replicates the specified data to the destination servers immediately. Running a replication rule is a once-only operation and does not change the replication schedule. All replication rules continue to be run as scheduled.

Table 6-1 Replication rule types

Type	Description
Events	Replicates Notification Server events.
Items	Replicates Notification Server configuration and management items such as policies, filters, and reports.
Resources	Replicates Notification Server resource types, resource targets, and specific data classes. If you include resource targets in a resource replication rule, remember that resource scoping applies to the contents (resources) of the replicated target. Therefore, the resources that are replicated depends on the owner of the resource target. The Notification Server administrator can choose to replicate resource targets in their current state (owned by somebody else, with the corresponding scope). Alternatively, they can take ownership of the targets, save them with the administrator's scope (which usually contains more resources) and replicate them in that state. All the current members of a resource target are replicated. The actual resource target item is replicated in the background as a dependent item.
Security	Replicates Notification Server security roles and privileges. Two types of security replication rules are available: Privilege and Role. The configuration procedure is identical for each. When you include a security role in a replication rule, you must also configure a replication rule to replicate all of the privileges in the role. The replicated security role does not recognize any privileges that already exist on the destination Notification Server.

Configuring replication rules

The replication rules that you configure on a Notification Server are items on that server. Therefore it is possible to replicate them to other Notification Servers. You may want to set up your item replication rules to ensure that replication rules are not included.

When a replication rule is replicated, its settings remain unchanged. A rule that is enabled on the source server is immediately enabled on the destination servers. However, the destination that is specified in the replication rule cannot be resolved. Each Notification Server uses its own unique GUIDs to identify resources, so the destination is valid only on the source Notification Server. You need to update the replication rule to point to the correct destination Notification Server.

See "About replication" on page 33.

See "About configuring replication" on page 37.

To configure a replication rule

1. In the Symantec Management Console, in the **Settings** menu, click **All Settings**.
2. In the left pane, expand the **Settings > Notification Server > Replication** folder.
3. In the Replication folder, do any of the following:

Create a new replication rule	Right-click the appropriate folder and click **New > Replication Rule**. The new rule appears in the folder and is selected automatically.
Modify an existing replication rule	Expand the appropriate folder, and then select the replication rule that you want to modify.
Enable or disable a replication rule	Expand the appropriate folder, and then right-click the replication rule and click **Enable** or **Disable**, whichever is appropriate. You can also enable or disable a rule in the Replication Rule page, by clicking the rule status (On/Off) icon to toggle the setting.
Run a replication rule	Expand the appropriate folder, and then right-click the replication rule that you want to run and click **Run**.

4. On the Replication Rule page, specify the appropriate settings.

   See "Replication rule settings" on page 39.
5. Click **Save Changes**.

Replication rule settings

Some replication rule settings apply only to a particular rule type.

See "About configuring replication" on page 37.

See "Configuring replication rules" on page 38.

Table 6-2 Replication rule settings

Setting	Description
Rule name and description	The first line of the page heading is the name of the replication rule. The second line of the page heading is its description. To change these, you can click the text to make it editable, and then type the rule name or description.
Rule status symbol	The current status of the replication rule: ■ On (Green light) – The rule is active. ■ Off (Red light) –The rule is idle. You can click the symbol to toggle the status to its alternative setting.
Resource Types Resource Targets	Applies to resource replication rules and event replication rules. Specifies the resources that you want to replicate. These two options are alternatives. You can click the appropriate option to activate the one that you want: ■ **Resource Types** Replicates the selected resource types. If you choose this option, you need to click **Resource Types**. In the **Select Resource Type** window, select the resource types that you want to include. ■ **Resource Targets** Replicates the selected resource targets. If you choose this option, you need to click **Resource Targets**. In the **Select a Group** window, select the resource targets that you want to include.
Data Classes	Applies to resource replication rules only. If you want to specify particular data classes to include, you need to click **Data Classes**. In the **Inventory Data Classes** window, select the classes that you want.
Event Classes	Applies to event replication rules only. The event classes to include. To select these, click **Event Classes** and, in the **Event Classes** window, select the classes that you want.
Items	Applies to item replication rules only. The items to include in the replication rule. To select these, click **Items** and, in the **Select Items** window, select the items that you want.

Table 6-2 Replication rule settings *(continued)*

Setting	Description
Roles Privileges	Applies to security replication rules only. The roles or privileges to replicate, according to the rule type. These settings are alternatives and only the appropriate option is displayed on the page. To select these, click **Roles/Privileges** and, in the Select Roles/Privileges window, select the roles or privileges that you want.
Destination	The Notification Server computers to which the data is replicated. See "Specifying destination Notification Servers in a replication rule" on page 41.
Credentials	The credentials that are required to connect to the destination Notification Servers.
Maximum Rows	Applies to event replication rules only. Specifies the maximum number of table rows to replicate.
Resend events that have been sent previously	Applies to event replication rules only. You should use this option if a destination server has recently purged its event classes or if you have experienced network problems between servers.
Use this schedule	In the drop-down list, select the schedule that you want to use. If you select Custom Schedule, you need to click **Define Custom Schedule** and, in the Schedule Editor, specify the schedule parameters.
Verify maximum of nn% of data during each replication	Applies to resource replication rules only. To reduce the load that is imposed on the server, you can verify small amounts of resource data on every replication. You can specify a verification percentage in the replication rule. For example, if you verify 10% of the data for each replication, that ensures that all data has been verified after 10 replications.

Specifying destination Notification Servers in a replication rule

You need to specify the Notification Server computers to which a replication rule replicates data. This procedure is the same for all replication rule types.

See "About replication" on page 33.

See "Replication requirements" on page 34.

See "About configuring replication" on page 37.

See "Configuring replication rules" on page 38.

To specify the destination Notification Servers in a replication rule

1. On the Replication Rule page, click the text beside the **Destination** field.
2. In the **Notification Servers** window, in the **Available Notification Servers** list, select the appropriate destination Notification Servers.
3. If necessary, you can add new Notification Servers to the list, or modify existing Notification Servers.

   See "Adding or modifying an available Notification Server " on page 42.
4. Click **Save Changes**.

   The selected Notification Servers are listed in the Destination field.

Adding or modifying an available Notification Server

If necessary, you can add new Notification Servers to the list of those available, or modify existing Notification Servers.

See "Specifying destination Notification Servers in a replication rule" on page 41.

To add or modify an available Notification Server

1. Do one of the following:

To add a new Notification Server	Click **Add**.
To modify an existing Notification Server	In the **Available Notification Servers** list, select the Notification Server computer that you want to modify, and then click **Edit**.

2. In the **Add a Notification Server by name or browse the network** window, enter the appropriate details in the following boxes:

   Notification Server Name

   Notification Server Web Site

3 If you want to select the Notification Server computer from your network, click **Browse**.

In the **Browse for Computer** dialog box, select the appropriate Notification Server.

4 Click **Add**.

The system connects to the specified server, verifies that it is suitable, and then adds it to the list of available Notification Servers.