Mn/DOT Contract No.: 97995

Admin No.: 24012

OET No.: 2677

IT Professional Technical Services
Master Contract Program
 # 902TS
Statement of Work (SOW)
For Technology Services
Issued by
Minnesota Department of Transportation (Mn/DOT)

Project Title: **SharePoint 2010 EDMS**

Service Categories: **FIRMS MUST BE QUALIFIED IN ONE OR MORE OF THE FOLLOWING SERVICE CATEGORIES IN ORDER TO BE CONSIDERED:**

- **Analyst-Business**
- **Project Management**
- **Web Applications Specialist – .NET/ASP**
- **Web Content Management – Metadata/Data Classifications**

1. Business Need

Mn/DOT requests responses for services to conduct a proof of concept pilot of Microsoft SharePoint 2010 to manage the agency's business documents, records, and workflows. The pilot will demonstrate whether SharePoint 2010 meets the requirements listed in Appendix A. Product evaluation topics include: document/records management, workflow, and forms; ease of operation and intuitiveness; web-based vs. client software; out-of-the-box functionality; and integration with Mn/DOT business and desktop applications.

Mn/DOT currently uses Open Text eDOCS version 5.2.103 (formerly Hummingbird) client-based software for EDMS. A gap analysis was conducted to determine if there are options that better meet business and technology requirements. The gap analysis addressed the need for improved use and expansion of EDMS in Mn/DOT. It recognized the need for added functionality, better alignment with Mn/DOT architecture, and better integration with standard desktop applications. A more effective licensing structure is also required to realize the desired performance level of the document/workflow management system.

Mn/DOT currently uses Bentley ProjectWise for management of engineering (CAD) files. A CAD management solution is outside the scope of this request for proposals. ProjectWise is included in the list (see Table 1) of applications operating in our current environment.

Table 1: Integration of Solution with Business Systems

Mn/DOT EDMS document, workflow and records management operates in a complex work environment. The solution should provide a seamless integration with Mn/DOT desktop applications, systems and architecture. Provided below is Mn/DOT standard desktop software and standard desktop utilities. For each software product identified below, describe how your solution integrates, and identify if the integration is out of the box or requires customization. If customization or an additional product or module is required please identify what is needed and provide an approximate cost.

Desktop Software	Current Version
Adobe Acrobat Professional & Standard Editions	8.2.1/8.2.1
Microsoft Office Professional 2007	SP2
Microsoft Outlook	SP2
Hummingbird DM (current product to be replaced)	5.2.103

Hummingbird DM Profile Handler (current product to be replaced)	1.9.26
Desktop Utilities	**Current Version**
Adobe Flash Player	10.0.45.2
Adobe Shockwave	11.5.0.596
Adobe Reader	9.3.0
McAfee Agent (ePO)	4
McAfee VirusScan Enterprise	8.5i Patch 7
Oracle Client	10g
ESRI ArcGIS Desktop	9.3 SP1
Business Objects Crystal Reports	XI R2
Bentley Microstation	V8i (08.11.07.443)
Bentley Descartes	V8i (08.11.07.100)
Bentley Geopak	V8i (08.11.07.246)
Bentley iPlot Organizer	V8i (8.11.07.89)
Bentley ProjectWise Navigator	V8i (08.11.07.171)
Bentley ProjectWise Explorer	V8i (08.11.07.107)
Microsoft Office Visio	2007
Microsoft Office Project	2007
BMC Remedy	ARSystem 7.5.4; Atrium CMDB 7.6.2; ITSM 7.5

Mn/DOT will be conducting a parallel pilot with the Bentley eB document management system and will consider potential integration between eB and SharePoint 2010.

Mn/DOT EDMS experience, 2002-present:

- Approximately 3 million cumulative document actions (created/edited/viewed)
- Approximately 300,000 active documents in the EDMS system
- 1,250 licensed users (employee population 4,800)
- Substantial customer support required due to client-based software installation and integration with Office 2007, Adobe Acrobat, GIS and ProjectWise, and e-signature solutions
- User experience with installation and integration issues have compromised or undermined the anticipated performance results
- Reliant on technical consultant for advanced problem resolution and customizations
- Mn/DOT staff spend considerable time resolving/reconciling customer support issues, rather than focusing on document/workflow management design and implementation projects
- Workstation upgrades required to effectively run EDMS with other desktop applications

Project Goal

It is the goal of this project to:

- Determine whether SharePoint 2010 can meet Mn/DOT's requirements for enterprise Document Management, Records Management, and Workflow, including electronic signature using ArX Cosign and Adobe Livecycle.
- Determine SharePoint 2010's ease of usability for end users and administrators for Document Management, Records Management, and Workflow.

It is expected that the Contractor will perform most of the tasks on-site in Mn/DOT's Central Office. Some tasks may be performed remotely with agreement from the Mn/DOT Project Manager.

2. Project Duties and Deliverables

The Selected Responder will perform the following duties and deliverables in accordance with the identified timeframe:

Task #	Task	Deliverables	Estimated Timeline
1	Set up a pilot environment to test SharePoint 2010 against the requirements in Appendix A.	Virtual server, licenses, administrative structure, and any required software and plug-ins to enable Mn/DOT staff to test SharePoint 2010 against the requirements in Appendix A. Approx. 2000 documents migrated into the pilot environment.	In first 30 days of contract
2	Develop test cases and associated traceability matrix based on the requirements in Appendix A. Recommend what to test, how to test, and how to measure results.	Test cases and traceability matrix written.	In first 30 days of contract
3	Develop performance criteria for evaluating usability and functionality of document management, records management, and workflow processes.	Performance criteria documented. If a requirement is not met, document how the product did not meet the requirement and what it would take to meet the requirement.	In first 30 days of contract
4	Demonstrate and document whether SharePoint 2010 operates seamlessly with Mn/DOT applications, systems and architecture as identified in Table 1.	Documentation on how SharePoint 2010 integrates with each of the software products in Table 1, and identification of whether integration is out of the box or requires customization. If customization or an additional product or module is required, include identification of what is needed and an approximate cost.	By end of pilot
4a	Demonstrate and document whether SharePoint 2010 operates seamlessly with the ArX Cosign e-signature tool to do the following: • Ability to upload e-forms and prepare documents for signing (Internal & external) • Provide the ability for state agency staff or external partners to review and sign documents via SharePoint and ArX Cosign; and provide the ability for staff to review and sign documents via SharePoint and Adobe Livecycle • Integrate with SharePoint to provide workflow and alert for documents requiring electronic signatures	Documentation on how SharePoint 2010 operates with ArX Cosign for electronic forms and electronic signature and approval workflow	20-day period within the pilot

	• Provide the ability to integrate with SharePoint to record and review the document activities related to the electronic signature process		
4b	Demonstrate and document whether SharePoint 2010 operates seamlessly with the Adobe Livecycle e-signature tool to do the following: • Ability to upload e-forms and prepare documents for signing (Internal & external) • Provide the ability for state agency staff or external partners to review and sign documents via SharePoint and ArX Cosign; and provide the ability for staff to review and sign documents via SharePoint and Adobe Livecycle • Integrate with SharePoint to provide workflow and alert for documents requiring electronic signatures • Provide the ability to integrate with SharePoint to record and review the document activities related to the electronic signature process	Documentation on how SharePoint 2010 operates with Adobe Livecycle for electronic forms and electronic signature and approval workflow	20-day period within the pilot
5	Support and mentor Mn/DOT staff in operating the pilot.	Troubleshooting and teaching provided as needed, adjustments to pilot environment made as needed.	Continuous during contract period
6	Demonstrate how the product fills requirements related to integration with legacy business database applications.	Integration with a selected Oracle database completed and tested.	February, 2011
7	Perform simulated testing of requirements as needed (for example, large numbers of simultaneous transactions or large document imports).	Tests conducted and results reported.	February, 2011
8	Demonstrate the ability to integrate SharePoint 2010 with Bentley eB and with Bentley ProjectWise.	Integration with Bentley eB and with Bentley ProjectWise completed and tested.	By end of pilot
9	Recommend improved document management, records management, and workflow practices based on SharePoint 2010 capabilities in these areas.	Report completed with recommendations.	By end of pilot
10	Develop a plan to migrate Mn/DOT documents from the current EDMS system to SharePoint 2010. Migration depends on the proven viability of	Migration plan completed.	By end of pilot

	SharePoint 2010 for Document Management, Records Management, and Workflow.		
11	Collaborate with Mn/DOT Office of Enterprise Technology (OET) staff for the creation of the SharePoint2010 pilot environment. See Appendix B	Troubleshooting and teaching provided as needed, adjustments to pilot environment made as needed.	In first 10 days of contract

3. Project Milestones and Schedule

3.1	Project start date:	Upon Contract Execution
3.2	Key deliverable dates:	See Section 2
3.3	End date:	04/30/2011

4. Project Environment (Mn/DOT Resources)

For all inquiries regarding this SOW contact the Mn/DOT Contract Administrator Melissa McGinnis at 651-366-4644. Contact with any other Mn/DOT personnel regarding this SOW may result in disqualification.

5. Project Constraints

Mn/DOT implementation requirements include:

5.1 Compliance with the Statewide Enterprise Architecture
5.2 Compliance with Statewide Project Management Methodology
5.3 Compliance with applicable industry/agency standards

6. Required Skills (These are to be rated on a pass/fail basis)

Required minimum qualifications are shown in the following table. The proposal must specifically indicate how members of the Responder's team meet these minimum qualifications. This portion of the proposal review will be conducted on a pass/fail basis. If Mn/DOT determines, in its sole discretion, that the Responder fails to meet one or more of these requirements (or that the Responder has not submitted sufficient information to make the pass/fail determination), then the proposal will be eliminated from further review.

