



DomainPatrol 5.0

How to install and configure

Version 1.0

Copyright Information

©2008 DomainPatrol AB

Under the copyright laws, this document may not be photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form, in whole or in part, without the prior written consent of DomainPatrol AB.

While every reasonable precaution has been taken in the preparation of this document, the author assumes no responsibility for errors or omissions, nor for the uses made of the material contained herein and the decisions based upon such use. No warranties are made, express or implied, with regard to either the contents of this work, its merchantability, or fitness for a particular purpose. The author shall not be liable for direct, indirect, special, incidental, or consequential damages arising out of the use or inability to use the contents of this document.

In no event shall the author be liable for any damages whatsoever (including without limitation, damages for loss of business profits, business interruption, loss of business information, or any other loss) arising out the use of or inability to use this material, even if the author has been advised of the possibility of such damages.

Lotus, Domino, Domino Designer, LotusScript, Lotus Notes, Notes and Sametime are trademarks or registered trademarks Lotus Development Corporation and/or IBM Corporation. IBM, S/390, AIX, DB2, and WebSphere are registered trademarks of International Business Machines, Incorporated. Windows is a trademark of Microsoft Corporation. Microsoft is a registered trademark and Windows, ActiveX, and Visual Basic are trademarks of Microsoft Corporation. Java and JavaScript are trademarks of Sun Microsystems, Inc.

All other marks are the property of their respective owners.

Table of Contents

Introduction - The Features of DomainPatrol	5
Key points	5
What DomainPatrol is.....	5
What DomainPatrol is NOT	6
Major administrator task areas.....	7
Step 1 - Install the DomainPatrol Application.....	8
Key points.....	8
Platforms supported by DomainPatrol.....	8
Obtain the DomainPatrol Template	8
Pre-installation: signer ID.....	9
Sign the DomainPatrol Template.....	9
Upgrading the DomainPatrol Database	9
Create a new DomainPatrol Database.....	9
Customize the DomainPatrol Database ACL.....	10
Import the DomainPatrol Licenses	11
Result.....	12
Step 2 – Pre configuration planning	13
Key points.....	13
To centralize or distribute?	13
Connectivity and Domino Server names	14
Authorizations.....	14
Decide what to include in the DomainPatrol Inventory.....	15
DomainPatrol Scanner Logging Options	21
Step 3 - Configure the Scanners	24
Key points.....	24
Create a new Scanner.....	24
Scanner Context.....	24
What to include in the Inventory	25
What to exclude from the Inventory	25
Logging options.....	26
Test Authorization	27
Step 4 - Run the Scanner	32
Key points.....	32
Running the DomainPatrol Client Scanner.....	32
Running the DomainPatrol Server Scanner	32
Scheduling the DomainPatrol Server Scanner	33
Troubleshooting.....	36
Scanner Logs	36
Error Logs.....	36

Description

This document will walk you thru the installation and configuration of the DomainPatrol Application and give you a brief overview of the features of DomainPatrol.

If you are looking for more in depth information on using the specific DomainPatrol features for administration or documentation refer to the documents DomainPatrol 5.0 Administration and DomainPatrol 5.0 Documentation.

Document goals

In this document you will learn:

- What DomainPatrol is
- What to use DomainPatrol for
- How to install and configure the DomainPatrol Application
- What information is stored in the DomainPatrol Inventory
- How to schedule the DomainPatrol Server Scanner

Audience

This document is part of a series of DomainPatrol Administration training documents.

This document is designed for Domino administrators who are responsible for installation of new applications in the Domino infrastructure and who:

- have a good understanding of Domino administration
- understands the access rights for server administration and execution of agents using unrestricted access
- have a good knowledge of the Domino infrastructure and server connectivity

For more information on using DomainPatrol for administration of Domino refer to the document DomainPatrol 5.0 Administration.

For more information on using DomainPatrol for documentation of databases refer to the document DomainPatrol 5.0 Documentation.

Document design

This document will give you the knowledge needed to make the right decisions when installing and configuring DomainPatrol. It will also guide you thru the installation steps.

Introduction - The Features of DomainPatrol

Key points

DomainPatrol is an extensible Administration Tool to:

- Investigate
- Control
- Document

Lotus Notes & Domino Applications.

What DomainPatrol is

The DomainPatrol Scanner crawls servers and databases and stores information about these in the DomainPatrol Inventory.

The Inventory contains filters and actions to find and control databases, templates, acl entries, agents and scriptlibraries.

The DomainPatrol Tools are designed to be able to run on multiple instances of the items in the inventory. For example you can resign all agents found by a specific filter regardless of where they are located, in multiple databases or even on multiple servers. This is a big benefit compared to using the Domino Administrator client where you can only control databases on one specific server at a time.

All items contained within the DomainPatrol Inventory can be filtered using Full Text searching. For example you can search for all your databases using a specific template and is located in a specific directory on any of your servers and has a specific user set as the access accountable. DomainPatrol is the only product on the market today that provides this kind of functionality for Lotus Notes & Domino administration.

Whenever you have found all the databases you are looking for using either a predefined filter or using a Full Text search you can use the action tools to make changes to all of the selected databases at once without worrying about what servers they are located on.

DomainPatrol has been designed to support organizations using ITIL (Information Technology Infrastructure Libraries) methodology to manage their IT environment. In support of this you can use DomainPatrol Documentation as a light weight CMDB (Configuration Management Database). Using the DomainPatrol Documentation function you can group databases into CIs (Configuration Items) and store documentation within those CIs. Within the CIs you can assign database responsibility roles like:

- Lifecycle accountable
- Access accountable
- Design accountable

Using the DomainPatrol Documentation you can also define dependencies and use relationships between CIs. Any database item from the DomainPatrol Inventory can be defined by a CI in the DomainPatrol Documentation.

DomainPatrol is extensible in two different ways.

