SHAREPOINT

PRACTICAL IT STRATEGIES FOR ENTERPRISE COLLABORATION /// MAY 2010

G GOVERNANCE

Time to Beef up Code Retention Policies

Organizations should use code retention policies in their governance plans to correct patch management policies for SharePoint servers. BY BRIEN M. POSEY

M MANAGEMENT

Managing Sandbox Solutions in SharePoint 2010

Isolated from other sites, sandbox solutions offer the ability to deploy solutions within the governance of Web applications. BY SHAWN SHELL

I IMPLEMENTATION

How to Use Email-Enabled Document Libraries in SharePoint

Find out when storing incoming messages in SharePoint document libraries might be a better option than using public folders. BY GEORGE KHALIL

SearchWinIT.com

SharePoint Damage Control

BY CHRISTINE CASATELLI

ARE YOU THE trusting type? Maybe not when it comes to patch management. Handing off that responsibility to another group may seem like a great idea. But it also means losing some control over your SharePoint servers.

If patch management and the testing process are taken out of your hands, you can still protect your SharePoint servers from buggy patches. Create code retention policies to help ensure that previous versions of system files remain available—even after a patch has been applied.

In "Time to Beef Up Code Retention Policies," Microsoft MVP Brien M. Posey describes how to put a damage control plan in place to protect your SharePoint servers from harm.

SharePoint 2010 has an interesting feature that allows administrators and site collection owners to upload new functionality scoped to a single site collection.

Although there are still some challenges, Microsoft's sandbox solutions help administrators overcome the potential disaster of installing numerous custom applications in a shared farm. Learn how to make the most of this new function in "Managing Sandbox Solutions in SharePoint 2010" by Shawn Shell.

Public folders continue to be a hot topic for SharePoint administrators. Have you ever considered that there might be a few reasons for storing incoming messages in SharePoint document libraries instead of in public folders? Weigh the pros and cons of each approach in "Using Email-Enabled Document Libraries in SharePoint" by George Khalil.

Got a SharePoint tip you'd like to share? Send it to ccasatelli@techtarget.com. ■

SearchWinIT.com

Cathleen Gagne, Editorial Director, cgagne@techtarget.com
Christine Casatelli, Editor, ccasatelli@techtarget.com
Martha Moore, Copy Editor, mmoore@techtarget.com
Linda Koury, Art Director of Digital Content, lkoury@techtarget.com
Jonathan Brown, Publisher, jebrown@techtarget.com
Peter Larkin, Senior Director of Sales, plarkin@techtarget.com

TechTarget, 275 Grove Street, Newton, MA 02466; www.techtarget.com

Time to Beef Up Code Retention Policies

Organizations should use code retention policies in their governance plans to correct patch management policies for SharePoint servers. **BY BRIEN M. POSEY**

TODAY, MANY MEDIUM to large organizations seem to have a team of people whose job it is to review and approve software patches. As a SharePoint administrator, placing the burden of patch management onto another team may initially seem like a great idea. However, doing that can mean losing some control over the SharePoint servers.

The big problem when you allow a dedicated team to handle patch management for SharePoint servers is that you have no way of knowing how thoroughly the patches are being tested. The patch management team should test each patch meticulously, but I have seen IT professionals who skip the testing process altogether, assuming that if a patch was released by Microsoft then it must be OK.

Microsoft openly admits that patches do not receive the same degree of testing as service packs do. Normally, Microsoft seems to do a decent job of releasing patches that work as advertised, but there have been a couple of buggy patches that have made it out the door. And buggy patches can severely cripple your servers.

> To avoid the potential for installing untested—or under-tested—patches is to take control of the patch management process.

The only way to completely avoid the potential for installing untested—or under-tested—patches is to take control of the patch management

process for your SharePoint servers. Corporate bureaucracy being what it is, though, that may be impossible. In that case, the next best thing is to hedge your bets and address patch management within your governance plan by placing an emphasis on code retention policies.