	Required Skill Type	**Minimum Number of Years Experience**
6.1	Expertise and applied experience in SharePoint 2007	2 years
6.2	Expertise and applied experience in SharePoint 2010. This includes business and technical implementation, maintenance, support, and use.	6 months
6.3	Applied experience in using SharePoint 2010 for enterprise document management.	6 months
6.4	Applied experience in using SharePoint 2010 for enterprise records management.	6 months
6.5	Applied experience in using SharePoint 2010 for complex workflows.	6 months
6.6	Applied experience writing test cases and traceability matrices for SharePoint 2007 – 2010	2 years
6.7	Applied experience in using electronic signature tools for signature, e-forms, and routing & approval workflow	1 year

7. Desired Skills

Mn/DOT desires a project team with the skills shown in the table below. The extent to which the Responder meets or exceeds the desired skills will be included as part of the qualitative evaluation of the proposal.

	Desired Skill Type	Minimum Number of Years Experience

7.1	Applied experience with connections between SharePoint and ESRI GIS	1 year
7.2	Applied experience with connections between SharePoint and Bentley ProjectWise	1 year
7.3	Applied experience with ArX Cosign and Adobe Livecycle	1 year
7.4	Applied experience with implementing SharePoint in public agencies (federal, state, or local)	3 or more projects. **Provide references to these projects in response.**

8. Process Schedule

8.1	Deadline for Questions	01/03/2011	2:00 PM Central Standard Time
8.2	Posted Response to Questions	01/07/2011	2:00 PM Central Standard Time
8.3	Proposals due	01/14/2011	2:00 PM Central Standard Time
8.4	Anticipated proposal evaluation begins	01/20/2011	
8.5	Anticipated proposal evaluation & decision	01/28/2011	

9. Questions

All questions regarding this SOW must be addressed to the Mn/DOT Contract Administrator listed below. Proposers may not discuss the content of this SOW with other Mn/DOT staff. Any questions regarding this SOW must be received via e-mail by 01/03/2011, 2:00PM Central Standard Time.

Contract Administrator: Melissa McGinnis
Email Address: melissa.mcginnis@state.mn.us

It is anticipated that questions and answers will be posted on the Office of Enterprise Technology's web site by 01/07/2011, 2:00pm Central Standard Time (www.oet.state.mn.us). Note that questions may be posted verbatim as submitted.

10. Indemnification

In the performance of this contract by Contractor, or Contractor's agents or employees, the Contractor must indemnify, save, and hold harmless the State, its agents, and employees, from any claims or causes of action, including attorney's fees incurred by the state, to the extent caused by Contractor's:

1) Intentional, willful, or negligent acts or omissions; or
2) Actions that give rise to strict liability; or
3) Breach of contract or warranty.

The indemnification obligations of this section do not apply in the event the claim or cause of action is the result of the State's sole negligence. This clause will not be construed to bar any legal remedies the Contractor may have for the State's failure to fulfill its obligation under this contract.

The "Standard Indemnification Clause" (see above) will apply to this project and will be incorporated into the work order issued for this project. No exceptions to, or deviations from, this clause will be permitted. Do not submit a proposal if you cannot accept this indemnification clause. Proposals which the State determines, in its sole discretion, indicate non-acceptance of this indemnification clause, will be rejected by the State.

11. SOW Evaluation Process

Mn/DOT representatives will evaluate proposals received by the deadline. Proposals will be evaluated on a "Best Value" basis of 70% qualifications and 30% cost considerations. The review committee will not open the cost proposals until after the qualifications points have been awarded.

The selection process being used for this project involves a two step process. Step one will include the pass/fail assessment and a qualitative evaluation of Contractors' technical proposal. Step Two will be an analysis of the cost proposal.

Mn/DOT will review proposals according to the following criteria:

- Experience of personnel assigned to this project and the extent to which they meet the Desired Skills 15%
- Proposed work plan, including the apparent ability to complete project on time and on budget 30%
- Expressed understanding of project objectives 10%
- Qualifications/experience of company 5%
- Extent to which services will be performed within the U.S.* 10%
- Cost 30%

Mn/DOT reserves the right to check references and to review previous performance reviews for work performed for Mn/DOT or other state agencies, and to take such references and reviews into account for consultant selection purposes.

The following contains additional information describing the proposal evaluation process:

Step One

In step one the proposals will first be reviewed to verify whether the proposer meets the "Required Skills" (see section six). Proposals receiving a "fail" on one or more of the required skills will not be reviewed further. Proposals which pass the Required Skills review will then be scored on the non-cost and non-interview factors listed above.

Step Two

Cost proposal will be evaluated and scored in accordance with the percentage listed above. Cost will not be revealed to selection committee members until after the technical scoring has been completed.

12. Response Requirements

12.1 Introduction.
12.2 Company overview.
12.3 Project overview.
12.4 An outline of the responder's background and experience with examples of similar work done and a list of personnel who will conduct the project, detailing their training and work experience. No change in personnel assigned to the project will be permitted without the written approval of Mn/DOT's Project Manager. Include specific experience with Document Management, Records Management, and Workflow.
12.5 Detailed response to "Project Approach".
Explain how the responder will approach their participation in the project. This includes:
12.5.1 Organization and staffing. Include staff qualifications in a chart **AND** resumes that will allow Mn/DOT to easily determine if assigned key staff meet the required skills and the extent to which assigned staff meet or exceed the desired skills. **The chart must align with the skills identified in the resumes.**

Required Skill type	**Personnel/ Years of Experience**	**Project(s) worked on demonstrating these skills**	**Reference (name, company, phone number)**

12.5.2 A detailed work plan that will identify the major tasks to be accomplished and be used as a scheduling and management tool, as well as the basis for invoicing. The work plan must present the responder's approach, task breakdown, deliverable due dates and personnel working on the project and the hours assigned to each individual to reach the project results. The work plan should also include a realistic plan to meet the projects target completion date.

12.5.3 Contract/change management procedures.

12.5.4 Project management (e.g. quality management, risk assessment/management, etc.).

12.5.5 Documentation of progress such as status reports.

12.5.6 Provide three references for similar work. Include contact person, firm, email address and phone number along with a brief description of the duties that the key personnel performed for that project.

12.6 Submit a cost proposal in a separate sealed envelope. Rates proposed may not exceed the rates approved under this program. Cost proposal must include the number of anticipated hours, classifications of personnel, personnel hourly rates and a total project cost. If direct expenses are anticipated they must be detailed in the cost proposal. **The cost estimate must correspond to the detailed work plan and schedule that includes time estimates, associated deliverables, and staff assigned to each task.**

12.7 Required forms to be returned or additional provisions that must be included in proposal:

12.7.1 **Location of Service Disclosure Form.**

12.7.2 **Conflict of Interest Form**

Proposer must provide a list of all entities with which it has relationships that create, or appear to create, a conflict of interest with the work that is contemplated in this request for proposals. The list should indicate the name of the entity, the relationship, and a discussion of the conflict.

The proposer warrants that, to the best of its knowledge and belief, and except as otherwise disclosed, there are no relevant facts or circumstances which could give rise to organizational conflicts of interest. An organizational conflict of interest exists when, because of existing or planned activities or because of relationships with other persons, a proposer is unable or potentially unable to render impartial assistance or advice to Mn/DOT, or the proposer's objectivity in performing the contract work is or might be otherwise impaired, or the proposer has an unfair competitive advantage. The proposer agrees that, if after award, an organizational conflict of interest is discovered, an immediate and full disclosure in writing must be made to Mn/DOT which must include a description of the action which the proposer has taken or proposes to take to avoid or mitigate such conflicts. If an organization conflict of interest is determined to exist, Mn/DOT may, at its discretion, cancel the contract. In the event the proposer was aware of an organizational conflict of interest prior to the award of the contract and did not disclose the conflict to Mn/DOT, Mn/DOT may terminate the contract for default. The provisions of this clause must be included in all subcontracts for work to be performed similar to the service provided by the prime contractor, and the terms "contract," "contractor," and "contracting officer" modified appropriately to preserve Mn/DOT's rights. Proposers must complete the attached "Conflict of Interest Checklist and Disclosure Form" and submit it along with the response, but not as a part of the response.

12.7.3 **Affidavit of non-collusion**

Proposers must complete the attached "Affidavit of Noncollusion" and include it with the response. The successful proposer will be required to submit acceptable evidence of compliance with workers' compensation insurance coverage requirements prior to execution of the Contract.

12.7.4 **Immigration Status Certification Form**

For all Contracts estimated to be in excess of $50,000.00, responders are required to complete the attached "Immigration Status Certification Form" page and include it with the response.

12.7.5 **Affirmative Action Certification**
For all Contracts estimated to be in excess of $100,000.00, responders are required to complete the attached "Affirmative Action Certification" page and include it with the response.

12.7.6 **Veteran-Owned/Service-Disabled Veteran-Owned Preference Forms.**
Proposers must complete and submit this form if claiming preference as a qualified proposer.

13. Proposal Submission Instructions

Submit 7 copies of the response. Responses are to be submitted in a mailing envelope or package, clearly marked "Proposal" on the outside. Cost proposals are to be submitted in a separate sealed envelope. An authorized member of the firm must sign each copy of the response in ink.

All responses must be sent to:

Melissa McGinnis, Contract Administrator
Minnesota Department of Transportation
395 John Ireland Boulevard
Consultant Services Section, Mail Stop 680
St. Paul, Minnesota 55155

All responses must be received not later than 2:00 p.m. Central Standard Time on 01/14/2011, as indicated by the time stamp made by the Contract Administrator. **Please note that Mn/DOT Offices have implemented security measures**. These procedures do not allow non-Mn/DOT employees to have access to the elevators or the stairs. You should plan enough time and follow these instructions for drop-off:

- Enter through the Rice Street side of the Central Office building (1st Floor).
- Once you enter through the doors, you should proceed to the first floor Information Desk.
- **Proposals are accepted at the first floor Information Desk only**. The receptionist will call the Contract Administrator to come down and to time stamp the proposal. Please keep in mind Mn/DOT is very strict on the proposal deadline. Proposals will not be accepted after 2:00pm.