1. Open Source Design

The DomainPatrol Database design and all the filters and action tools are open source. This makes it easy for you to:

- Create specific views or actions based on existing ones in the design
- Integrate with external systems such as help desk applications or external CMDBs

2. DomainPatrol Power Tools

DomainPatrol Power Tools are add in modules that you can create on your own. The DomainPatrol Power Tools can be exported and imported to and from files so they can also be shared with other users of DomainPatrol.

There are a few really powerful DomainPatrol Power Tools published for download on the DomainPatrol homepage.

Examples of DomainPatrol Power Tools are:

- Report User Access Level for selected databases
- Set ACL for mail file Owners to Editor
- Find all mail enabled databases
- Set Quota for selected databases to 20MB above the current size
- Restore folder structure in mail database from backup

What DomainPatrol is NOT

DomainPatrol do not enforce security based on the documentation for specific databases or roles. For example a database access accountable does not get manager access to databases because they are listed as the databases access accountable in the documentation for the database this is still handled by the Domino Server checking the access levels in the ACL of the database.

DomainPatrol is not a real-time monitoring tool. As the DomainPatrol Scanner gathers information on a scheduled basis and stores this information within the DomainPatrol Inventory the information within the Inventory can be out of date if changes are made directly to a database using the Domino Administrator client until the next scan is executed.

DomainPatrol do not circumvent the Domino Security Model. This means that you can only perform changes using DomainPatrol that the Database and Server Access Control Lists authorize.

Domainpatrol is not a full featured CMDB as defined in ITIL(Information Technology Infrastructure Libraries) v3.

Major administrator task areas

Now that you know what DomainPatrol is, here is a very high-level list of what administrators need to know how to do:

- Install and configure the DomainPatrol Database
- Decide what information should be stored within the Inventory
- Schedule the DomainPatrol Scanner
- Using the various filters to find items in the Inventory
- Using the various action tools to make changes to items in the Inventory
- Download and use various Power Tools
- Document databases using the DomainPatrol Documentation features

Step 1 - Install the DomainPatrol Application

Key points

Installing the DomainPatrol Database is pretty much like installing any database from a template. The important points is to make sure the ACL is correct and that you use a signer that has the correct privileges to run the scanner.

Platforms supported by DomainPatrol

All of the DomainPatrol Scanner features are supported on Domino version 6.5.4 or later running on a Windows 32 bit platform.

The scanner will run on any Domino supported platform version 6.5 or later with reduced functionality. The scanning feature that is not implemented for non Windows 32 bit platforms is the scanning of Database usage.

The scanner does not support scanning a Domino server version 5 or earlier.

Obtain the DomainPatrol Template

The DomainPatrol Template is downloaded as a compressed zip archive file from the DomainPatrol Web site at the following url:

<http://domainpatrol.org/downloads>

To be able to download the DomainPatrol Template you need to register for a free account on the DomainPatrol web site.

When you have downloaded the archive file you can open it using windows explorer.

If you are using any other platform you can extract the contents of the compressed archive file using any program that handles zip compression. For example 7zip that you can download for free on the Web.

When you have extracted the contents of the archive file, copy the template file ddp.ntf to the Lotus Notes data directory on your client.

Pre-installation: signer ID

For the DomainPatrol Server Scanner to be able to run it needs “Unrestricted” privileges on the server it will run on. The signer of the agent should be added to the field “Sign or run unrestricted methods and operations:” on the security tab of the server document for the server where the scanner is set-up to run on.

We recommend that you use a specific signer ID for the purpose of signing the DomainPatrol Database agent to make it easier and more secure to:

- Add the signer ID to the security fields on the servers where the scanner will run
- Add the signer ID to the ECL (Execution Control List) on the clients using the DomainPatrol Database.

Sign the DomainPatrol Template

When you have decided on what signer ID to use you open the Domino Administrator client using the signer ID and sign the DomainPatrol Template using that signer ID.

Upgrading the DomainPatrol Database

If you are upgrading the DomainPatrol Database from a previous version you need to:

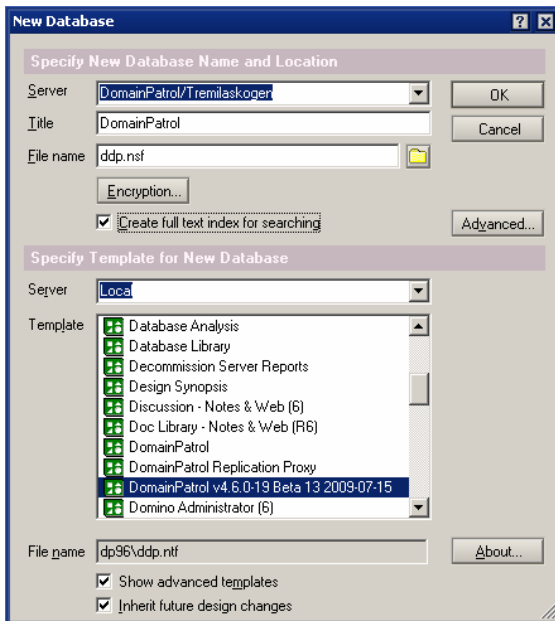
- Refresh the DomainPatrol Database design from the new Template
- Customize the DomainPatrol ACL roles to only contain:
 - [Administrator]
 - [PowerTools]
 - [YtriaTools]
- Remove and reinstall licenses
- Remove all configuration documents and recreate them

Create a new DomainPatrol Database

Some of the DomainPatrol Filters and Action Tools are designed to use the Domino directory on the server where the DomainPatrol Database is located for lookup of information about servers, users and groups in the Domain.

For this reason you should create the DomainPatrol Database on a server in the Domain that you want to administrate using DomainPatrol.

Create a new database using the Lotus Notes client menu action “File”-“Database”-“New”.



- Choose the server where the DomainPatrol Database is to be created.
- You can choose any title for the Database such as “DomainPatrol”
- You should not include any non ASCII characters or spaces in the filepath for the DomainPatrol Database. We recommend that you name it ddp.nsf and place it in the root folder of your server.
- For full functionality we recommend that you select to create a full text index for searching the DomainPatrol Database.
- For the template to be displayed you need to select “Show advanced templates” in the dialog.