So what are code retention policies? They dictate how existing and legacy versions of known code should be retained. Such policies may document how many different versions of a file should be kept on hand and how that code is to be stored and documented. The bottom line is that you should have a damage control plan in place so that your team will know how to respond when a buggy patch puts SharePoint at risk.

■ **Documentation.** Start out by creating a policy stating that each patch that is to be applied must be documented. The trick is to set up the documentation requirements in a way that will help you recover your servers should the need arise. Begin by documenting the Microsoft Knowledge Base article ID number that corresponds to the patch, along with the date and time when the patch is supposed to be applied. Having this information on hand makes the troubleshooting process a lot easier if something goes wrong.

Start out by creating a policy stating that each patch that is to be applied must be documented.

Why Stop With System Files?

THERE IS NO reason why code retention policies needs to be limited solely to system files. SharePoint sites are typically made up of individual Web parts. Because a single Web part can be included in multiple SharePoint sites, any changes to a Web part have the potential to affect any site that depends on that part. Because of that, code retention policies are important for any custom code used on your SharePoint sites. That way, if a Web part becomes infected with a virus or if a developer makes an unwanted change to a Web part, you have a known good version of the Web part that can be retrieved. ■

Editor's Note

G
Time to Beef Up Code Retention Policies

M
Managing Sandbox Solutions in SharePoint 2010

I
Using Email-Enabled Document Libraries in SharePoint

Another step in the documentation process involves obtaining a copy of the patch that is to be applied and extracting its contents to an empty folder. You can do this by specifying the Extract switch after the executable file name.

After extracting the patch file, make a note of the files that it contains. That way, you will know which system files are going to be replaced, and you can make a backup copy of those files before you install the patch.

- **Backups.** So why not just make a full system state backup of your SharePoint servers before a patch is applied? You could use that approach, but it isn't always practical. Imagine, for example, the time and resources required to manually create full system state backups of a hundred different SharePoint servers every time there is a patch that needs to be deployed.

- **System Recovery Points.** I once read an article in which someone wrote that backups prior to patch deployment are unnecessary because Windows automatically creates system restore points that you can fall back to should the patch cause problems. I will be the first to admit that system restore points are a great feature, but I wouldn't stake my job on their ability to reverse server damage.

The problem with system recovery points is that they are not retained indefinitely. If you apply a patch to a server, and then half an hour later you notice that the server is having problems, then reverting to a recovery point is probably the way to go.

But, what happens if you don't notice the problem for six weeks? By that time, the recovery point that you need may have been overwritten by newer recovery points. In the end, code retention is simply more reliable than system recovery points.

- **Patch Removal.** The argument could be made that retaining legacy code is unnecessary because buggy patches can be uninstalled. In a perfect world, this is absolutely true. In fact, your governance plan should directly state that the first course of action against a buggy patch should be to try to uninstall that patch.

Sometimes, though, you may find that a patch's flaws are severe enough that uninstalling the patch or rolling back the system to a recovery point becomes impossible. Restoring legacy system files may be the only means of recovery in such situations.

- **Structure Your Backups.** Even if creating a special backup every time a new patch is to be deployed ends up being impractical, anyone who regularly backs up their SharePoint servers is already performing at least some degree of code retention. As

such, it makes a lot of sense to examine your backup processes to see how well they would serve you if a buggy patch were to cause problems with your SharePoint servers.

One thing that you can do to make the recovery process easier is to structure your backups in a way that simplifies the recovery process. SharePoint stores all of its data and most of its configuration information in a SQL database. If you are not already doing it, back up the SQL database in a separate backup job from the SharePoint server's system files. That way, if problems do occur, the person who is tasked with fixing the server can restore the server's system files without any fear of accidentally overwriting data.

One last recommendation: Avoid applying large numbers of new patches at the same time—aside from initially provisioning a server.

Imagine, for instance, that the patch management team informs you that it needs to apply 20 new patches to your SharePoint servers. If problems occur after the patches have been applied, then how will you know which patch caused the problem? Applying patches individually or in small batches goes a long way to make the troubleshooting process easier if problems should occur.