14. General Requirements

14.1 **Proposal Contents**
By submission of a proposal, Proposer warrants that the information provided is true, correct and reliable for purposes of evaluation for potential award of a work order. The submission of inaccurate or misleading information may be grounds for disqualification from the award as well as subject the proposer to suspension or debarment proceedings and other remedies available at law.

14.2 **Disposition of Responses**
All materials submitted in response to this SOW will become property of the State and will become public record in accordance with Minnesota Statutes, section 13.591, after the evaluation process is completed. Pursuant to the statute, completion of the evaluation process occurs when the government entity has completed negotiating the contract with the selected Proposer. If the Proposer submits information in response to this SOW that it believes to be trade secret materials, as defined by the Minnesota Government Data Practices Act, Minn. Stat. § 13.37, the Proposer must: clearly mark all trade secret materials in its response at the time the response is submitted, include a statement with its response justifying the trade secret designation for each item, and defend any action seeking release of the materials it believes to be trade secret, and indemnify and hold harmless the State, its agents and employees, from any judgments or damages awarded against the State in favor of the party requesting the materials, and any and all costs connected with that defense. This indemnification survives the State's award of a contract. In submitting a response to this RFP, the

Proposer agrees that this indemnification survives as long as the trade secret materials are in possession of the State.

Mn/DOT will not consider the prices submitted by the Proposer to be proprietary or trade secret materials.

15. No State Obligation

Issuance of this Statement of Work does not obligate Mn/DOT to award a contract or complete the assignment, and Mn/DOT reserves the right to cancel this solicitation if it is considered to be in its best interest. Mn/DOT reserves the right to reject any and all proposals.

16. Veteran-owned/Service Disabled Veteran-Owned Preference

In accordance with Laws of Minnesota, 2009, Chapter 101, Article 2, Section 56, eligible certified veteran-owned and eligible certified service-disabled veteran-owned small businesses will receive a 6 percent preference in the evaluation of their proposal.

Eligible veteran-owned and eligible service-disabled veteran-owned small businesses should complete the Veteran-Owned/Service Disabled Veteran-Owned Preference Form in this solicitation, and include the required documentation. Only eligible, certified, veteran-owned/service disabled small businesses that provide the required documentation, per the form, will be given the preference.

Eligible veteran-owned and eligible service-disabled veteran-owned small businesses must be **currently** certified by the U.S. Department of Veterans Affairs prior to the solicitation opening date and time to receive the preference.

Information regarding certification by the United States Department of Veterans Affairs may be found at http://www.vetbiz.gov.

The balance of this page has been intentionally left blank.

Appendix A: Requirements for proof-of-concept pilot for Mn/DOT Document Management, Records Management, and Workflow

Document Management

1. User can quickly see a list of the documents they have recently worked on.
2. User can check out and check in files.
3. User can see status of a document (checked out to whom, available, read-only, etc.).
4. User can save searches.
5. User can perform Boolean searches.
6. Administrator can set the maximum number of search results delivered.
7. User can search full text and/or index data.
8. Ability to save and view all standard image file formats, video files, audio files, MS Office files, MS Project, Visio, Access, and MicroStation files.
9. Ability to insert the URL hyperlink for a document into another document, database, web page (intranet or external), or email message.
10. Each document, folder, and subfolder has a unique URL and index data.
11. User can save email and attachments directly from Outlook.
12. Administrator can set up metadata based on the defined document taxonomy of the agency, can create dropdown lists and lookup tables, and can set mandatory metadata for saving documents.
13. Metadata lookups can be populated through interfaces to line of business databases.
14. Metadata can be auto-populated when saving a document, based on business rules and interfaces with line of business databases. For example, when the user types in a State Project Number, the system supplies additional index data from a designated database based on the S.P. number.
15. User can overtype index data that has been auto-populated.
16. Multiple index values can be entered in index fields.
17. Administrator can set defaults based on user groups or roles. Defaults may apply to individual documents or to folders.
18. Supports federated search and viewing from identified repositories and databases. In particular, supports retrieval and viewing from Bentley ProjectWise.
19. All actions taken on a document must create an audit trail, which can be easily viewed.
20. A date and timestamp is automatically supplied when document is saved.
21. Ability to batch import existing electronic files.
22. Documents imported from existing repositories retain original file creation date on import.
23. User can create multiple versions of a document, and add version comments.
24. User can save edits as a new document or a new version.
25. Index data can be changed for a batch of documents.
26. Documents can be accessed and viewed from mobile devices such as Blackberry.
27. Read-only templates can be stored for re-use.

Workflow

1. Design a multi-approval, conditionally branched workflow
2. Push and pull data from a business application (Oracle database)
3. Must be able to notify specified persons when errors occur (missing data, undeliverable email, etc.)
4. Users must have a choice to receive email task notifications, or work from a worklist on a web site.
5. Tasks must be assignable to multiple persons and be removed from others' worklists when one person accepts the task.
6. Users must be able to add permanent comments to a workflow.

7. Permissions must be definable at a granular level.
8. Task reassignments for current running workflows can be made by user, a defined supervisor, or a workflow administrator.
9. Emails created by workflow must be able to contain attachments that are links to specific documents (users within the firewall) but also be able to contain attachments in their native formats (users outside the firewall).
10. Documents presented by workflow must be editable, subject to documents' assigned security.
11. Users must be able to apply electronic signatures using either ArX Cosign or Adobe Livecycle.
12. Reporting capabilities must allow a workflow administrator to produce:
    - A report showing where any specific workflow sits at a given time, both tabular and graphically
    - A report of all running instances of a given workflow template, and separately, all workflow templates, showing history and current status
    - A report of all completed workflows showing date/times of completed tasks, who completed the task, elapsed times, and workflow comments

Records Management

1. Ability to define and place legal, audit or pending holds on documents and to manage email for such holds.
2. Ability to place multiple holds on documents.
3. Ability to mark records as public or nonpublic for compliance with Minnesota Data Practices Act.
4. Must guarantee the integrity of the records, including index data; must be a document management system that can be considered to store electronic information in a trustworthy and reliable manner.
5. Document categories can correspond to retention schedule categories, so that retention can be placed on documents.
6. Reports can be generated to indicate whether documents are in compliance with the retention schedule.
7. Administrator can control settings so that deletion requests may result in either removal of both the Document and the Marker, or removal of the Document but retention of the Marker and Index Data.
8. When a user "deletes" a document, it goes into a "queue" until deleted by an administrator, and can be restored during that period by an administrator.
9. Ability to track and manage physical records (boxes, microfilm, etc.)
10. Ability to track and manage all records for changes in location, disposition or media type, including scheduling rules, trigger events or actions.
11. Documents imported from another EDMS system retain their versions.
12. Support backward compatibility so that a document created in previous versions of an application can be opened in future versions of the application.
13. Ability for a retention rule to trigger an action on a document, such as flagging it for destruction, marking its status (expired, transferred, made permanent, etc.) or moving it to an archive.
14. Ability to integrate with barcode technologies.
15. Ability to generate labels.

Security and Access Control

1. Administrator can set security defaults by user group or by document criteria.
2. Users can be given full rights to their documents, including rights to change security.
3. Subfolders inherit the permissions of the parent folders.
4. Administrator can override the security policy on a document or folder.
5. Single sign-on is supported for users authenticated to the Mn/DOT network.
6. Documents can be made read-only and archived for storage and viewing.

7. Users can have full functionality using remote access with a secure login.
8. Allow users outside Mn/DOT with authorized access to have the ability to check out and check in files.
9. Viewing rights to documents can be given to an external guest group for placing URL links to documents on an external web page.

Other

1. Ability to have links with ArcGis server so that a GIS user can click on a geospatial item on a map and bring up documents that have that geospatial item in their index data.
2. Provide open API to development interfaces to other applications.
3. Provide electronic forms functionality.
4. Ability to automatically archive email messages and attachments based on business rules, including recognition of duplicates.
5. Ability to do batch scanning including Optical Character Recognition for import into the system.

ProjectWise Integration

The following tasks shall be completed from a SharePoint interface and utilizing data / documents from the Mn/DOT ProjectWise system without copying the documents into any other (non-ProjectWise) repository.

Document Management

1. User can quickly see a list of the ProjectWise (PW) documents they have recently worked on.
2. User can see status of a PW document (checked out to whom, available, read-only, etc.).
3. User can perform Boolean searches of PW from within SharePoint.
4. SharePoint Administrator can set the maximum number of search results delivered.
5. User can search full text data.
6. Ability to view all standard image file formats, video files, audio files, MS Office files, MS Project, Visio, Access, and MicroStation files stored in PW.
7. Ability to open / check out standard file formats, (MS Office files, and CAD (MicroStation, AutoCAD, Raster) files stored in PW by launching ProjectWise and the native application.
8. Administrator can set defaults based on user groups or roles.
9. Supports federated search and viewing from identified repositories and databases. In particular, supports retrieval and viewing from Bentley ProjectWise.
10. All actions taken on a document must create or be appended to the PW audit trail, which can be easily viewed from SharePoint.
11. Users must be able to apply electronic signatures using ArX Cosign or Adobe Livecycle.

Security and Access Control

1. Single sign-on is supported for users authenticated to the Mn/DOT network.
2. Users can have full functionality using remote access with a secure login.
3. Allow users outside Mn/DOT with ProjectWise logins to have the ability to check out and check in files, based on PW permissions (granted via AD groups.)

Other

1. Ability to have links with ArcGis server so that a GIS user can click on a geospatial item on a map and bring up documents that have that geospatial item in their index data.

