

Ensuring High Availability of Your Active Directory Forest

Written by
Derek Melber
Microsoft MCSE and MVP

**© 2010 Quest Software, Inc.
ALL RIGHTS RESERVED.**

This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Quest Software, Inc. ("Quest").

The information in this document is provided in connection with Quest products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest products. EXCEPT AS SET FORTH IN QUEST'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software World Headquarters
LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
E-mail: legal@quest.com

Refer to our Web site for regional and international office information.

Trademarks

Quest, Quest Software, the Quest Software logo, AccessManager, ActiveRoles, Aelita, Akonix, AppAssure, Benchmark Factory, Big Brother, BridgeAccess, BridgeAutoEscalate, BridgeSearch, BridgeTrak, BusinessInsight, ChangeAuditor, ChangeManager, Defender, DeployDirector, Desktop Authority, DirectoryAnalyzer, DirectoryTroubleshooter, DS Analyzer, DS Expert, Foglight, GPOAdmin, Help Desk Authority, Imceda, IntelliProfile, InTrust, Invirtus, iToken, IWatch, JClass, Jint, JProbe, LeccoTech, LiteSpeed, LiveReorg, LogAdmin, MessageStats, Monosphere, MultSess, NBSpool, NetBase, NetControl, Npulse, NetPro, PassGo, PerformaSure, Point,Click,Done!, PowerGUI, Quest Central, Quest vToolkit, Quest vWorkSpace, ReportAdmin, RestoreAdmin, ScriptLogic, Security Lifecycle Map, SelfServiceAdmin, SharePlex, Sitraka, SmartAlarm, Spotlight, SQL Navigator, SQL Watch, SQLab, Stat, StealthCollect, Storage Horizon, Tag and Follow, Toad, T.O.A.D., Toad World, vAutomator, vControl, vConverter, vFoglight, vOptimizer, vRanger, Vintela, Virtual DBA, VizionCore, Vizioncore vAutomation Suite, Vizioncore vBackup, Vizioncore vEssentials, Vizioncore vMigrator, Vizioncore vReplicator, WebDefender, Webthority, Xaffire, and XRT are trademarks and registered trademarks of Quest Software, Inc in the United States of America and other countries. Other trademarks and registered trademarks used in this guide are property of their respective owners.

Contents

- Abstract 3
- Introduction..... 4
- The Active Directory Forest..... 5
 - Symptoms of a Failing (or Failed) Active Directory Forest 5
- Preparing for an Active Directory Forest Disaster..... 6
- Recovering Your Active Directory Forest..... 7
 - Quest Recovery Manager for Active Directory Forest Edition 7
- Conclusion..... 8
- About the Author 9

Abstract

Active Directory is essential to business critical applications from sales tools to e-mail. Because its domains are connected by trusts, the loss of any domain in your AD forest can seriously hurt your business. This document describes the symptoms of a failing or failed domain or forest, details how to prepare for the possibility of domain or forest failure, and compares the manual forest recovery procedure recommended by Microsoft with Quest's automated recovery solution, Recovery Manager for Active Directory Forest Edition.

Introduction

The failure of even a portion of your Active Directory forest has serious consequences: E-mail would no longer be functioning. Databases would fail to allow reads or writes to the data stored within the tables. All applications that rely on Active Directory for authentication would fail to function (sales, accounting and marketing tools, file shares, even printing.)

Therefore, organizations need to be able to recover from the failure of an Active Directory domain or entire forest quickly and completely. Unfortunately, Microsoft's recommended recovery procedure is long and complex, and imposes requirements that are difficult or impossible to meet. Quest Recovery Manager for Active Directory Forest Edition overcomes these limitations, offering automated forest recovery that is dramatically faster and more complete.

The Active Directory Forest

Active Directory (AD) is dynamic, complex, and sophisticated. Because all domains in your Active Directory forest are connected by trusts, any loss of a trust or domain will cause significant communication issues. For example, if you have a domain that is non-responsive, the entire forest will be affected. All applications that rely on Active Directory—such as e-mail, sales quoting software, sales processing applications, CRM software, as well as accounts receivable and payable applications—will fail. Nothing will make the overall network function properly until the domain is fully functional again.

Of particular importance to the forest is the root domain. The root domain is the epicenter for central communication, decisions, and overall control of the forest. If the root domain is lost, damaged or otherwise unavailable, the entire structure is placed in jeopardy. Therefore, organizations need to be able to quickly and reliably recover when a forest fails.

Symptoms of a Failing (or Failed) Active Directory Forest

How can you tell that a domain or an entire Active Directory forest is faltering and might soon fail? The symptoms are a variety of odd behaviors that usually frustrate administrators and users alike.

One common symptom of a failing Active Directory forest is slow logons. First, DNS must be working properly to ensure that clients and servers are directed to resources properly, so slow logons can be a symptom of DNS problems. Slow logons can also be the result of problems with the domain controllers, servers, authentication, applications, or trust relationships, all of which point back to issues with the Active Directory forest.

Another common symptom of Active Directory issues is when users, clients, servers, applications, or services cannot access one or more domains or network resources. Since all of the moving parts of your forest are essential to resource access, one small glitch can cause problems for everyone.

Essential business applications can also fail, since they rely on authenticating to Active Directory. If Active Directory, DNS, domain controllers, network communication or anything else is faltering, users can have problems accessing these business applications.

When these symptoms arise, it is clear there is a problem, but tracking down the root issue is often difficult. More often than not, issues related to the failure of an Active Directory forest are not logged, because of limitations of the operating system and Active Directory itself. If the root issue is due to malicious behavior, logs will also likely be unavailable, since monitoring must have been implemented before the malicious activity took place.