Even if the patch management and testing process is out of your hands, you aren't powerless to protect your SharePoint servers against buggy patches. Code retention policies can help to ensure that previous versions of system files remain available even after a patch has been applied, and that the servers can be reverted to a previous state. ■

SharePoint stores all of its data and most of its configuration information in a SQL database. If you are not already doing it, back up the SQL database in a separate backup job from the SharePoint server's system files.

ABOUT THE AUTHOR

Brien M. Posey has received Microsoft's Most Valuable Professional award six times for his work with Windows Server, IIS, file systems/storage and Exchange Server. He has served as CIO for a nationwide chain of hospitals and healthcare facilities and was once a network administrator for Fort Knox.

Managing Sandbox Solutions in SharePoint 2010

Isolated from other sites, sandbox solutions offer the ability to deploy solutions within the governance of Web applications. **BY SHAWN SHELL**

MICROSOFT HAS A new function in SharePoint 2010 that it calls "Sandbox" or "User Solutions," which allows administrators and site collection owners to upload new functionality scoped to a single site collection. This means that site collection owners can host custom code or third-party add-ons that are useful to them without affecting others on the same farm.

This functionality is incredibly useful in situations where organizations have shared SharePoint farms that serve the needs of various groups. It's also useful if organizations are looking to leverage services like SharePoint Online—which is a SaaS-based version of SharePoint—but historically have been prevented from including custom code.

A site administrator or site collection owner can add user solutions through a new gallery option in Site Settings. Anyone who has worked with SharePoint 2007 will already be familiar with the Web part, site template, master page/layout and content type galleries. The solution gallery is the latest edition.

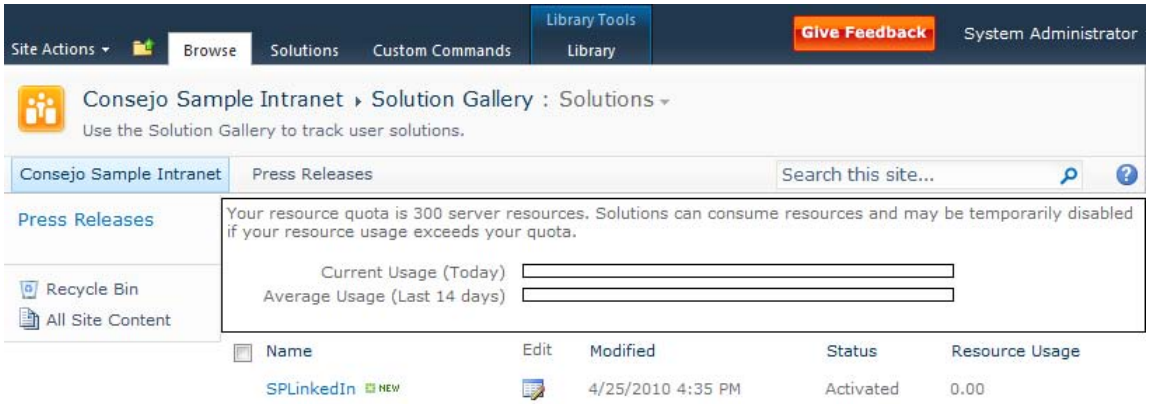
In this new gallery, user solutions

A site administrator or site collection owner can add user solutions through a new gallery option in Site Settings.

for the site collection are stored. In **FIGURE 1** (see page 9), owners can quickly access the solution gallery and add specially written SharePoint solutions to their individual site collections. These solutions are actually written a bit differently than 2007 solutions in that the code must

FIGURE 1

The solution gallery for site collections



adhere to certain restrictions. Solutions are not permitted to execute operations that would affect either the server on which they run or cross the site collection boundary.

In the gallery, owners or administrators can see what solutions are loaded and can activate or deactivate them. This reduces the administrative burden on folks managing SharePoint farms because it puts more administrative control into the hands of qualified users—or specially designated owners of site collections.