The DomainPatrol Template is named “DomainPatrol “ and suffixed with a version number and release date. For example “DomainPatrol 5.0 2009-08-01”

- Click OK and the DomainPatrol Database will be created.

Customize the DomainPatrol Database ACL

The different users that need access to the DomainPatrol Database can be grouped as the following:

- DomainPatrol/Domino Administrator
- Scanning servers
- Domino Administrator using the DomainPatrol Power Tools
- Domino Administrator using the Ytria Tools
- Developer/Administrator updating documentation for databases
- End user

DomainPatrol/Domino Administrator

This is the person responsible for configuring the DomainPatrol Database. This user needs the [Administrator] role and at least editor access with the privilege to delete documents.

This is probably the same person that creates the DomainPatrol Database – in this case you need to add the [Administrator] role to yourself.

Domino Administrators also need this accesslevel and the role [Administrator] to be able to use all the filters and actions tools in the Inventory.

Scanning servers

The servers where the DomainPatrol Scanner will run need to be able to load the agent in the DomainPatrol Database and create and delete any document.

This means that the servers should have at least Editor access with the privilege to delete documents.

By default the ACL will contain the group LocalDomainServers assigned Manager access to accomplish this.

Domino Administrator using the DomainPatrol Power Tools

This is the most common group of users of the DomainPatrol Database. They should have at least Editor access with the role [PowerTools] enabled.

Domino Administrator using the Ytria Tools

Users that have installed Ytria Tools from Ytria Inc can start the Ytria tools to run on selected items in the Inventory. For this to work they need the role [YtriaTools] enabled in the ACL.

Developer/Administrator updating documentation for databases

Users that only needs to update documentation for databases should have Editor access and no explicit role in the ACL is needed.

End user

End users can use the DomainPatrol Inventory to find and open databases. For these users Reader access without any roles is sufficient.

Summary

When you have finished customizing the ACL you need to close the DomainPatrol Database and reopen it for the [Administration] role to be effective. This is needed when you go to the next step and import the DomainPatrol Licenses.

Import the DomainPatrol Licenses

Open the DomainPatrol Database and navigate to “Setup” – “Licenses”.

DomainPatrol provides to different license types:

- Server Licenses
- Client Demo Licenses

The DomainPatrol Licenses can either be mailed to you as an attached license file or if you only need the DomainPatrol Client Demo Licenses they can be downloaded from the DomainPatrol Licenses view directly.

If you have a license file it can be imported using the action “Import license file...” found in the DomainPatrol Licenses view.

Result

At this stage of the installation you should have done the following:

- Created a DomainPatrol Database
- Customized the DomainPatrol Database ACL
- Installed the licenses in the DomainPatrol Database

Step 2 – Pre configuration planning

Key points

The DomainPatrol Scanner is used to gather information about all databases on your servers that should be included in the DomainPatrol Inventory.

There are a few different options on how to configure the DomainPatrol Scanner for different infrastructures and there are some differences on how you would configure this in DomainPatrol version 4.x and 5x.

These instructions will only cover version 5.x. although the decisions for the different configurations are the same in all versions.

These instructions will give you a good understanding on the different options and how to configure them.

To centralize or distribute?

The DomainPatrol Scanner can run either distributed on all servers or just on one server reaching out to scan all other servers.

Configurations

- Hub and spoke topology where each server will scan its own databases.
- Hub and spoke topology where the hub server will scan all spokes servers sequentially.
- Mesh where the DomainPatrol Database is replicated to every server.
- DomainPatrol Client Scanner

Note: In the Hub - Spoke scenarios only one DomainPatrol Database will be needed on the Hub server. The spokes servers are the once to be scanned. The hub server can scan itself in both of the “Hub and spoke topologies”.

How do I decide what configuration to use?

The differences lye in speed, resource utilization and security settings.

	<i>Speed</i>	<i>Security Configuration</i>	<i>Network Utilization</i>	<i>Disk usage</i>	<i>CPU Utilization</i>	<i>Memory Utilization</i>
Hub - Spoke Scanner on each server	Very High	Medium	Medium	Low	Medium	Medium
Hub – Spoke Scanner on one server	Low	High	High	Low	Low	Low
Mesh – Database on each server						
Scanner on each server	Medium	Medium	Low	Very High	High	High
DomainPatrol Client Scanner	Very Low	Low	High	Low	Low	Low

Table compares the different scanner configurations

Recommendations

The impact of running the DomainPatrol Client Scanner is minimal on the servers resource utilization and needs minimal security configuration but it is extremely slow compared to running any configuration using the DomainPatrol Server Scanner.

Replicating the DomainPatrol Database to each server to scan will consume a lot of disk space as the DomainPatrol Database tends to get very large and it is also not recommend when using the different tools to make changes to the databases in the DomainPatrol Inventory. This configuration could be interesting for investigation if the network connection is very limited between the site where administrators use the DomainPatrol Database and the server that should be scanned.

I would recommend using the Hub - Spoke configuration with one server to scan the others only for servers that are part of a Domino partition. In this configuration there would be a high impact for running the scanner simultaneously on all the servers that share the same hardware.

This boils down to the recommendation to configure the DomainPatrol Server Scanner so that each server will run its own scanner and use a hub server to store the DomainPatrol Database.

Connectivity and Domino Server names

For the DomainPatrol Server Scanner to find the server where the DomainPatrol Database is located the server name for the server hosting the DomainPatrol Database can not contain any spaces or non ASCII characters.

If you are in a situation where the name of the server hosting the DomainPatrol Database do contain spaces or non ASCII character, please contact DomainPatrol Support for more information on how to solve this.

