shortcut

Performing an Active Directory Health Check

(Digital Shortcut)

Andrew Abbate

Edited by Rand Morimoto

SAMS

www.samspublishing.com

The author(s) and publisher have taken care in the preparation of this work, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

Visit us on the Web: www.samspublishing.com

Pearson Education, Inc.
Rights and Contracts Department
One Lake Street
Upper Saddle River, NJ 07458
United States of America
Fax: (201)236-3290

ISBN 0-768-66842-5

First release, August 2006

The `RidManager` test simply checks whether the RID Master is accessible and if it contains the proper information.

The `MachineAccount` test checks whether the machine account is correctly registered in Active Directory and that its services are advertised. If this test fails, you can try to use the `/RecreateMachineAccount` switch to attempt a repair if the local machine account is missing. You can also use the `/FixMachineAccount` switch if the machine account flags are incorrect.

The next test, `Services`, simply determines whether the appropriate domain controller services are running. The various tests include

- `OutboundSecureChannels` determines whether the secure channels exist from all the domain controllers in the domain to the domains specified by `/testdomain`. You can expand the scope of this test to domain controllers outside the local AD site by using the `/nositerestriction` parameter.
- `ObjectsReplicated` checks to see that Machine Account and DSA objects have replicated. You can test additional objects by using `/objectdn:`*`dn`* with `/n:`*`nc`* parameters.
- `Frssysvol` checks to see that the File Replication Service (FRS) SYSVOL is ready.
- `Frsevent` reads the event log to see whether errors exist in the File Replication Service. This test may show a false positive (failure) if run shortly after fixing FRS errors because the event log would still be relatively fresh in terms of errors.
- `Kccevent` checks to see that the Knowledge Consistency Checker is completing without errors.
- `Systemlog` checks the event log to determine whether the system is running without errors. This test can also generate false positives (failures) if issues were recently fixed.

- `CheckSDRefDom` checks that all application directory partitions have correct security descriptor reference domains.
- `VerifyReplicas` checks that all application directory partitions are fully instantiated on all replica servers.
- `CrossRefValidation` verifies the validity of cross-references where applicable.
- `VerifyReferences` verifies that specific system references are intact for the FRS and replication infrastructure.
- `VerifyEnterpriseReferences` verifies that certain system references are intact for the FRS and replication infrastructure across all objects in the enterprise on each domain controller.

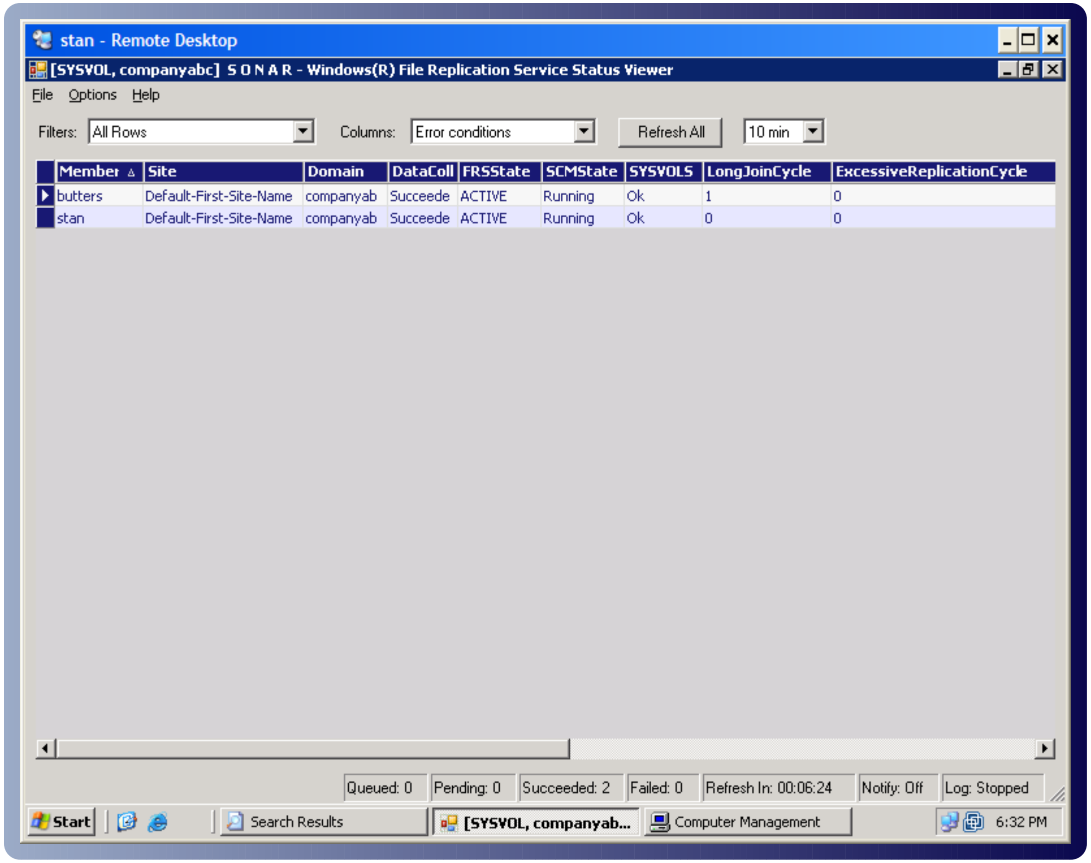
Reviewing the Results of the SONAR Utility and Addressing Any Errors it Finds