Appendix B: SharePoint 2010 Server Environment for Mn/DOT EDMS Pilot

Mn/DOT and the Minnesota Office of Enterprise Technology (OET) wish to collaborate on creation of a SharePoint 2010 environment for the Mn/DOT EDMS Pilot. The desired environment will be built to support both the Mn/DOT EDMS Pilot and OET's pending migration to Microsoft's dedicated Business Productivity Online Suite (BPOS-D). From a high-level view, the intended server environment will provide both Mn/DOT and OET with a preview of the capabilities, administration tasks, development roles, and issues involved in using the BPOS-D environment for both OET and Mn/DOT's long-term projects and initiatives.

Prospective responders to this RFP will be expected to work directly with OET and Mn/DOT staff to create a SharePoint 2010 server environment that supports the needs of the Mn/DOT EDMS Pilot defined in the main RFP document, Appendix A, and the following server environment requirements:

1. Work with OET and Mn/DOT staff to define the correct SharePoint 2010 architecture necessary to support the combined needs of OET's BPOS-D test environment and Mn/DOT's EDMS Pilot.
2. Build the defined SharePoint 2010 architecture in a VMWare environment according to the processes defined in the "Microsoft SharePoint Online Dedicated 2010 Build Guide".
3. Work with OET staff, hardware, software, and networking resources to build the base EDMS Pilot environment.
4. Collaborate with and mentor OET and Mn/DOT staff on the details of the build process.
5. Use OET and Mn/DOT provided staff, hardware, software, and networking resources to enhance the EDMS Pilot environment so that it is suitable for the tasks defined in this RFP.
6. Follow Microsoft provided guidelines for establishing a BPOS-like Active Directory management forest with necessary connections to agency forests containing user accounts.
7. Provision the Pilot environment with necessary Active Directory accounts for the RFP tasks.
8. Install the server environment in conformance to OET network, firewall, and security standards.
9. Work with OET and Mn/DOT staff to establish network connections between the EDMS Pilot environment and Mn/DOT network resources necessary for the RFP tasks.
10. Work with OET staff to define, document, and execute necessary SharePoint administration tasks that exceed the Site Collection Administration capabilities that will be assigned to Mn/DOT staff. Because the BPOS-D environment does not provide Farm Administration capabilities, OET and Mn/DOT will work together to understand and work within this role boundary.

STATE OF MINNESOTA
LOCATION OF SERVICE DISCLOSURE AND CERTIFICATION

LOCATION OF SERVICE DISCLOSURE

Check all that apply:

☐ The services to be performed under the anticipated contract as specified in our proposal will be performed ENTIRELY within the State of Minnesota.

☐ The services to be performed under the anticipated contract as specified in our proposal entail work ENTIRELY within another state within the United States.

☐ The services to be performed under the anticipated contract as specified in our proposal will be performed in part within Minnesota and in part within another state within the United States.

☐ The services to be performed under the anticipated contract as specified in our proposal DO involve work outside the United States. Below (or attached) is a description of:

- The identity of the company (identify if subcontractor) performing services outside the United States;
- The location where services under the contract will be performed; and
- The percentage of work (in dollars) as compared to the whole that will be conducted in each identified foreign location.

CERTIFICATION

By signing this statement, I certify that the information provided above is accurate and that the location where services have been indicated to be performed will not change during the course of the contract without prior, written approval from the State of Minnesota.

Name of Company: _____

Authorized Signature: _____

Printed Name: _____

Title: _____

Date: _____

Telephone Number: _____

STATE OF MINNESOTA
VETERAN-OWNED/SERVICE DISABLED VETERAN-OWNED PREFERENCE FORM

In accordance with Laws of Minnesota, 2009, Chapter 101, Article 2, Section 56, eligible certified veteran-owned and eligible certified service-disabled veteran-owned small businesses will receive a 6 percent preference in the evaluation of their proposal.

Eligible veteran-owned and eligible service-disabled veteran-owned small businesses include certified small businesses that are majority-owned and operated by either (check the box that applies and attach the certification documents required with your response to this solicitation):

☐ (1) recently separated veterans, who are veterans as defined in Minn. Stat. §197.447, who have served in active military service, at any time on or after September 11, 2001, and who have been discharged under honorable conditions from active service, as indicated by the person's United States Department of Defense form DD-214 or by the commissioner of veterans affairs; or

Required Documentation:

- certification by the United States Department of Veterans Affairs as a veteran-owned small business
- discharge form (DD-214) dated on or after September 11, 2001 with condition honorable

☐ (2) Veterans who are veterans as defined in Minn. Stat. § 197.447, with service-connected disabilities, as determined at any time by the United States Department of Veterans Affairs.

Required Documentation:

- certification by the United States Department of Veterans Affairs as a service-disabled veteran-owned small business.

Eligible veteran-owned and eligible service-disabled veteran-owned small businesses must be **currently** certified by the U.S. Department of Veterans Affairs prior to the solicitation opening date and time to receive the preference.

Information regarding certification by the United States Department of Veterans Affairs may be found at http://www.vetbiz.gov .

You must submit this form and the documentation required above with your response in order to be considered for this preference.

CONFLICT OF INTEREST CHECKLIST AND DISCLOSURE FORM

Purpose of this Checklist. This checklist is provided to assist proposers in screening for potential organizational conflicts of interest. The checklist is for the internal use of proposers and does not need to be submitted to Mn/DOT, however, the Disclosure of Potential Conflict of Interest form should be submitted in a separate envelope along with your proposal.

Definition of "Proposer". As used herein, the word "Proposer" includes both the prime contractor and all proposed subcontractors.

Checklist is Not Exclusive. Please note that this checklist serves as a guide only, and that there may be additional potential conflict situations not covered by this checklist. If a proposer determines a potential conflict of interest exists that is not covered by this checklist, that potential conflict must still be disclosed.

Use of the Disclosure Form. A proposer must complete the attached disclosure form and submit it with their Proposal (or separately as directed by Mn/DOT for projects not awarded through a competitive solicitation). If a proposer determines a potential conflict of interest exists, it must disclose the potential conflict to Mn/DOT; however, such a disclosure will not necessarily disqualify a proposer from being awarded a Contract. To avoid any unfair "taint" of the selection process, the disclosure form should be provided separate from the bound proposal, and it will not be provided to selection committee members. Mn/DOT Contract Management personnel will review the disclosure and the appropriateness of the proposed mitigation measures to determine if the proposer may be awarded the contract notwithstanding the potential conflict. Mn/DOT Contract Management personnel may consult with Mn/DOT's Project Manager and Department of Administration personnel. By statute, resolution of conflict of interest issues is ultimately at the sole discretion of the Commissioner of Administration.

Material Representation. The proposer is required to submit the attached disclosure form either declaring, to the best of its knowledge and belief, either that no potential conflict exists, or identifying potential conflicts and proposing remedial measures to ameliorate such conflict. The proposer must also update conflict information if such information changes after the submission of the proposal. Information provided on the form will constitute a material representation as to the award of this Contract. Mn/DOT reserves the right to cancel or amend the resulting contract if the successful proposer failed to disclose a potential conflict, which it knew or should have known about, or if the proposer provided information on the disclosure form that is materially false or misleading.

Approach to Reviewing Potential Conflicts. Mn/DOT recognizes that proposer's must maintain business relations with other public and private sector entities in order to continue as viable businesses. Mn/DOT will take this reality into account as it evaluates the appropriateness of proposed measures to mitigate potential conflicts. It is not Mn/DOT's intent to disqualify proposers based merely on the existence of a business relationship with another entity, but rather only when such relationship causes a conflict that potentially impairs the proposer's ability to provide objective advice to Mn/DOT. Mn/DOT would seek to disqualify proposers only in those cases where a potential conflict cannot be adequately mitigated. Nevertheless, Mn/DOT must follow statutory guidance on Organizational Conflicts of Interest.

Statutory Guidance. Minnesota Statutes §16C.02, subd. 10 (a) places limits on state agencies ability to contract with entities having an "Organizational Conflict of Interest". For purposes of this checklist and disclosure requirement, the term "Vendor" includes "Proposer" as defined above. Pursuant to such statute, "Organizational Conflict of Interest" means that because of existing or planned activities or because of relationships with other persons: (1) the vendor is unable or potentially unable to render impartial assistance or advice to the state; (2) the vendor's objectivity in performing the contract work is or might otherwise be impaired; or (3) the vendor has an unfair advantage.

Additional Guidance for Professionals Licensed by the Minnesota Board of Engineering. The Minnesota Board of Engineering has established conflict of interest rules applicable to those professionals licensed by the Board (see Minnesota Rules part 1805.0300) Subpart 1 of the rule provides "A licensee shall avoid accepting a commission where duty to the client or the public would conflict with the personal interest of the licensee or the interest of another client. Prior to accepting such employment the licensee shall disclose to a prospective client such facts as may give rise to a conflict of interest".

An organizational conflict of interest may exist in any of the following cases:

- The proposer, or its principals, own real property in a location where there may be a positive or adverse impact on the value of such property based on the recommendations, designs, appraisals, or other deliverables required by this Contract.

- The proposer is providing services to another governmental or private entity and the proposer knows or has reason to believe, that entity's interests are, or may be, adverse to the state's interests with respect to the specific project covered by this contract. **Comment:** the mere existence of a business relationship with another entity would not ordinarily need to be disclosed. Rather, this focuses on the nature of services commissioned by the other entity. For example, it would not be appropriate to propose on a Mn/DOT project if a local government has also retained the proposer for the purpose of persuading Mn/DOT to stop or alter the project plans.

- The Contract is for right-of-way acquisition services or related services (e.g. geotechnical exploration) and the proposer has an existing business relationship with a governmental or private entity that owns property to be acquired pursuant to the Contract.