CONSTRAINTS AND QUOTAS

User solutions are scoped to the site collection. This means that the code within the solution is restricted to running operations within the site collection to which it's been deployed. This constraint provides the first level of management because administrators don't have to worry about solutions crossing site collections and running wild.

In addition to the site collection constraint, there are automatic quotas applied to all site collections. These quotas, like SharePoint 2007, have a storage component. In SharePoint 2010, there is also a resource component related to user solutions. By default, each site collection gets 300 quota points. Solutions use up the quota points by using farm resources. Depending on the resource or operation, a specific threshold translates to a single quote point.

For example, 3,600 seconds of CPU execution time translates to

a single point. By contrast, a single abnormally terminated process also translates to a single quote point. A list of these thresholds can be found in the sandbox solutions architecture guide on MSDN.

Once the site collection's quota for resource consumption is reached, SharePoint automatically shuts down all user solutions for that site collection. This prevents solutions in one site collection from consuming an inordinate amount of farm resources. However, remember that the quota is per site collection and applies to all user solutions within the site collection.

MANAGING SOLUTIONS

Management of solutions within a farm is a shared responsibility. At

Editor's Note

G Time to Beef Up Code Retention Policies

M Managing Sandbox Solutions in SharePoint 2010

I Using Email-Enabled Document Libraries in SharePoint

Management Tips for SharePoint 2010

IF YOU'RE CONSIDERING user solutions in your environment, here are a few tips that may make your management job easier:

1. **The default value of 300 points for a solution quota should provide plenty of "head room" for most solutions. Keep in mind that the quota applies to the entire site collection, not a single solution, which means that all solutions within a site collection share the 300 points. Once the quota is reached, all solutions for that site collection will be shut down.**
2. **There is no good way to monitor solutions across site collections, which is a major detractor for this feature. So consider keeping your sandbox solutions in just a few site collections initially. This will reduce the burden of monitoring lots of site collections. Once you're comfortable, you can expand sandbox solutions usage.**
3. **Sandbox solutions run in their own process that you can start and stop within Central Administration. This also means they don't run in the main w3wp.exe process, and you don't have to recycle the app pools or restart IIS to see changes.**
4. **Because site owners can now add solutions on their own, you'll want to be even more careful about who is granted this role. ■**

the farm level, administrators set policy in the form of quotas. This means that although there's a default 300-point quota for solutions, administrators can adjust that on a per-site collection basis.

Furthermore, much like SharePoint 2007, administrators can create quota templates that include both storage and quota points. Once you establish a template, you can apply it to one or more site collections within a SharePoint application.

Administrators also have the option of blocking solutions. If a specific solution appears to be consistently causing a problem, administrators can block solutions, which is done in Central Administration from the User Solution Management interface. This same management function also provides the ability to decide how the code is run—all requests on the same machine or load-balanced across servers running the User Code Service.

At the Site Collection's level, the solution gallery exposes reporting on quota usage for all solutions in this site collection. Although the interface does not provide a lot of management, site owners are shown how much of their quota has been consumed. In Figure 1, owners can see the daily usage as well as usage over the last 14 days. They then have the option of shutting down or deactivating certain tools that may be consuming more resources than others.

Once you establish a template, you can apply it to one or more site collections within a SharePoint application.

Although SharePoint 2010 is still relatively new—the information here is based on the beta version—user solutions are a way to enable different groups to share a farm and provide the flexibility to deploy custom code, while allowing administrators to manage those add-ons. Clearly, there are still challenges in this new model, but it helps administrators overcome the management and potential disaster of installing numerous custom applications in a shared farm. ■

Editor's Note

G
Time to Beef Up Code Retention Policies

M
Managing Sandbox Solutions in SharePoint 2010

I
Using Email-Enabled Document Libraries in SharePoint

ABOUT THE AUTHOR

Shawn Shell is the founder of Consejo Inc., a consultancy based in Chicago that specializes in Web-based applications, employees and partner portals as well as enterprise content management. He has spent more than 19 years in IT, with the last 10 focused on content technologies. Shell is a co-author of *Microsoft Content Management Server 2002: A Complete Guide,* published by Addison-Wesley, and he is the lead analyst/author on the CMSWatch SharePoint Report 2009.