The third tool we discussed was SONAR. Unlike the two previous tools, SONAR is a graphical application that can either be viewed in real-time or it can generate log files showing its results.

The initial view you get after the first polling of the domain controllers is shown in Figure 1.

As you can see in Figure 1, the domain controllers have been identified along with the site and domain they belong to. You can see that the data collection succeeded and that the FRS state of both servers is active. If you scrolled to the far right of the view, you would also see when FRS last started on each server.

FIGURE 1
Results from SONAR polling.



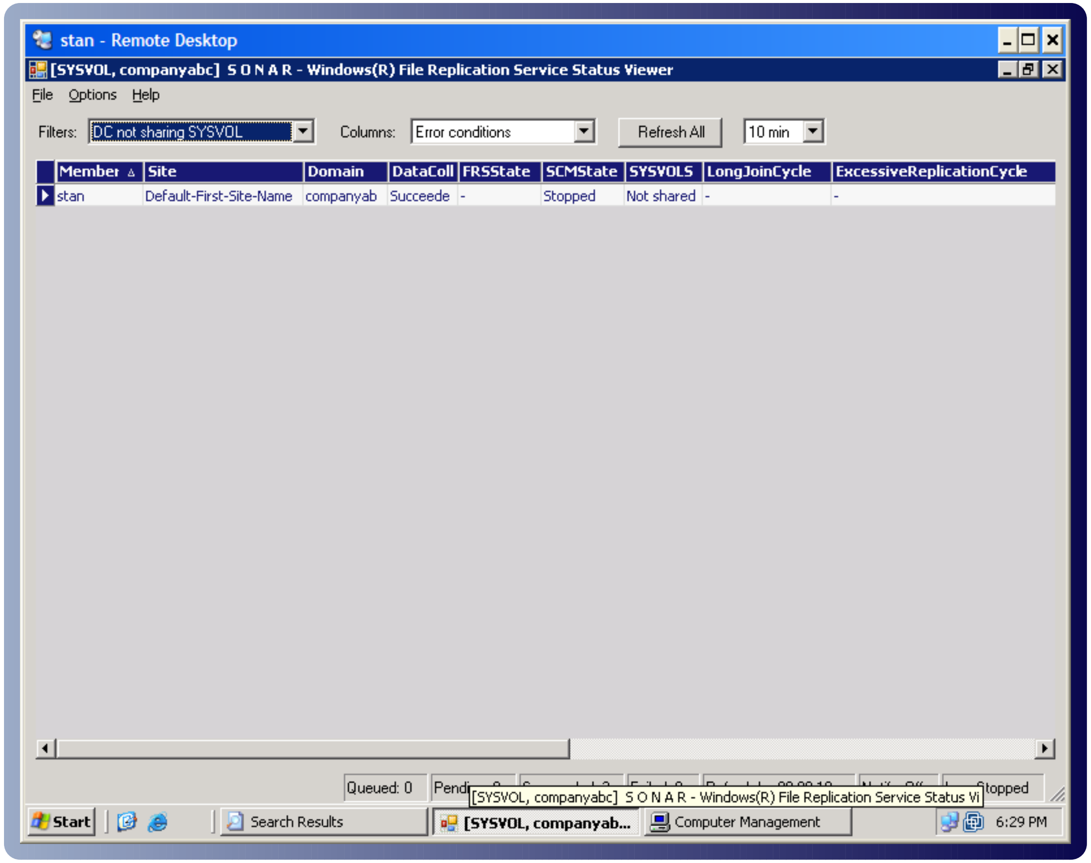
Filters: All Rows   Columns: Error conditions   10 min