Preparing for an Active Directory Forest Disaster

Organizations can help prepare for the possibility of a forest-wide disaster by documenting their Active Directory infrastructure in detail. Although this might seem like a small task, it actually takes tremendous time and patience. Leaving out even one detail about the forest can halt the recovery or cause it to fail completely.

At a minimum, you should document the following information:

- Active Directory-related information
 - Domain names (NetBIOS and DNS)
 - Domain relationships such as trusts (both internal and external)
 - Group memberships (admin groups, all security groups, and distribution groups)
 - Exchange details and information
 - Group Policy Objects (GPOs) and all links
 - AD sites, IP subnets, and replication intervals
- Domain controller-related information
 - Domain controller names
 - FSMO roles
 - Global catalog servers
 - Certificates for all security
- DNS-related information
 - AD-integration
 - Delegations
 - Permissions
 - Special settings and entries

As you can see, many small details need to be documented. A third-party product can help; be sure to look for one that not only documents all of this information automatically, but also keeps it updated as your environment changes. Having detailed, up-to-date information about your forest is critical for recovery situations, and also useful in troubleshooting Active Directory problems.

Recovering Your Active Directory Forest

Microsoft has published several documents detailing how to recover from a loss of your Active Directory forest. Unfortunately, the procedures in these documents have considerable drawbacks.

First, the procedures rely on manual Microsoft tools. These tools require that all steps be performed by an administrator in the proper order, with the administrator babysitting the entire process. The documents do not estimate the time required to complete the restoration procedure, but it could easily take many days.

Second, the Microsoft procedure specifies 67 steps for each domain or domain controller being restored. Although some companies have just a few domains and domain controllers, medium to large organizations might have 10, 20, or 30 domains, each with 50 or 100 domain controllers. Performing a 6-step procedure for each one would be prohibitively long, and missing a step or performing a step out of order is highly likely.

Third, most steps in the Microsoft restoration procedure require that the administrator be physically present at the domain controller being restored. However, organizations today are spread over states, regions, and even continents, making this requirement nearly impossible to meet in a reasonable time frame.

Finally, the Microsoft procedure initially restores only a subset of your domain controllers, giving you only limited functionality. The rest of the domain controllers have to be created from scratch after the forest is restored, so restoring complete functionality takes additional work and time.

Together, these drawbacks to Microsoft's procedure for manually restoring an Active Directory forest make the logistics of restoration nearly impossible.

Quest Recovery Manager for Active Directory Forest Edition

Quest Recovery Manager for Active Directory Forest Edition offers an alternative that is closely aligned with Microsoft's approach. Forest Edition documents all of your domains, domain controllers, and other essential Active Directory components for you. When a failure occurs, it walks you through the restore procedure, ensuring all steps are done in the proper order and that no steps are missed.

Forest Edition also eliminates the requirement that the administrator be physically present at each domain controller being restored. And it can restore all your domain controllers simultaneously rather than one at a time. This reduces the overall recovery time and eliminates the complexity of determining which domain controller must be restored first, second, third, etc.

With Forest Edition, you can get your entire Active Directory forest back online as fast as possible, without the manual steps and other drawbacks of the Microsoft procedure.

Conclusion

Because a failed Active Directory domain or forest can have a devastating effect on your organization's business continuity, it is critical to have a disaster recovery plan in place. Quest Recovery Manager for Active Directory Forest Edition will help you restore your Active Directory forest, regardless of the root issue, with little manual effort on your part. It automatically keeps an up-to-date record of all important details of your forest, eliminating significant manual effort. Then, if a failure occurs, it restores all your domain controllers simultaneously, without requiring an administrator to visit each domain controller and without the risk of steps being missed or performed out of order. With Forest Edition, your Active Directory forest will be back up dramatically faster than with any other restore procedure.

About the Author

Derek Melber (MCSE and MVP) is president of BrainCore.Net AZ, Inc., an independent consultant and speaker, as well as author of many IT books. Derek educates and evangelizes Microsoft technology, focusing on Active Directory, Group Policy, Security, and desktop management. As one of only 8 MVPs in the world on Group Policy, Derek's company is often called upon to develop end-to-end solutions regarding Group Policy for companies. Derek is the author of the [The Group Policy Resource Kit](#) by MSPress, which is the defacto book on the subject. Derek is also author of the [Group Policy Video Mentor](#) (Pearson), perfect for learning Group Policy basics.

About Quest Software, Inc.

Quest Software (Nasdaq: QSFT) simplifies and reduces the cost of managing IT for more than 100,000 customers worldwide. Our innovative solutions make solving the toughest IT management problems easier, enabling customers to save time and money across physical, virtual and cloud environments. For more information about Quest solutions for application management, database management, Windows management, virtualization management, and IT management, go to www.quest.com.

Contacting Quest Software

PHONE 800.306.9329 (United States and Canada)

If you are located outside North America, you can find your local office information on our Web site.

E-MAIL sales@quest.com

MAIL Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract.

Quest Support provides around-the-clock coverage with SupportLink, our Web self-service. Visit SupportLink at <https://support.quest.com>.

SupportLink gives users of Quest Software products the ability to:

- Search Quest's online Knowledgebase
- Download the latest releases, documentation, and patches for Quest products
- Log support cases
- Manage existing support cases

View the Global Support Guide for a detailed explanation of support programs, online services, contact information, and policies and procedures.



5 Polaris Way, Aliso Viejo, CA 92656 | PHONE 800.306.9329 | WEB www.quest.com | E-MAIL sales@quest.com

If you are located outside North America, you can find local office information on our Web site.

© 2010 Quest Software, Inc.
ALL RIGHTS RESERVED.

Quest, Quest Software, the Quest Software logo are registered trademarks of Quest Software, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. WPW_EnsureHighAvailofAD_US_EC_20101221