- The proposer is providing real estate or design services to a private entity, including but not limited to developers, whom the proposer knows or has good reason to believe, own or are planning to purchase property affected by the project covered by this Contract, when the value or potential uses of such property may be affected by the proposer's performance of work pursuant to this Contract. "Property affected by the project" includes property that is in, adjacent to, or in reasonable proximity to current or potential right-of-way for the project. The value or potential uses of the private entity's property may be affected by the proposer's work pursuant to the Contract when such work involves providing recommendations for right-of-way acquisition, access control, and the design or location of frontage roads and interchanges. **Comment**: this provision does not presume proposers know or have a duty to inquire as to all of the business objectives of their clients. Rather, it seeks the disclosure of information regarding cases where the proposer has reason to believe that its performance of work under this contract may materially affect the value or viability of a project it is performing for the other entity.

- The proposer has a business arrangement with a current Mn/DOT employee or immediate family member of such employee, including promised future employment of such person, or a subcontracting arrangement with such person, when such arrangement is contingent on the proposer being awarded this Contract. This item does not apply to pre-existing employment of current or former Mn/DOT employees, or their immediate family members. **Comment:** this provision is not intended to supersede any Mn/DOT policies applicable to its own employees accepting outside employment. This provision is intended to focus on identifying situations where promises of employment have been made contingent on the outcome of this particular procurement. It is intended to avoid a situation where a proposer may have unfair access to "inside" information.

- The proposer has, in previous work for the state, been given access to "data" relevant to this procurement or this project that is classified as "private" or "nonpublic" under the Minnesota Government Data Practices Act, and such data potentially provides the proposer with an unfair advantage in preparing a proposal for this project. **Comment**: this provision will not, for example, necessarily disqualify a proposer who performed some preliminary work from obtaining a final design Contract, especially when the results of such previous work are public data available to all other proposers. Rather, it attempts to avoid an "unfair advantage" when such information cannot be provided to other potential proposers. Definitions of "government data", "public data", "non-public data" and "private data" can be found in Minnesota Statutes Chapter 13.

- The proposer has, in previous work for the state, helped create the "ground rules" for this solicitation by performing work such as: writing this solicitation, or preparing evaluation criteria or evaluation guides for this solicitation.
- The proposer, or any of its principals, because of any current or planned business arrangement, investment interest, or ownership interest in any other business, may be unable to provide objective advice to the state.

DISCLOSURE OF POTENTIAL CONFLICT OF INTEREST

Having had the opportunity to review the Organizational Conflict of Interest Checklist, the proposer hereby indicates that it has, to the best of its knowledge and belief:

☐ Determined that no potential organizational conflict of interest exists.

☐ Determined a potential organizational conflict of interest as follows:

Describe nature of potential conflict
Describe measures proposed to mitigate the potential conflict

Signature _____ Date _____

If a potential conflict has been identified, please provide name and phone number for a contact person authorized to discuss this disclosure form with Mn/DOT contract personnel.

Name _____ Phone _____

STATE OF MINNESOTA
AFFIDAVIT OF NONCOLLUSION

I swear (or affirm) under the penalty of perjury:

1. That I am the Responder (if the Responder is an individual), a partner in the company (if the Responder is a partnership), or an officer or employee of the responding corporation having authority to sign on its behalf (if the Responder is a corporation);

2. That the attached proposal submitted in response to the _____ Statement of Work has been arrived at by the Responder independently and has been submitted without collusion with and without any agreement, understanding or planned common course of action with, any other Responder of materials, supplies, equipment or services described in the Request for Proposal, designed to limit fair and open competition;

3. That the contents of the proposal have not been communicated by the Responder or its employees or agents to any person not an employee or agent of the Responder and will not be communicated to any such persons prior to the official opening of the proposals; and

4. That I am fully informed regarding the accuracy of the statements made in this affidavit.

Responders' Firm Name: _____

Authorized Signature: _____

Date: _____

Subscribed and sworn to me this _____ (day) day of _____ (Month Year)

Notary Public _____

My commission expires: _____

State of Minnesota — Immigration Status Certification

By order of the Governor (Governor's Executive Order 08-01), vendors and subcontractors MUST certify compliance with the Immigration Reform and Control Act of 1986 (8 U.S.C. 1101 et seq.) and certify use of the *E-Verify* system established by the Department of Homeland Security.

E-Verify program information can be found at http://www.dhs.gov/ximgtn/programs.

If any response to a solicitation is or could be in excess of $50,000.00, vendors and subcontractors must certify compliance with items 1 and 2 below. In addition, prior to the delivery of the product or initiation of services, vendors MUST obtain this certification from all subcontractors who will participate in the performance of the Contract. All subcontractor certifications must be kept on file with the Contract vendor and made available to the state upon request.

1. The company shown below is in compliance with the Immigration Reform and Control Act of 1986 in relation to all employees performing work in the United States and does not knowingly employ persons in violation of the United States immigration laws. The company shown below will obtain this certification from all subcontractors who will participate in the performance of this Contract and maintain subcontractor certifications for inspection by the state if such inspection is requested; and
2. By the date of the delivery of the product and/or performance of services, the company shown below will have implemented or will be in the process of implementing the *E-Verify* program for all newly hired employees in the United States who will perform work on behalf of the State of Minnesota.

I certify that the company shown below is in compliance with items 1 and 2 above and that I am authorized to sign on its behalf.

Name of Company		Date:	
Authorized Signature		Telephone Number	
Printed Name:		Title:	

If the Contract vendor and/or the subcontractors are not in compliance with the Immigration Reform and Control Act, or knowingly employ persons in violation of the United States immigration laws, or have not begun or implemented the *E-Verify* program for all newly hired employees in support of the Contract, the state reserves the right to determine what action it may take. This action could include, but would not be limited to cancellation of the Contract, and/or suspending or debarring the Contract vendor from state purchasing.

For assistance with the *E-Verify* Program
Contact the National Customer Service Center (NCSC) at **1-800-375-5283** (TTY 1-800-767-1833).

For assistance with this form, contact:
Mail: 112 Administration Building, 50 Sherburne Avenue, St. Paul, Minnesota 55155
E-Mail: MMDHelp.Line@state.mn.us
Telephone: 651-296-2600
Persons with a hearing or speech disability may contact us by dialing 711 or 1-800-627-3529

SAMPLE WORK ORDER LANGUAGE

STATE OF MINNESOTA
IT Professional Services Master Contract Work Order

This work order is between the State of Minnesota, acting through its Commissioner of Transportation ("State") and [fill in name of contractor, be sure to indicate if corporation, partnership, limited liability company, sole proprietor, etc] ("Contractor"). This Work Order is issued under the authority of Master Contract T-Number 502TS, CFMS Number [fill in CFMS number from the contractor's master contract], and is subject to all provisions of the Master Contract which is incorporated by reference.

Recitals

1. Under Minn. Stat. § 15.061 [Insert additional statutory authorization if necessary] the State is authorized to engage such assistance as deemed necessary.
2. The State is in need of [Add brief narrative of the purpose of the contract].
3. The Contractor represents that it is duly qualified and agrees to perform all services described in this work order to the satisfaction of the State.

Work Order

1 Term of Work Order; Incorporation of Exhibits; Survival of Terms

1.1 Effective date. This Work Order will take effect on the date the State obtains all required signatures as required by Minn. Stat. § 16C.05, subd. 2.
The Contractor must not begin work under this work order until it is fully executed and the Contractor has been notified by the State's Authorized Representative to begin the work.

1.2 Expiration date. This Work Order will expire on [fill in date], or when all obligations have been satisfactorily fulfilled, whichever occurs first.

1.3 Exhibits. Exhibits [fill in, e.g. A – D] are attached and incorporated into this Work Order.

1.4 Survival of terms. All clauses which impose obligations continuing in their nature and which must survive in order to give effect to their meaning will survive the expiration or termination of this Work Order.

2 Contractor's Duties

The Contractor, who is not a state employee, will:

[Provide a <u>detailed</u> scope of services. The services must define specific duties, deliverables, and deliverable completion dates. Do not simply attach the same scope that was used in the "Statement of Work" (RFP) as a greater level of detail is needed in this work order. If using a separate attachment, use "Perform the duties specified in Exhibit A, "Scope of Services".]

3 Consideration and Payment

3.1 Consideration

The State will pay for all services performed by the Contractor under this work order as follows:

3.1.1 *Compensation.* The Contractor will be paid as follows:
[Provide a detailed explanation of how the Contractor will be paid, for example a fixed hourly rate, or a lump sum per deliverable, some examples may be:
an Hourly Rate of $_____up to maximum of ____hours, but not to exceed $_____.

a Lump Sum of $_____.]
[Rate: rates paid may not exceed the Contractor's rates specified in their Master Contract.]

3.1.2 *Travel Expenses*. Reimbursement for travel and subsistence expenses actually and necessarily incurred by Contractor, as a result of this Work Order, will be reimbursed for travel and subsistence expenses in the same manner and in no greater amount than provided in the current Minnesota Department of Transportation Travel Regulations. Contractor will not be reimbursed for travel and subsistence expenses incurred outside Minnesota unless it has received State's prior written approval for out of state travel. Minnesota will be considered the home state for determining whether travel is out of state. See Exhibit ____ for the current Minnesota Department of Transportation Reimbursement Rates for Travel Expenses.

3.1.3 *Total Obligation*. The total obligation of the State for all compensation and reimbursements to the Contractor under this Work Order will not exceed $ [fill in].

3.2 Payment

3.2.1 *Invoices*. State will promptly pay Contractor after Contractor presents an itemized invoice for the services actually performed and State's Authorized Representative accepts the invoiced services. Invoices must be submitted in the format prescribed in Exhibit ____ and according to the following schedule:

[INDICATE WHEN YOU WANT THE CONTRACTOR TO SUBMIT INVOICES, FOR EXAMPLE: "MONTHLY" OR "UPON COMPLETION OF SERVICES," OR IF THERE ARE SPECIFIC DELIVERABLES, LIST HOW MUCH WILL BE PAID FOR EACH DELIVERABLE. THE STATE DOES NOT PAY MERELY FOR THE PASSAGE OF TIME.]