To verify the connectivity from the server to run the DomainPatrol Server Scanner to the server hosting the DomainPatrol Database – issue a trace command on the server to run the DomainPatrol Server Scanner with the common name of the server hosting the DomainPatrol Database.

Authorizations

DomainPatrol Client Scanner

To be able to run the DomainPatrol Client Scanner you need authorization to send server commands to the servers you want to scan.

DomainPatrol Server Scanner

For the DomainPatrol Server Scanner to be able to run it needs "Full Access" privileges on the server it will scan. The **signer** of the agent should therefore be added to the field "Sign or run unrestricted methods and operations:" on the security tab of the server document for the servers that will run the DomainPatrol Server Scanner.

If you want to configure the DomainPatrol Server Scanner to scan another server than the one it is running on you should also grant "Full Access administrators:" rights to the **server** running the DomainPatrol Server Scanner on the server to scan.

Note: There is no need in DomainPatrol version 5.x to grant any server "Trusted servers:" access as was the case in DomainPatrol version 4.x using the Java based scanner.

Summary

If you will only run the DomainPatrol Client Scanner **you** need to have rights to issue server console commands to the servers you want to scan. The minimum authorization required is "View-only Administrators:" in the server documents for the servers you want to scan.

If you configure the DomainPatrol Server Scanner to run on each server then you need to:

1. add the **signer** to the following field on the server that will run the DomainPatrol Server Scanner:
 - "Sign or run unrestricted methods and operations:"

If you configure the DomainPatrol Server Scanner to run on one server to scan all other servers you need to:

2. add the **signer** to the following field on the server that will run the DomainPatrol Server Scanner:
 - "Sign or run unrestricted methods and operations:"
3. add the **server** that will run the DomainPatrol Server Scanner to the following fields on all servers that will be scanned:
 - "Full Access administrators:"

Decide what to include in the DomainPatrol Inventory

The DomainPatrol Inventory can contain a lot of information about the databases on your servers. It is possible to limit the information stored within the DomainPatrol Inventory to only the items that are of interest to you on a day to day basis.

If you choose to store less information in the DomainPatrol Inventory the DomainPatrol Scanner will run faster and the size of the DomainPatrol Database will be smaller.

The following sections will give you detailed information on all the options.

Database details

All of the information stored in the DomainPatrol Inventory is read from the databases on your servers. If you choose not to include database details then you will only store a small part of the database information.

Choosing not to include database details will limit the items stored in the DomainPatrol Inventory to only contain databases and only the following fields for those databases:

- Server
- File Path
- Title
- Design Template Name
- Template Name
- Replica ID
- Size
- Percent used
- ODS version
- Quota
- Warning threshold
- Transaction logging
- DAOS Enabled
- Last compacted
- Categories

Choosing “Database details” will add the following fields to the database documents in the DomainPatrol Inventory:

- Admin Server
- Is Mail database
- Is Mail Archive
- Mail database owner
- Created date
- Last modified
- Design last modified
- Number of document
- Use JavaScript when generating pages
- Require SSL connection
- Don't allow URL open
- Allow design locking
- Show in open database dialog

- Include in multi database indexing
- Mark modified documents as unread
- List as advanced template in “New Database” dialog
- Copy profile documents with design
- Single copy template
- Multilingual
- Default language
- Default region
- Default sort order
- Unicode standard sorting
- Optimize document table map
- Overwrite free space
- Maintain last accessed property
- Enable transaction logging
- Support specialized response hierarchy
- Use LS1 compression for attachments
- Allow headline monitoring
- Allow more fields in database
- Allow soft deletion
- Soft deletion expire time in hours
- Limit entries in \$UpdatedBy fields
- Limit entries in \$Revisions fields
- Maintain unread marks
- Allow background agents
- Allow use of stored forms
- Display images after loading
- Allow document locking
- Allow connections to external databases using DCRs
- Replication: abstract
- Replication: cutoff date
- Replication: cutoff delete
- Replication: cutoff interval

- Replication: disabled
- Replication: Don't send local security updates
- Replication: Ignore deletes
- Replication: Ignore destination deletes
- Replication: Priority

Database usage and exclusion list

When you choose to include database details you can also choose to include “Database usage”.

Database usage stores information in the DomainPatrol Database Documents about the uses of the database. You can choose to exclude specific servers, users and groups from the statistics of the Database usage using the exclusion list.

For example you might not want to include statistics for LocalDomainAdmins and LocalDomainServers in the Database usage information.

To exclude specific servers, users and groups add them to the field “Database usage exclusion list”

When you choose to include “Database usage” the following fields will be added to the database documents in the DomainPatrol Inventory:

- Number of Uses for:
 - Last Day
 - Last Week
 - Last Month
 - Last ## of days
- Number of Reads for:
 - Last Day
 - Last Week
 - Last Month
 - Last ## of days
- Number of Writes for
 - Last Day
 - Last Week
 - Last Month
 - Last ## of days
- List of usernames for:
 - Last Day
 - Last Week

- Last Month
- Last Period

As the amount of usage data contained within any Domino database is limited the period for the usage data might be limited. When the limit is reached the oldest information is discarded and replaced by the most recent database usage information. This is the reason that there are fields that show “Last ## of days” which will be the number of days contained in the usage data and “Last Period” which will contain the whole list of usernames for the period that the usage data contains.

ACL Entries

When you choose to include database details you can also choose to include “ACL Entries”.

The ACL Entries will be stored in separate items from the database items in the DomainPatrol Inventory.

The ACL Entries are displayed in special views in the DomainPatrol Inventory with the ability to run filters and action tools against them directly.

The ACL entries contain the following fields:

- Database: Server
- Database: File Path
- Database :Title
- ACL Entry: Full Name
- ACL Entry: Level
- ACL Entry: Roles

Agents

When you choose to include database details you can also choose to include “Agents”.

The Agents will be stored in separate items from the database items in the DomainPatrol Inventory.

The Agents are displayed in special views in the DomainPatrol Inventory with the ability to run filters and action tools against them directly.