Member	Site	Domain	DataColl	FRSState	SCMState	SYSVOLS	LongJoinCycle	ExcessiveReplicationCycle
butters	Default-First-Site-Name	companyab	Succeede	ACTIVE	Running	Ok	1	0
stan	Default-First-Site-Name	companyab	Succeede	ACTIVE	Running	Ok	0	0

Queued: 0   Pending: 0   Succeeded: 2   Failed: 0   Refresh In: 00:06:24   Notify: Off   Log: Stopped

In this next view, shown in Figure 2, you can see that SONAR has identified a domain controller where SYSVOL isn't being shared. This is a quick sign of a domain controller that is having a problem, which will directly impact end users.

FIGURE 2
SONAR results of a SYSVOL not being shared.



stan - Remote Desktop
[SYSVOL, companyabc] S O N A R - Windows(R) File Replication Service Status Viewer
File Options Help
Refresh All

Filters: DC not sharing SYSVOL
Columns: Error conditions
10 min

Member	Site	Domain	DataColl	FRSState	SCMState	SYSVOLS	LongJoinCycle	ExcessiveReplicationCycle
stan	Default-First-Site-Name	companyab	Succeede	-	Stopped	Not shared	-	-

Queued: 0 | Pendi… | …topped

[SYSVOL, companyabc] S O N A R - Windows(R) File Replication Service Status Vi
Start
Search Results
[SYSVOL, companyab...
Computer Management
6:29 PM

In this case, you would first check to see that the Netlogon service is started, which includes the following steps:

1. Click Start, Programs, Administrative Tools, Services.
2. Scroll down to the Netlogon Service and check its status.
3. Right-click the Netlogon Service and choose Start if it isn't already started.

If this isn't the cause of the error, you would look at the Event Viewer by doing the following:

1. Right-click My Computer on the desktop.
2. Choose Manage.
3. Expand System Tools.
4. Expand Event Viewer.
5. Review each event in the System category for references to Netlogon.

To more easily track long-term system data from SONAR, do the following:

1. Click File.
2. Click Log.
3. Click Configure to set the location of the log file.
4. Click Start Log.

Reviewing the Results of the RepAdmin Utility and Addressing Any Issues

RepAdmin, the fourth tool we reviewed, can be used both to trigger replication events as well as to view system messages regarding configurations and statuses of replication events. Following are outputs from tests that can be used to help determine the health of Active Directory replication.

`Repadmin /failcache`—This command displays a list of failed replication events that were detected by the Knowledge Consistency Checker.

```
repadmin running command /failcache against server localhost
==== KCC CONNECTION FAILURES ============================
(none)
==== KCC LINK FAILURES ==================================
    Default-First-Site-Name\BUTTERS
        DC object GUID: cd9e43b2-c5ae-45af-8f1f-2d0cba6056ec
        No Failures.
```

In the preceding example, the KCC did not detect any failures.

`Repadmin /kcc`—This command forces the KCC to recalculate replication topology for a particular directory server. This capability can be helpful if you think you are having issues with your KCC. This process normally occurs every 15 minutes, so it is helpful to force this event to occur while troubleshooting AD.

```
repadmin running command /kcc against server localhost
Consistency check on localhost successful.
```