Continuous Availability for SharePoint 2010

- Protect individual SharePoint installations or complete SharePoint farms against unplanned outages and planned downtime
- Provide a consistent approach that goes across SQL databases, file system content and Exchange
- Provide one SLA to protect the entire collaboration, workflow and content management platform

neverfail®

WWW.NEVERFAILGROUP.COM

Microsoft® GOLD CERTIFIED Partner

512-327-5777 | info@us.neverfailgroup.com

Using Email-Enabled Document Libraries in SharePoint

Find out when storing incoming messages in SharePoint document libraries might be a better option than using public folders.

BY GEORGE KHALIL

PRIOR TO THE release of Exchange Server 2007, Microsoft announced that the future of public folders was in question and that SharePoint libraries would take their place. Microsoft changed its stance and continues to support Exchange public folders.

But there might still be a number of compelling reasons why you would want to consider storing incoming messages in SharePoint document libraries—instead of public folders. SharePoint can enable incoming mail on lists and libraries. It also has several out-of-the-box features like Alerts, Enterprise Search and Information Management policies, all of which provide for a richer collaborative experience.

One instance where these features are valuable has to do with technical newsletters. Many SharePoint users subscribe to various email-based technical newsletters, and they forward those messages to team members. Email-enabled document libraries provide a central location to store the newsletters and remove the administrative burden of manually sharing the information with other team members.

Microsoft changed its stance and continues to support Exchange public folders.

The feature also allows users to subscribe to the document library via SharePoint Alerts. These alerts can be set to immediate, daily or weekly summary notifications.

Newsletter subscriptions that are automatically delivered to an email-

enabled document library form part of SharePoint's full-text index. Users can search this index at a later date using SharePoint's Enterprise Search capability.

FIRST STEPS

Before going any further, make sure these two actions have taken place:

1. You have enabled email support within SharePoint's Central Administration.
2. You have configured Microsoft Exchange Server to route messages to the SMTP service on a SharePoint Web front-end server.

To enable incoming email within a document library, navigate to **Settings/Document Library** settings. In the *Communications* section located on the right, select **Incoming email settings**. The resulting screen has a number of options allowing you to enable incoming email (see **FIGURE 1**).

Editor's Note

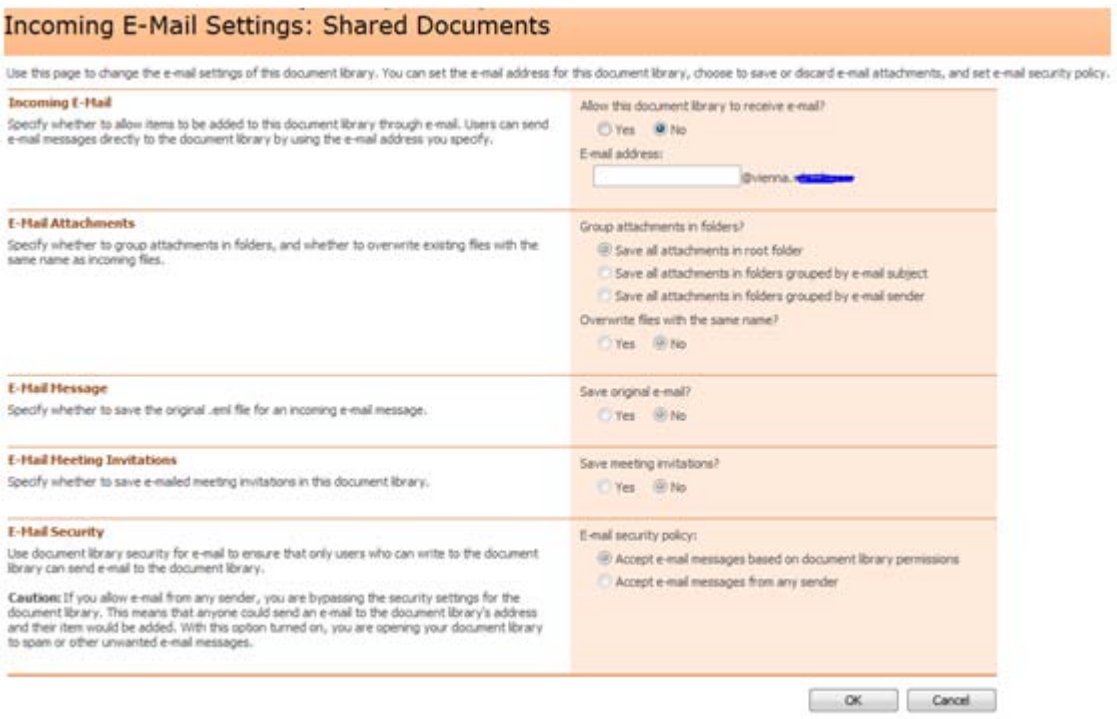
G
Time to Beef Up Code Retention Policies