The Agents contain the following fields:

- Name
- Alias
- Commend
- Updated by
- Last modified
- Path
- Last run

- Exit code
- Enabled
- Was signed by
- Trigger
- Schedule
- Run location
- Run server
- Show in search
- Run as web users
- Run on behalf of
- Activatable
- Client background thread
- Allow remote debugging
- Store highlights
- Formula type
- Restrictions
- No refresh
- Propagate No replace
- Hide
- Public
- Private
- Designer version
- Inherit from template
- Code

It is possible to exclude the source code from the Agents by selecting “Exclude code”. This will limit the size of the DomainPatrol Database if you do not need the code for the Agents in the DomainPatrol Inventory.

Script libraries

When you choose to include database details you can also choose to include “Scriptlibraries”.

The Scriptlibraries will be stored in separate items from the database items in the DomainPatrol Inventory.

The Scriptlibraries are displayed in special views in the DomainPatrol Inventory with the ability to run filters and action tools against them directly.

The Scriptlibraries contain the following fields:

- Name
- Alias
- Commend
- Updated by
- Last modified
- Path
- No refresh
- Propagate No replace
- Hide
- Public
- Private
- Designer version
- Inherit from template
- Code

It is possible to exclude the source code from the Scriptlibraries by selecting “Exclude code”. This will limit the size of the DomainPatrol Database if you do not need the code for the Scriptlibraries in the DomainPatrol Inventory.

DomainPatrol Scanner Logging Options

When the DomainPatrol Scanner runs it will log its progress and any problems encountered. There are some options to choose on what to log and where to log this information.

Log Levels

The following information will be included in the DomainPatrol Scanner Log depending on what option is selected:

Verbose	<ul style="list-style-type: none">• Scanner start and end• Progress on reading the data store• Progress on database scan• Creation, updates and deletes on all items in the Inventory• Warning messages• Error messages• Fatal messages• Summary number of created, updated and deleted items in the
---------	---

	Inventory
Info	<ul style="list-style-type: none"> • Scanner start and end • Progress on database scan • Warning messages • Error messages • Fatal messages • Summary number of created, updated and deleted items in the Inventory
Warn	<ul style="list-style-type: none"> • Scanner start and end • Warning messages • Error messages • Fatal messages • Summary number of created, updated and deleted items in the Inventory
Error	<ul style="list-style-type: none"> • Scanner start and end • Error messages • Fatal messages • Summary number of created, updated and deleted items in the Inventory
Fatal	<ul style="list-style-type: none"> • Scanner start and end • Fatal messages • Summary number of created, updated and deleted items in the Inventory
No Log	Nothing

Console Log Level

The Console Log Level determines what will be displayed on the Domino server console and the Domino Server Log log.nsf file when running a DomainPatrol Server Scanner.

When you run a DomainPatrol Client Scanner the Console Log Level determines what will show in the DomainPatrol Client Scanner Progress Dialog.

Document Log Level

The Document Log Level determines what information will be stored in a Scanner Log Document in the DomainPatrol Database.

You can choose the “No Log” option if you don’t want any Scanner Log Documents stored in the DomainPatrol Database.

E-mail Document Log Recipients

You can choose to e-mail the Scanner Log Document to any recipient when the DomainPatrol Scanner has finished.

File Log Level

The File Log is stored in a DomainPatrol.log file in the Domino Data directory on the server where the DomainPatrol Server Scanner is running.

When you run the DomainPatrol Client Scanner the File Log is created in the Lotus Notes Data directory on your client.

The recommendation is to not use the File Log unless necessary.

Step 3 - Configure the Scanners

Key points

From the previous chapter you will have a good idea of what you want to Include in the DomainPatrol Inventory, what logging options you want for the DomainPatrol Scanner and where to run the DomainPatrol Scanner.

This chapter will help you configure the DomainPatrol Scanners and select the options that are right for your Domino Domain.

Create a new Scanner

1. Open the DomainPatrol Database and navigate to “Setup” – “Scanners”
2. Select “new Scanner”

A new Scanner Configuration Document will be created where you specify all configuration options for the Scanner.

Scanner Context

Where to run the DomainPatrol Scanner

Select wheter you want this Scanner to run from a Client or on a Server.

Scanner Name

If you choose to run the Scanner from a Client you need to give this Scanner a Name. Do not use hierarchical names that include the / character.

NOTE: In previous releases you could specify “default” as the name of the Scanner to get specific functionality. In DomainPatrol version 5.0 you can use default as the Scanner Name like any other name, it will not be treated differently.

Server to run the DomainPatrol Scanner

If you choose to run the Scanner on a Server you need to specify which server this Scanner should run on.

NOTE: In previous releases you could specify “default” as the name of the server to run the Scanner to get specific functionality. In DomainPatrol version 5.0 you can not use default as the name of the server to run the Scanner.(If your server is named “default” then it is of course valid to use it as the name of the server to run the Scanner)

Servers to scan

A list of servers that will be scanned by this Scanner. Servers can be added by typing their name (separated by semi colon), but more often by clicking the button to open the Select Names window. This will bring up a list of all Licenses installed in the DomainPatrol Database. Select Servers to scan in the left margin. Click the OK button when you are finished.

What to include in the Inventory

Database details

Choose whether to scan Database details or not. No means that only basic information will be gathered.

Yes means that all the Database advanced properties will be included. Further options will appear;

Database usage

Includes usage statistics for the databases.

Database Usage Exclusion List

Select the persons, servers and groups to exclude from the Database Usage Statistics

Persons, servers can be added by typing their name (separated by semi colon). If you want to select groups click the button to open the Select Names window. Browse the Address Book and select person, servers and groups to exclude by clicking the Add button. Click the OK button when you are finished. The groups selected will be converted into the member names.

ACL entries

Includes ACL entries for the database.

Agents

Includes agents, the agent code, signer, triggers and schedules.

Select "Exclude code" if you do not want to include the Agents source code in the Inventory.