3.2.1.1 Each invoice must contain the following information: Mn/DOT Contract Number, Mn/DOT Contract invoice number (sequentially numbered), billing address if different from business address, and Contractor's original signature attesting that the invoiced service and costs are new and that no previous charge for those services or goods has been included in any prior invoice.

3.2.1.2 Direct nonsalary costs allocable to the work under this Work Order must be itemized and supported with invoices or billing documents to show that such costs are properly allocable to the work. Direct nonsalary costs are any costs that are not the salaried costs directly related to the work of Contractor. Supporting documentation must be provided in a manner that corresponds to each direct cost.

3.2.1.3 The original of each invoice must be sent to State's Authorized Representative for review and payment. A copy of the invoice will be sent to State's Project Manager for review.

3.2.1.4 Contractor must provide, upon request of State's Authorized Representative, the following supporting documentation:

3.2.1.5 Direct salary costs of employees' time directly chargeable for the services performed under this Work Order. This must include a payroll cost breakdown identifying the name of the employee, classification, actual rate of pay, hours worked, and total payment for each invoice period; and

3.2.1.6 Signed time sheets or payroll cost breakdown for each employee listing dates and hours worked. Computer generated printouts of labor costs for the project must contain the project number, each employee's name, hourly rate, regular and overtime hours, and the dollar amount charged to the project for each pay period.

3.2.1.7 If Contractor is authorized by State to use or uses any subcontractors, Contractor must include all the above supporting documentation in any subcontractor's contract, and Contractor must make timely payments to its subcontractors. Contractor must require subcontractors' invoices to follow the same form and contain the same information as set forth above.

3.2.2 *Retainage*. Under Minnesota Statutes § 16C.08, subdivision 5(b), no more than 90% of the amount due under this Contract may be paid until State's agency head has reviewed the final product of this Contract. The balance due will be paid when State's agency head determines that Contractor has satisfactorily fulfilled all the terms of this Contract.

3.2.3 *Federal Funds*. If federal funds are used, Contractor is responsible for compliance with all federal requirements imposed on these funds and accepts full financial responsibility for any requirements imposed by Contractor's failure to comply with these federal requirements.

3.2.4 *Progress Reports*. Contractor will submit progress reports in a format and timeline designated by the State's Project Manager.

4 Indemnification

In the performance of this contract by Contractor, or Contractor's agents or employees, the Contractor must indemnify, save, and hold harmless the State, its agents, and employees, from any claims or causes of action, including attorney's fees incurred by the state, to the extent caused by Contractor's:

1) Intentional, willful, or negligent acts or omissions; or
2) Actions that give rise to strict liability; or
3) Breach of contract or warranty.

The indemnification obligations of this section do not apply in the event the claim or cause of action is the result of the State's sole negligence. This clause will not be construed to bar any legal remedies the Contractor may have for the State's failure to fulfill its obligation under this contract.

5 Foreign Outsourcing

The Contractor agrees that the disclosures and certifications made in its Location of Service Disclosure and Certification Form submitted with its proposal are true, accurate and incorporated into this work order contract by reference.

6 Authorized Representatives

6.1 State's Authorized Representative. State's Authorized Representative will be:
NAME, TITLE
ADDRESS
TELEPHONE NUMBER
FAX NUMBER
E-MAIL ADDRESS

State's Authorized Representative or his /her successor, will monitor Contractor's performance and has the authority to accept or reject the services provided under this Work Order.

6.2 State's Project Manager. State's Project Manager will be:
NAME, TITLE
ADDRESS
TELEPHONE NUMBER
FAX NUMBER
E-MAIL ADDRESS

State's Project Manager, or his/her successor, has the responsibility to monitor Contractor's performance and progress.
State's Project Manager will sign progress reports, review billing statements, make recommendations to State's Authorized Representative for acceptance of Contractor's good or services and make recommendations to State's Authorized Representative for certification for payment of each Invoice submitted for payment.

6.3 Contractor's Authorized Representative. Contractor's Authorized Representative will be:

NAME, TITLE
ADDRESS
TELEPHONE NUMBER
FAX NUMBER
E-MAIL ADDRESS

If Contractor's Authorized Representative changes at any time during this contract, Contractor must immediately notify State.

6.4 Contractor's Key Personnel. Contractor's Key Personnel will be:
(names, titles)

Key Personnel assigned to this project cannot be changed without the written approval of the State's Project Manager. Contractor will submit a change request in writing to the State's Project Manager along with a resume for each potential candidate. Potential new or additional personnel may be required to participate in an interview. Upon approval of new or additional personnel, the State's Authorized Representative may issue a change order to add or delete key personnel.

7 Time

The Contractor must comply with all the time requirements described in this Work Order. In the performance of this Work Order, time is of the essence.

8 Employee Status

Pursuant to the Governor's Executive Order 08-01, if this contract, including any extension options, is or could be in excess of $50,000, Contractor certifies that it and its subcontractors:

8.2 Comply with the Immigration Reform and Control Act of 1986 (U.S.C. 1101 et. seq.) in relation to all employees performing work in the United States and do not knowingly employ persons in violation of United States immigrations laws; and

8.3 By the date of the performance of services under this contract, Contractor and all its subcontractors have implemented or are in the process of implementing the E-Verify program for all newly hired employees in the United States who will perform work on behalf of the State of Minnesota.

Contractor must obtain certifications of compliance with this section from all subcontractors who will participate in the performance of this contract. Subcontractor certifications must be maintained by Contractor and made available to the state upon request. If Contractor or its subcontractors are not in compliance with 1 or 2 above or have not begun or implemented the E-Verify program for all newly hired employees performing work under the contract, the state reserves the right to determine what action it may take including but not limited to, canceling the contract and suspending or debarring the contractor from state purchasing.

9 Additional Provisions

[Use this space to add information not covered elsewhere in this Work Order. If not needed, delete this section or state "None". The following should be used in any Work Order that includes web design:

The Contractor will comply with the "Minnesota Office of Enterprise Technology: Web Design Guidelines" available at the URL: http://www.state.mn.us/portal/mn/jsp/content.do?programid=536911233&id=-536891917&agency=OETweb.

The balance of this page has been intentionally left blank.

Microsoft®
Online Services

Microsoft SharePoint Online Dedicated 2010 Build Guide

Published: July 2010

Pre-Release Documentation

Contents

1 Introduction

This document details the processes associated with configuring the individual components of Microsoft SharePoint Online 2010.

1.1 Purpose of this Document

This document is a variant of the build guide used by SharePoint Online Operations to build out the hosted SharePoint environment. This variant is missing information specific to the Microsoft Data Centers, does not include details for SQL mirroring or backup related tasks, makes references but does not include details for building a secondary farm for disaster recovery, and does not detail the pre-production environment. The intent in releasing this document is to provide customers of SharePoint Online Dedicated sufficient information for setting up and configuring a development or test environment to mimic the production environment. The goal, however, is not to provide sufficient detail to construct a complete mirror of the production environment. Customers interested in performance testing will find the details insufficient to ensure a complete match to the production environment but should find enough information to interpolate.

1.2 Audience

This document is intended for development/test resources directly employed or contracted by a Microsoft SharePoint Online Dedicated customer. This audience is involved in the setup, configuration, and management of a test/development environment. The following skill set is assumed:

- Ability to read and interpret server logs to determine causes of failure
- Ability to configure advanced Windows Server 2008 server settings
- Ability to configure advanced IIS 7 settings
- Ability to install SQL Server 2008 R2 and configure advanced settings

1.3 Microsoft Contact

Please contact your technical account manager (TAM) with any questions concerning this document.

2 Overview

At a high level the document is divided into the following build instruction sets:

- Validate Hardware provided
- Configure Host Machines
- Create VMs in Hyper-V on Host Machines
- Configure General VM settings
- Configure the SQ Role
- Configure the BK Role
- Configure FE and AP Roles
- Create and configure SharePoint Farm

This document contains steps to virtualize the environment and set up the various roles on virtual machines.

3 Prerequisites

3.1 Release Management

- Confirm that servers (host machines) are ready for build out
- Confirm VLANs have been added to Top of Rack (TOR) switch and ports are configured
- Customer provided build record details are captured

3.2 Accounts

The following accounts should be available in the managed domain:

Accounts from Managed Domain		
Account name	**Domain**	**Description**
ms-svc-sca	Managed	Central Administration and Farm account. This account must be able to logon locally to the AP-01 server to setup FIM for profile synchronization.
ms-svc-srh	Managed	Search Service default content access account.
ms-svc-sps	Managed	Content applications web pool account.
ms-svc-spa	Managed	Service applications web pool account.
ms-svc-sql	Managed	SQL Database service and SQL Agent account.
ms-svc-ptc	Managed	Sandbox Code Low Permissions Account.
ms-svc-sup	Managed	Super User Account Used for Publishing Object Cache.
ms-svc-rea	Managed	Super Reader Account Used for the Publishing Object Cache
Accounts from Customer Domain		
Deskless Workers	Customer	One or more AD groups or Role claims that represent all deskless workers at the customer.
Information Workers	Customer	One or more AD groups or Role claims that represent all IW users at the customer
Partners	Customer	One or more AD groups or Role claims that represent all partner users for a customer.
Unattended Account	Customer	An account name from the customer forest for unattended data connections for Excel/Visio.
BCS Profile Import	Customer	An account name from the customer forest for profile import using the BCS service application
On-Premise Search	Customer	An account for use in crawling on-premise data sources. One account for all content sources.
People Picker AD Account	Customer	Account with permissions to look up users/groups from AD for configuration of the people picker.
Profile Import Account	Customer	Account that has dir sync permissions to the customer AD forests. Link for more information about dir sync.
Accounts from Management Domain *		
Admin Group	Management	Farm administrators group