M
Managing Sandbox Solutions in SharePoint 2010

I
Using Email-Enabled Document Libraries in SharePoint

FIGURE 1

SharePoint offers several choices to enable incoming email.



Editor's Note

G
Time to Beef Up Code Retention Policies

M
Managing Sandbox Solutions in SharePoint 2010

I
Using Email-Enabled Document Libraries in SharePoint

Next, follow these steps:

- In the Incoming E-mail section, select **Yes**, which is located under *Allow this document library to receive e-mail?*

- Next, specify a unique label to form part of the email address. Be as specific as possible. For example, if this document library was set up to receive TechTarget's SearchExchange.com newsletter, you would enter the following address: searchexchange.techtarget@<domain>.com.

- There are a few options to choose in the *E-mail Attachments* section. If email messages that enter this library do not contain attachments, you can ignore this section.

- In the *E-mail Message* section, you can set it to save the original email.

IMPORTANT: If you're receiving HTML newsletters, select **Yes**. If the newsletters are always attachments—such as PDFs—within an email, select **No** and rely on the *E-mail Attachments* section to deal with attached documents.

- In the *E-mail Meeting Invitations* section, you have the option to store attachments to any meeting invitations that are sent to this document library. Select **No** because you're not going to use this document library to facilitate meeting requests.

- In the *E-mail Security* section, you can specify who can send email messages to this library—site members or anyone. If you're using this document library to receive email messages from external sources or anonymous users, you will need to select **Accept e-mail messages from any sender**.

- Click **OK** to confirm your changes.

On the back end, the Microsoft SharePoint Directory Management Service that is connected to Active Directory creates a contact in the form of <Site Name> <Document Library Name> and assigns it a valid SMTP address. The Active Directory container that the contact is created in is specified under Central Administration -> Operations > Incoming Email Settings.

To confirm that the contact has been created, launch the Exchange Server 2007 Management Console and navigate to **Recipient Configuration node/Mail Contact**. The recently created contact will also be listed in your Outlook Global Address List.

Sending an email to the Exchange/Outlook contact that was just created

should route automatically to the document library (see **Figure 2**).

CONFIGURING INFORMATION MANAGEMENT POLICIES

Content managers and site administrators can also use SharePoint's Information Management policies to create expiration policies and automated workflows to control the lifecycle of email that's delivered and stored within a document library. The policies can potentially archive or dispose of content that resides in these libraries after a specified period of time.

Information Management policies can be created at the site collection level and can be reused throughout all SharePoint sites—or at the document library level.

Enabling expiration policies on a document library gives you a basic Information Lifecycle Management strategy for email-enabled document libraries. With expiration options, you create a consistent retention period for your email messages based on a created or modified date.

To set an expiration policy, go to a document library and click on **Settings/Document Library**, followed by **Information Management policy settings**, located under the *Permissions and Management* section.

