

Battle Scarred But Still Standing: A SharePoint Administrator's Tell All

Jason Himmelstein (Raytheon Company)

www.sharepointlonghorn.com

@sharepointlhorn

Cornelius J. van Dyk (Crayveon Corporation)

www.cjvandyk.com/blog

@cjvandyk



Who are we? Where are we? What the...

- Cornelius J. van Dyk
 - 6 time Microsoft MVP
 - Enterprise Architect
 - Starfleet rank: Captain
 - @cjevandyk
 - <http://www.cjevandyk.com/blog>



- Jason Himmelstein
 - Raytheon SharePoint Architect
 - Enterprise Architect
 - Hula nickname: Sumo Longhorn
 - @sharepointlhorn
 - <http://www.sharepointlonghorn.com>

SharePoint
CONNECTIONS + Microsoft
Coast to Coast TOW SharePoint
BOOTCAMP

Demystify me, oh Demystifiers!

- What are we going to cover?
 - Service Accounts
 - what to use and why
 - Loopback Check
 - why can't I see my site from my server?
 - Managed Accounts
 - what the heck are they
 - Site Template Size Limit
 - How to fix it
 - Known Claims Authentication Issues
 - What have we found, and what to avoid
 - Introducing RBS...
 - The weight loss program for Content Databases

Service Accounts

- SQL Server service & administration: **SQL_Service**, **SQL_Admin**
- SharePoint Administrator and Setup User: **SP_Admin**
- SharePoint Farm Service: **SP_Farm**
- Application pool accounts: **SP_WebAppPool**, **SP_ServiceAppPool**
- SharePoint search crawl account: **SP_Crawl**
- User Profile Synchronization service account: **SP_UserSync**

SQL_Service, SQL_Admin

- SQL Server service account: **SQL_Service**
 - Domain user account
 - Assigned as the identity for MSSQLSERVER and SQLSERVER AGENT services during the setup of SQL Server
 - Additional least privilege
 - Use a unique account for SQLSERVER AGENT
 - **See TechNet for SQL hardening**
 - Setting Up Windows Service Accounts
<http://technet.microsoft.com/en-us/library/ms143504.aspx>
 - SQL Server Configuration Manager
<http://msdn.microsoft.com/en-us/library/ms174212.aspx>
- Unique account for SQL administrator: **SQL_Admin**
 - Domain user account
 - Local Administrators group of the SQL server
 - Assigned as a SQL administrator during installation of SQL Server

SP_Admin

- SharePoint Administrator and Setup User
- An account for a person performing
 - Install SharePoint prerequisites
 - Install SharePoint products
 - Configure SharePoint (SharePoint Products Configuration Wizard)
 - Update, patch, add/remove servers, etc.
- Must be:
 - Domain user account
 - In the local **Administrators** group of each server in the farm
 - SQL Server login with **securityadmin** and **dbcreator** server roles
 - **SharePoint_Shell_Access** database role for any database against which Windows PowerShell will be used (Add-SPShellAdmin)
- Unique, “generic” SharePoint administrative account
 - **Not your “normal” user or admin account**
 - After setup, you will add your “normal” account to Farm Administrators



SP_Farm

- SharePoint Farm Service
- An account used for **highly privileged** SharePoint services
 - Central Administration application pool
 - STS & Topology service application pool
 - Windows services including Timer, Workflow Timer
 - SharePoint services including User Profile Synchronization
- Domain user account
- Is given these permissions automatically
 - During farm setup: dbcreator and securityadmin fixed server roles
 - Creating databases: db_owner fixed db role for all SharePoint databases
 - Adding servers to farm: Given permissions a new server automatically
- ***Before provisioning User Profile Synchronization Service***
 - **Add to local Administrators** group of the server running UPS. Reboot.
 - Provision User Profile Synchronization.
 - After UPS has started, **remove** from group. Reboot.

SP_ServiceApps, SP_WebApps

- Web and service application pool account(s)
- Keeping it simple for this discussion... two accounts
- Domain user accounts
- Registered as managed accounts in the SharePoint farm
- Assigned as the application pool identity
 - First web application app pool: **SP_WebApps**
 - Additional web applications are added to the same, shared pool
 - First service application app pool: **SP_ServiceApps**
 - Additional service applications are added to the same, shared pool
- Permissions required depend on the web or service application
 - Generally assigned automatically by SharePoint

SP_Crawl

- Default SharePoint Search crawl account
 - Used to access SharePoint and other indexed content
- Domain user account
- Requires read permission to all indexed content sources
 - Automatically given Read permission to all SharePoint content
 - Through web application policy
 - **Assign read permission** to all other indexed content sources
- Unique account that does *not* have the ability to modify content
 - **Do not use the account for any other purpose**
- Additional crawl & index accounts
 - Separate accounts with access to crawl specific content sources

SP_UserSync

- SharePoint User Profile Synchronization
 - Used to synchronize user profile data between
- Active Directory and SharePoint
- Domain user account
- Unique account
 - **Do not use the account for any other purpose**
- Requires **Replicating Directory Changes** permission on domain
 - If a Windows Server 2003 domain
 - Add account to Pre-Windows 2000 Compatible Access group
 - This is **not a “big deal”!**
 - This permission is really “Detect changes to Domain NC”
 - Does not give access to “secrets” (e.g. passwords)
 - An educated Active Directory team should not have an issue with this
 - See TechNet user profile synchronization documentation

Why can't I see my SharePoint Sites from my SharePoint Server?!?!?!?