Script libraries

Includes script libraries, the code and signer.

Select "Exclude code" if you do not want to include the Script libraries source code in the Inventory.

What to exclude from the Inventory

These options lets you exclude databases based on file path pattern or design template name.

File path pattern

Can be used to exclude databases based on the path in the following format:

CN=Servername/OU=Organizational Unit/O=Organization!!folder/filename.nsf.

Wildcards can be used. Some examples:

mail/.nsf

Excludes all database files in the “mail” folder on all Servers.

CN=Server01/#!/restore/*

Excludes all files in the “restore” folder on the server Server01.

Design template name(s)

Excludes all databases based on these design templates. Write the names of the design templates that you want to exclude, separated by semicolon ‘ ; ’.

Logging options

The following information will be included in the DomainPatrol Scanner Log depending on what option is selected:

Verbose	<ul style="list-style-type: none">• Scanner start and end• Progress on reading the data store• Progress on database scan• Creation, updates and deletes on all items in the Inventory• Warning messages• Error messages• Fatal messages• Summary number of created, updated and deleted items in the Inventory
Info	<ul style="list-style-type: none">• Scanner start and end• Progress on database scan• Warning messages• Error messages• Fatal messages• Summary number of created, updated and deleted items in the Inventory
Warn	<ul style="list-style-type: none">• Scanner start and end• Warning messages• Error messages• Fatal messages• Summary number of created, updated and deleted items in the

	Inventory
Error	<ul style="list-style-type: none"> • Scanner start and end • Error messages • Fatal messages • Summary number of created, updated and deleted items in the Inventory
Fatal	<ul style="list-style-type: none"> • Scanner start and end • Fatal messages • Summary number of created, updated and deleted items in the Inventory
No Log	Nothing

Console Log Level

The Console Log Level determines what will be displayed on the Domino server console and the Domino Server Log log.nsf file when running a DomainPatrol Server Scanner.

When you run a DomainPatrol Client Scanner the Console Log Level determines what will show in the DomainPatrol Client Scanner Progress Dialog.

Document Log Level

The Document Log Level determines what information will be stored in a Scanner Log Document in the DomainPatrol Database.

You can choose the “No Log” option if you don’t want any Scanner Log Documents stored in the DomainPatrol Database.

E-mail Document Log recipients

You can choose to e-mail the Scanner Log Document to any recipient when the DomainPatrol Scanner has finished.

File Log Level

The File Log is stored in a DomainPatrol.log file in the Domino Data directory on the server where the DomainPatrol Server Scanner is running.

When you run the DomainPatrol Client Scanner the File Log is created in the Lotus Notes Data directory on your client.

The recommendation is to not use the File Log unless necessary.

Test Authorization

There are different authorizations needed depending on if you will run the DomainPatrol Scanner on the Client or the Server

The easiest way to get the authorizations correct is to first test the authorizations to run the DomainPatrol Scanner from the client and when this is working correctly move on to testing the authorizations to run the DomainPatrol Scanner on the server.

NOTE: You can run any DomainPatrol Scanner configured to run on the server from the Client as well.

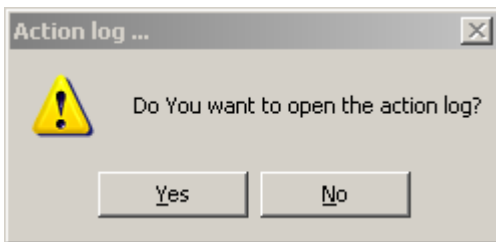
DomainPatrol Client Scanner

To be able to run the DomainPatrol Scanner on the Client you need at least “View-only Administrators:” authorizations to be able to send restricted console commands to the servers you want to scan.

You can test your authorization to send restricted console command to the servers you want to scan from the Licenses view in the DomainPatrol Database.

1. Open the DomainPatrol Database and navigate to “Setup” – “Licenses”
2. Select the servers in the view the you want to test your authorizations for
3. From the DomainPatrol Actions select “Server Tools” – “Run server command on selected servers”
4. In the dialog you type in “SHOW CONFIG SERVERNAME”

In the “Action log...” choose Yes to display a file containing the results of the command



This is an example of the results of the command where you have the correct authorizations for the two first servers but not the third.

```
server6/Tremilaskogen SHOW CONFIG SERVERNAME
SERVERNAME=server6/Tremilaskogen
-----
DomainPatrol/Tremilaskogen SHOW CONFIG SERVERNAME
SERVERNAME=DomainPatrol/Tremilaskogen
-----
DomainPatrol65/Tremilaskogen Notes error: You are not
authorized to use the remote console on this server
-----
```

If you get the message “Notes error: You are not authorized to use the remote console on this server” for any of your servers that means that you do not have proper authorizations to send restricted server commands to that server.

To enable you to run restricted server commands to that server:

1. Open the names.nsf database on that server
2. Navigate to the view “Configuration”-“Servers”-“All Server Documents”
3. Open the server document for the server where you need access
4. Navigate to the tab “Security”
5. In the section “Administrators” the field “View-only Administrators:” needs to either contain:
 - Your name
 - A group that you belong to

NOTE: The administrator fields are hierarchical in that the fields granting more rights also include the rights from the other fields.

The administrator fields grant access privileges in the following order where the higher level also includes the authorizations of the lower levels:

1. Full Access Administrators
2. Administrators
3. Full Remote Console Administrators
4. View-only Administrators

This means that if you are listed in any administrator field with higher authorization than “View-only Administrator” you will also have access to issue restricted server console commands.

DomainPatrol Server Scanner

To be able to start, stop and schedule the DomainPatrol Server Scanner you need to have at least “Full Remote Console Administrators” access to the server.

You can verify that you have this access in pretty much the same way as described in the previous section on testing for authorization to run the DomainPatrol Client Scanner.

Instead of issuing the server console command “SHOW CONFIG SERVERNAME” you can try to make a change or set a notes.ini parameter by issuing the server console command “SET CONFIG DOMAINPATROL=TEST” instead.