- Select "Define a policy ..."
- The *Edit Policy: Document* page will appear and give you a number of policy options. Select the **Enable Expiration** checkbox.
- The options here include the ability to set retention periods

Editor's Note

G
Time to Beef Up Code Retention Policies

M
Managing Sandbox Solutions in SharePoint 2010

I
Using Email-Enabled Document Libraries in SharePoint

Figure 2

The created Exchange/Outlook contact will route to the document library.

and the option to choose which action to take once the set time period is reached. **FIGURE 3** shows setting an expiration policy to delete items after two years, based on the creation date.

- Click **OK** to apply the expiration policy.

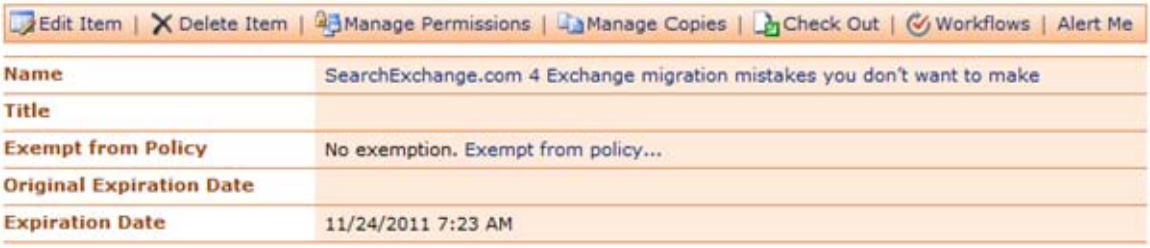
View the individual item's properties, found in the document library, to confirm that the expiration policy has been enabled (see **FIGURE 4**). ■

FIGURE 3

This is where you can set an expiration policy for your items.

FIGURE 4

Confirm that the item's expiration policy has been enabled.



Editor's Note

G
Time to Beef Up Code Retention Policies

M
Managing Sandbox Solutions in SharePoint 2010

I
Using Email-Enabled Document Libraries in SharePoint

ABOUT THE AUTHOR

George Khalil has 12 years of experience as manager of the information technology team at William Buck, an Australian national business advisory firm. Khalil is responsible for overseeing the provision of day-to-day IT support, as well as designing and implementing the company's IT systems. He is a Microsoft Certified IT Professional, Technology Specialist, Systems Engineer and Systems Administrator. Read his blog at http://sharepointgeorge.com/

- **DocAve Connector Delivers any Network or Cloud File Shares without Migration Directly to SharePoint**
- **Stream File Share Audio and Video Files Migration-Free into SharePoint, with DocAve Connector**
- **Seamlessly Present and Manage Network and Cloud File Share Content in SharePoint**

About AvePoint, Inc.: AvePoint is a global technology company and software innovator. Since 2001, AvePoint has been a leader in enterprise-strength infrastructure management solutions for the world's most popular collaboration platforms. Propelled by one of the world's largest development teams, AvePoint's award-winning DocAve and Atlas Software Platforms deliver comprehensive and flexible infrastructure support for SharePoint backup and recovery, replication, migration, administration, archiving, storage optimization, deployment management, compliance, and SharePoint-Salesforce integration.

- **Neverfail for SharePoint**
- **Neverfail for SharePoint datasheet**
- **Complimentary Continuous Availability for SharePoint Farms Whitepaper**

About Neverfail: Neverfail is a leading global software company providing affordable data protection, high availability, and disaster recovery solutions focused on keeping users productive. Neverfail's software solutions enable users to remain continuously connected to the live software application irrespective of hardware, software, operating system, or network failures. Neverfail's mission of eliminating application downtime for the end user delivers the assurance of business continuity, removes the commercial and IT management costs associated with system downtime and enables the more productive use of IT resources. Neverfail is a member of the Microsoft Gold Certified Partner Program, the Microsoft US Managed ISV Alliance Partner Program and is a member of the Microsoft SQL Server Always On Alliance.