- Not a SharePoint Issue
- Local Loopback Check policy
 - Why?
 - DDoS attacks
- How do I fix this?
 - Option 1 (Production Servers)
 - create a Multi-String Value that has all of your AAMs for the server and restart the IISADMIN service.
 - Option 2 (non-Production Servers)
 - disable the LoopbackCheck on the server
- Where can I find more information on this for later?
 - <http://www.sharepointlonghorn.com/Lists/Posts/Post.aspx?ID=16>

What's up with this Managed Service Account thing?

- What is a service account?
 - A domain user account
 - Used as the identity of a service like SQL or SharePoint
- The pain point around service accounts is....

PASSWORD CHANGES

- What generally happens:
 - Service account password is changed
 - Update each location in which the service account is used
 - Result... Admins set Password never expires
 - Terrible for security
 - Service accounts are typically highly-privileged

Managed Service Accounts – cont'd

- What is a Managed Service Account?
 - An Active Directory account that has been *registered* in SharePoint
 - SharePoint can then submit requests to change the password on behalf of the account
- Register a managed account
 - Central Administration → Security → Configure managed accounts
 - Register a managed account
 - Enter the user name and current password
 - Enter user name as DOMAIN\name (e.g.: jase@spflogger.com)
 - MUST have the current password to register
- Use a managed account
 - When creating or configuring an app pool
 - Service Apps
 - Web Apps
 - When managing Windows services related to SharePoint
 - Timer, Search, Document Conversion

Changing Managed Account Passwords: Method 1

- Automatic
 - Set a schedule in the Central Administration → Security → Configure managed accounts → Edit screen
 - Set the change policy for number of days before expiration to change the password
 - Schedule
 - Based on scheduled date or domain password policy expiration
 - The system will take action based upon whichever comes first
 - Can Notify administrators by email
 - The service will be “down” while it recycles with the new password
- Benefits of Automatic method
 - Lower risk
 - SharePoint doesn't forget to change the password... come on Admins, we have all done it!
 - One less late night for your IT Staff
 - Zero chance of a fat finger mistake
 - Admins don't need to keep a list of passwords

Changing Managed Account Passwords: Method 2

- Manual
 - Go to Central Administration → Security → Configure managed accounts → Edit screen and:
 - Tell SharePoint to change the password to the password you specify
 - Or
 - Tell enter the new password that you have already set outside of SharePoint
- Benefits of Manual method
 - Total control
 - Can still have a centralized repository of all passwords offline

How secure is this?

- Farm passphrase
 - Secured key of registry accessible only by farm account (SP_Farm)
- Farm encryption key
 - Generated when you run PSConfig for first server in farm
 - Encrypted with farm passphrase
 - Stored in the Configuration Database
- Managed accounts are registered in the Configuration Database
 - Encrypted with the farm encryption key
- The results
 - Admins and developers do not need to know (and should NOT EVER know) service account passwords
- It is possible for farm administrators to retrieve the passwords
 - <http://www.sharepointlonghorn.com/Lists/Posts/Post.aspx?ID=11>

Site Template Size Limit

- Increase the site template size limit
 - STSADM -o setproperty -pn max-template-document-size -pv 524288000

Known Claims Authentication Issues

- SharePoint 2010 and the Site Directory
 - When you enable the Site Directory and you are using SharePoint 2010 in Claims mode for your web apps (including the site that houses the site directory) Central Administration is in Classic mode (the default and recommended way) and actions that call a web service from CA that touch back to the Site Directory will fail with errors that do not give you any real clues as to what is going on.
- PowerPivot Automated Data Refresh
 - On Classic Web apps: refresh works perfectly!
 - On Claims-enabled Web apps: refresh fails within seconds
 - Issue is in that the code for PowerPivot calls directly into the SharePoint Object Model and does not pass back to the WFE to get a claims token
 - Multiple cases are open, Microsoft is actively working to determine the overall right path forward

Attack of the BLOBs!!!!

- BLOBs
 - binary large objects are large blocks of data stored in a database that is known by its size and location instead of by its structure
 - Such as Office documents or video files.
- SharePoint Best Practice for Content Database size?

200 GB

- Why 200GB?
 - Backup & Restore concerns
 - How quickly does a 500GB database restore?

Introducing RBS... The weight loss program for Content Databases

- What is RBS?
 - A library API set that is incorporated as an add-on feature pack for Microsoft SQL Server 2008 R2 that allows SQL Server to store BLOBs in a location outside the content databases
- What are some of the benefits of RBS?
 - Ability to relocate largest parts of ContentDBs to inexpensive storage
 - Increased performance
 - Better I/O throughput on SQL Databases due to lower contention against BLOBs
 - Faster access to BLOBs due to lower contention against SQL
- How to implement RBS
 - FileStream - Free
 - Built in functionality of SQL Server (off server BLOB storage requires Enterprise License)
 - AvePoint DocAve Extender – Free
 - <http://www.avepoint.com>
 - StoragePoint – Costs money
 - <http://www.storagepoint.com>



Handy Reference Information

- **Useful Blogs**

- <http://www.cjvandyk.com/blog> - Corne's blog
 - @cjvandyk
 - c@sharepointmvp.net
- <http://www.sharepointlonghorn.com> – Jase's blog
 - @sharepointlhorn
 - jase@sharepointlonghorn.com



Your Feedback is Important

Please fill out a session evaluation form.

Thank you!