Admin Accounts	Management	Admin Accounts for individual farm administrators

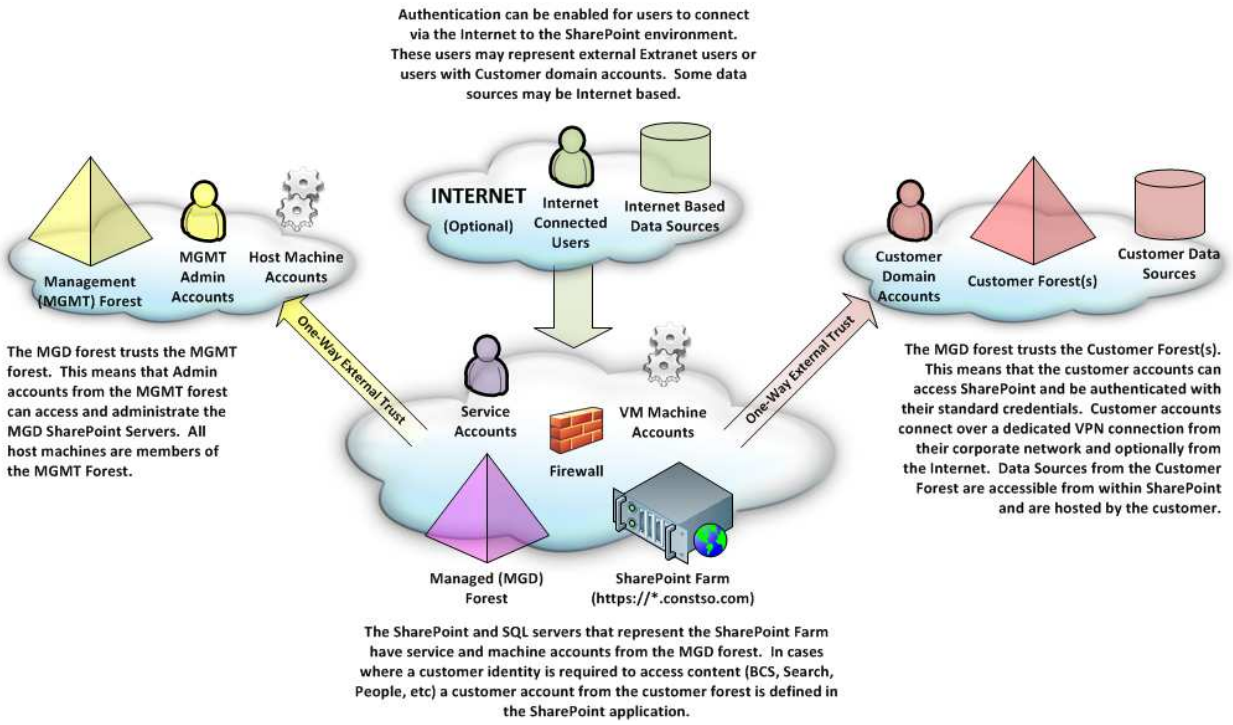
* If you build out a management domain as outlined in the following instructions, the following accounts are required to be in that domain. If you do not build out a management domain, place them in the managed domain.

4 The SharePoint Online Hosted Environment

4.1 MGD, MGMT, and Customer Forest

The Online environment is structured to manage the hosting of multiple customer environments each isolated to meet security and compliance requirements. The isolation begins with separate customer Virtual Local Area Networks (VLANs) and separate managed customer Active Directory Forests (managed Forest). The basic trust relationship and configuration is outlined in the diagram below. There are generally 3 Forests, one for Management (central forest for all Management Admin Accounts), one for Managed (the forest where SharePoint is hosted), and one forest provided by the customer (Customer Domain Accounts and Customer Data Sources).

Figure 1: Forest Diagram

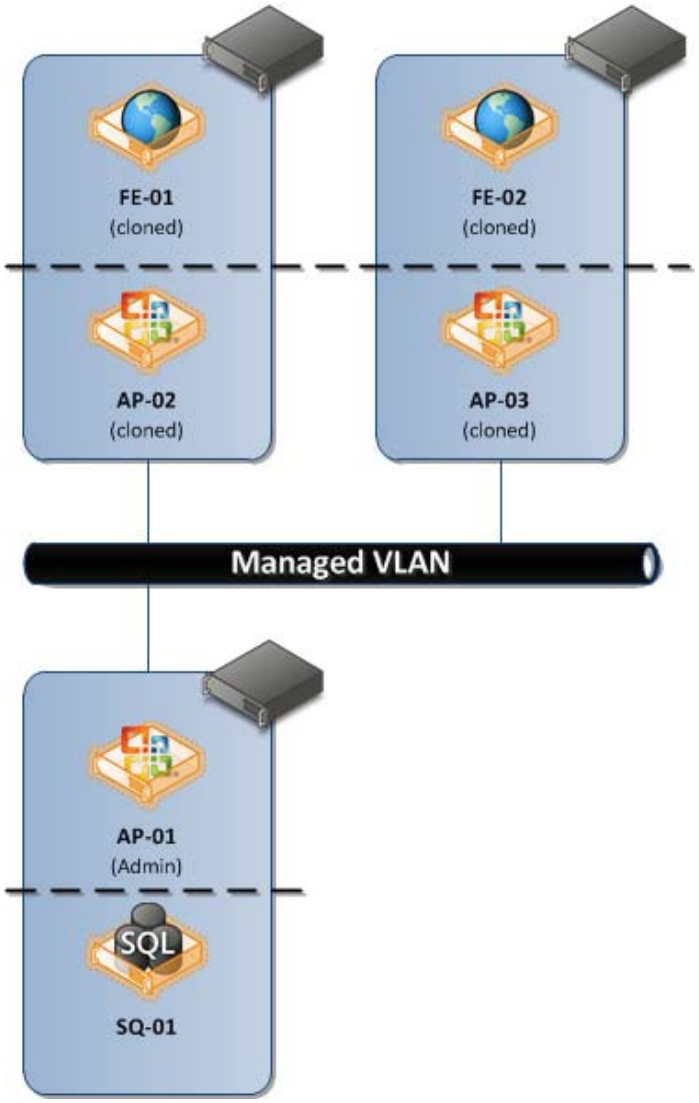


4.2 Service Distribution

This document will detail out how to setup the SharePoint Farm assuming the other components (VLANs, Forests, Forest Trusts, Accounts, Machine Accounts, SMTP Host etc.) already exist in your development/test environment. The document will also assume that the build out will involve both physical hosts and virtual machines (VMs). If you are not comfortable with virtual machines then you can build out the environment if you wish on physical hardware. It is also not necessary to build out the management forest; all admin accounts can be from the managed forest for test/development purposes. If you choose to not build out the MGMT forest, the host machines should also be members of the MGD forest. Build instructions will assume that the host machines and admin accounts are from the MGMT forest. This document will not detail out sizing information for the number of VMs assigned

to a given customer, this varies from customer to customer, but for testing and development purposes the Service distribution can be structured similar to the following diagram. Note normally we configure the backup VM as a witness server for a SQL mirror pair but to simplify the build guide, will skip the configuration of the backup file share (not shown in diagram) and the second SQL server:

Figure 2: Farm Distribution for Illustration Purposes



The diagram above has been simplified but represents the tiered approach used within the primary and secondary data centers.

- **Tier 1 (Front Ends):** The FE tier is responsible for Web traffic activities. All FE machines are cloned and identically configured.
- **Tier 2 (Application Load Balanced):** The first of the app tiers is used to host load balanced redundant services. These AP boxes are all identical in size and configuration.

- **Tier 3 (Application Single Instance):** The second of the app tiers shares the backend SKU with the SQL machines. These app tiers contain either the single instance non-load balanced services like central admin and profile or search which requires more space than can be provided on the App SKU.
- **Tier 4 (Data – Storage, Backup, and Reporting):** The fourth tier is the data tier, compromised of the SQL or Backup roles.

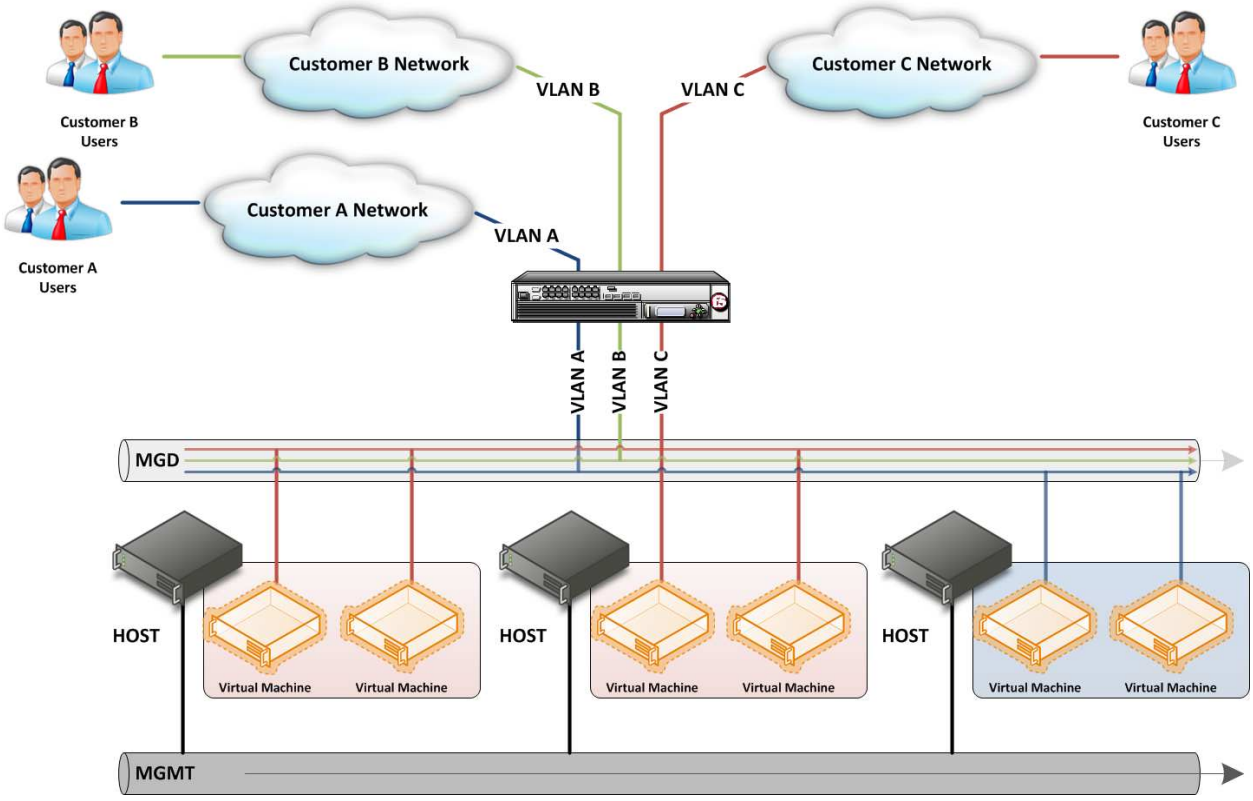
The following diagram details what SharePoint services or server roles are running on what tier.