If this was successful you can remove the DOMAINPATROL notes.ini variable by issuing the command “SET DOMAINPATROL=” after the test has completed.

To be able you to run unrestricted server console commands to the server:

1. Open the names.nsf database on that server
2. Navigate to the view “Configuration”-“Servers”-“All Server Documents”
3. Open the server document for the server where you need access
4. Navigate to the tab “Security”
5. In the section “Administrators” the field “Full Remote Console Administrators:” needs to either contain:
 - Your name
 - A group that you belong to

NOTE: The administrator fields are hierarchical in that the fields granting more rights also include the rights from the other fields.

The administrator fields grant access privileges in the following order where the higher level also includes the authorizations of the lower levels:

1. Full Access Administrators
2. Administrators
3. Full Remote Console Administrators

This means that if you are listed in any administrator field with higher authorization than “Full Remote Console Administrators” you will also have access to issue unrestricted server console commands.

For the server to be able to load the DomainPatrol Server Scanner Agent the signer of the DomainPatrol Database needs to have the authorization “Sign or run unrestricted methods and operations” set in the server document on the “Security” tab in the section “Programmability Restrictions”.

To enable the server running the DomainPatrol Server Scanner to load the Agent:

1. Open the names.nsf database on that server
2. Navigate to the view “Configuration”-“Servers”-“All Server Documents”
3. Open the server document for the server where you need access
4. Navigate to the tab “Security”
5. In the section “Programmability Restrictions” the field “Sign or run unrestricted methods and operations:” needs to contain:
 - The name of the signer of the DomainPatrol Database
 - A group that the name of the signer of the DomainPatrol Database belong to

If the DomainPatrol Server Scanner is scanning another server than the server it is running on then the server running the DomainPatrol Server Scanner needs to have at least “View-only Administrators” rights to the server it should scan. It is recommended to give the server running the DomainPatrol Server Scanner “Full Access Administrators” rights on the server it will scan. This will enable it to access most of the databases on the server to scan even if the server running the DomainPatrol Server Scanner is not listed in the database ACL.

To enable the server running the DomainPatrol Server Scanner to scan databases on another server:

1. Open the names.nsf database on the server that should be scanned
6. Navigate to the view “Configuration”-“Servers”-“All Server Documents”
7. Open the server document for the server that should be scanned
8. Navigate to the tab “Security”
9. In the section “Administrators” the field “Full Access Administrators” needs to either contain:
 - The name of the server running the DomainPatrol Server Scanner
 - A group that the name of the server running the DomainPatrol Server Scanner belong to

Step 4 - Run the Scanner

Key points

The DomainPatrol Scanner reads the Scanner Configuration Document and scans the database on the servers specified. The information gathered by the DomainPatrol Scanner is stored as items in the DomainPatrol Inventory.

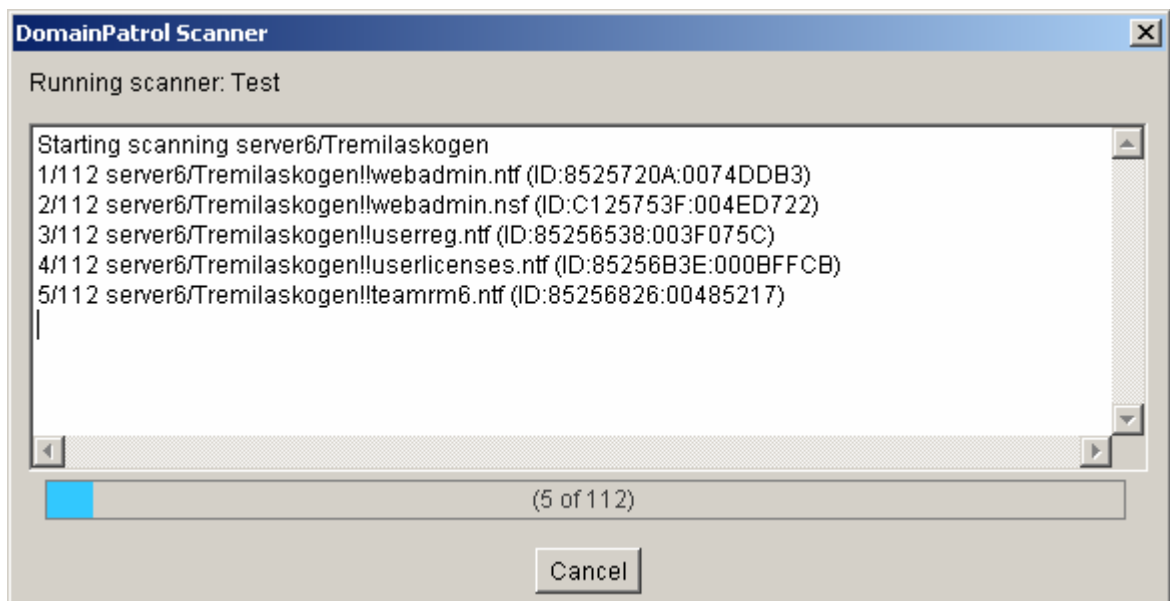
The DomainPatrol Scanner can run either from the Lotus Notes Client or on a Domino Server.

Running the DomainPatrol Client Scanner

To run the DomainPatrol Client Scanner:

1. Open the DomainPatrol Database and navigate to “Setup”-“Scanners”
2. Select the Scanner that you want to run
3. From the DomainPatrol Actions select “Client Scanner Tools”-“Run selected Scanner from this Client”

The DomainPatrol Client Scanner will start and display a dialog showing the scanning progress.



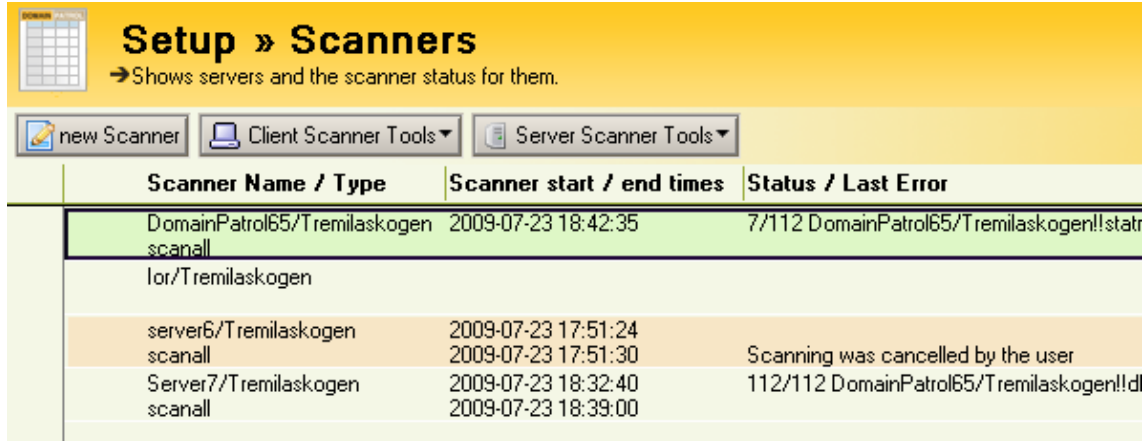
Running the DomainPatrol Server Scanner

To run the DomainPatrol Server Scanner

1. Open the DomainPatrol Database and navigate to “Setup”-“Scanners”
2. Select the Scanner that you want to run

- From the DomainPatrol Actions select “Server Scanner Tools”-“Run selected Scanners and use incremental scan”

As the DomainPatrol Server Scanner runs you can see the scanning progress in the view “Setup”-“Scanners” by updating the view. If you want the view to update automatically you can select the checkbox “Auto update view” in the upper right corner of the view.



The DomainPatrol Scanners will show in the view using different background colours depending on the status of the scanning process.

Red	There is an error condition or that the scanner was cancelled by the user
Green	The scanner is active and the progress is reported in the third column
Grey	This is an inactive scanner that has either finished or has never been run

Scheduling the DomainPatrol Server Scanner

In DomainPatrol version 5.0 the server scanner is implemented as an Agent. Using the following command the scanner agent can run on any server even if the DomainPatrol database is not located on that server:

```
tell amgr run "servername!!ddp.nsf" 'scan'
```

To schedule this server command we need to create a program document in the name and address book, but there is a small problem to include double quotes in the command.

To be able to schedule a server command we would create a program document and set the field "Program name:" to nserver. This is specific to a Domino server on the Windows platform.

The field "Command line:" would be set to

```
-c "servercommand"
```

If we would like to add the command to run the scanner it would look like this:

```
-c "tell amgr run "servername!!ddp.nsf" 'scan'"
```

This would be interpreted by the server as:

```
-c "tell amgr run "
```

This is because we cannot use a double quote in the string as the server sees this as the string terminator for the command.

To solve this problem we need to make a text file containing the server command to run the scanner agent.

Save the text file in the server program directory where the notes.ini file is located and name it "DomainPatrolScan.txt".

The content should be:

```
tell amgr run "servername!!ddp.nsf" 'scan'
```

In the program document the field "Command line:" should then be:

```
-c " < DomainPatrolScan.txt"
```

Now you can choose the "Server to run on:" and setup the schedule for the command to run.

There is a DomainPatrol Action Tool to help you create the text files and the program documents in the Domino Addressbook:

1. Open the DomainPatrol Database and navigate to "Setup"->"Scanners"
2. Select the Scanners that you want to schedule
3. From the DomainPatrol Actions select "Server Scanner Tools"->"Create program documents for scheduling selected Scanners"

When the Action has completed there will be two text files in the Domino Data directory created on the selected servers:

- DomainPatrolScan.txt
- DomainPatrolScanall.txt

For each server selected there will be two program documents created in the Domino Addressbook on that server. The two program documents refer to the two different text files.

The text files contain two different commands:

scan	Runs an incremental scan for databases that has been changed since the last scanning was completed. This is faster and does not open database that has not been changed.
scanall	Runs a complete scan for all databases and checks for any

	inconsistencies between the information stored in the DomainPatrol Inventory compared to what is found in the scanned databases. NOTE: Updates are only done if there are any changes that needs to be updated.
--	--

When the program documents have been created you need to manually edit them and set a schedule that is suitable for your Domino Domain.

It is recommended that you run a 'scan' each night and run 'scanall' once every week.

Troubleshooting

The DomainPatrol Scanner Logs and the DomainPatrol Error Logs will help you troubleshoot any issues with either running the DomainPatrol Scanner or any of the DomainPatrol Action Tools and the DomainPatrol Power Tools.

If the problem is that the DomainPatrol Server Scanner do not start check the Domino Log.nsf file for information.

Scanner Logs

If you have configured the DomainPatrol Scanner to create log Documents you will find them in the DomainPatrol Database in the view “Setup”-“Scanner Logs”.

The DomainPatrol Scanner Logs will contain different levels of information depending on the configurations selected for the DomainPatrol Scanner.

The messages contained if you choose the verbose option for the Document Log are:

- Scanner start and end
- Progress on reading the data store
- Progress on database scan
- Creation, updates and deletes on all items in the Inventory
- Warning messages
- Error messages
- Fatal messages
- Summary number of created, updated and deleted items in the Inventory

You can use the information in the Document Log to troubleshoot any issues. This information is also required when contacting DomainPatrol Support to find an answer to any problems with the DomainPatrol Scanner.

Error and fatal messages will also be updated in the DDM Domino Domain Monitoring database if you have one set up.

Error Logs

Error Logs are created when something goes wrong using either the DomainPatrol Action Tools or the DomainPatrol Power Tools.

Use the Error Logs to troubleshoot issues and when you contact DomainPatrol Support.