Figure 3: Service Distribution for Illustration Purposes

4.3 Trunk Network Design

Within the production environment, we use trunk porting for our network design when connecting Virtual Machines (VMs) to the managed VLAN. When developing a test/development environment this is not a necessary step; you can bind the TRUNK NIC to a VLAN that represents the managed network. This will result in a few changes to the network card configuration for the host machine. The TRUNK NIC in this situation should be configured exactly the same as the MGMT NIC but the IP from should from the managed VLAN. The following diagram details the fundamentals of the production environment, when building for a test/development environment you can simplify this to a single Customer Network with a single VLAN for all VMs.

Figure 4: Trunk Network Diagram

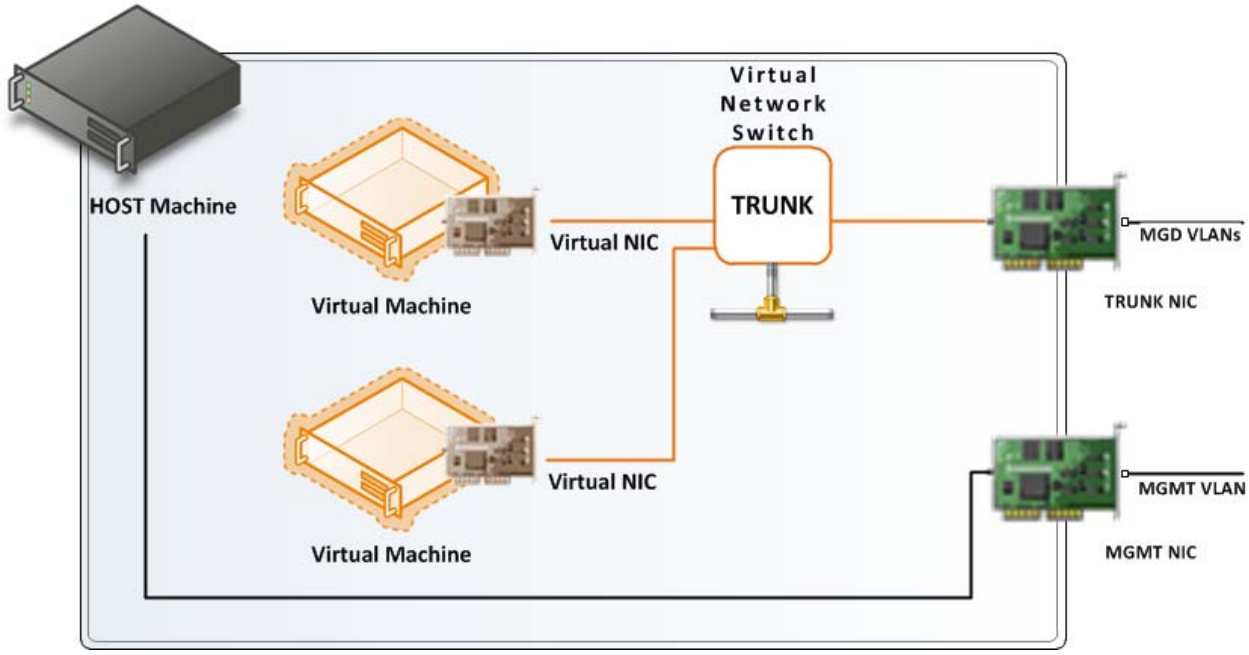


Note: the same load balancer is used for all customer VLANs in managed in production. Only the VMs have network adapters connected to the managed VLAN, the Host server is only connnected to the MGMT network.

4.4 Virtual/Physical Network Interface Cards

Each physical machine has two Network Interface Cards (NICs) that are each connected to different VLANs. One is connected to the Management (MGMT) VLAN with the host machine a member of the MGMT Active Directory Forest. The second is connected to the TRUNK NIC which is connected to the managed VLAN. When using Trunk Porting there is no IP address assigned to the physical NIC on the host machine but when we create a virtual network within Hyper-V we will associate the VM to a VLAN ID for the appropriate customer. This is illustrated below:

Figure 5: Virtual/Physical NICs



4.5 Basic Characteristics about the Host and Virtual Machines

All hardware/configuration assumes 64-bit configured hardware running Windows 2008 R2 64-bit and SQL 2008 R2 64-bit. Some software detailed like Forefront for SharePoint may not be available at this time in a trial version and can skipped for development/test purposes (will influence performance test results). If you do not have a license for Microsoft SQL 2008 R2, it is fine for test purposes for the September 2010 release, Microsoft SQL 2008 will be fine.

Rather than detailing a specific configuration, SKU, or vendor for hardware, what follows are the basic specs of the host machines currently used in production:

Host SKU	Storage (Hard Drives)	RAM	CPU	NIC	Notes
WFE/App Host	8 HDD Direct Attached	24 GB	2 x Quad Core	Dual Port Gig-E	Used for most app roles and all web front end VMs
Back End Host	25 HDD Direct Attached and 10 HDD with attached shelf; 35 HDD Total	48 GB	2 x Quad Core	Dual Port Gig-E	Host SQL VMs and Search App VMs

The basic characteristics of the VMs are as follows, note for test/development purposes you can size the VMs as you have the capacity to host them. Within the build instructions, any notes of specific size like VHDs of 2 TB should be sized appropriately to meet capacity limits on the test/development hardware.

VM	Storage/VHDs	RAM	CPU	NIC	Host
FE/AP	• OS	10 GB	4 Cores	1 Virtual	WFE/App Host

VM	Storage/VHDs	RAM	CPU	NIC	Host
AP (Search)	• OS	10 GB	4 Cores	1 Virtual	Back End Host
SQ	• OS • DATA1 • DATA2 • DATA3 • LOGS	32 GB	4 Cores	1 Virtual	Back End Host

Ensure you leave memory, storage, and CPU cycles for the host machine if virtualizing when sizing the VMs to available hardware. Though not detailed in the build instructions, Microsoft Online Services uses Microsoft Systems Center Virtual Machine Manager (SCVMM) to manage the host and virtual machines. These build instructions have been scrubbed of any references to SCVMM specific requirements to reduce software dependencies for customer dev/test environments.

4.6 Best Practices for Configuring a Test/Development Environment

When you configure a test/development environment there are a few core elements that must be replicated to adequately test any custom code built or tested by the customer:

1. All host URLs must use SSL certificates and be fully qualified i.e. https://team.contoso.com. Failure to do so will mask potential problems in how the browser will treat the site with respect to zones and protocols. This is especially important for connectivity with internal Line of Business systems and data sources.
2. All customer accounts must come from a forest that has a one-way external trust between managed and the customer forest. Failure to do so may mask authentication/impersonation issues when connecting to Line-Of-Business applications or data sources within the customer forest. Note: Kerberos authentication is not supported; it doesn't work across Forest boundaries.
3. Use a minimum of two Web Front End (FE) role machines to ensure that any and all custom code properly deploys across multiple machines in a farm.
4. Use static IP addresses if at all possible. If you use dynamic IP addresses, there is a good chance over time that the farm will have problems, especially with any load balancing solution you use.
5. This document does not detail a load-balancing solution. We use a hardware load balancing solution in our production and pre-production environments, for test/development purposes Windows Network Load Balancing (WNLB) should be adequate. There will be differences in performance that is unavoidable when contrasting hardware vs. software based load balancing solutions.

5 Configuring Hosts

5.1 Creating LocalAdmin account on Host Machine

We create a LocalAdmin account because it is used to log into a machine if a domain controller is not available.

1. Create a new local admin account called **LocalAdmin**, and provide the standard password from the password spreadsheet. Configure the account to never expire. Note: Microsoft SharePoint Online recommends that you setup a different password for each machine.
2. Add the account to the local administrators group.

5.2 Configuring disk layout on the host machine

1. Launch any Array Configuration Software installed for setting up RAID configuration of your disks.
2. As storage permits, configure your disk as follows.

Host	Array	Drives	Purpose	RAID	Notes
Application Host (HA)	1	C:\	Host OS	RAID 1	Simple; Entire Volume
	2	E:\	VHDs	RAID 0 + 1 (6 drives)	Simple; All remaining disks
Back End Host (HB)	1	C:\	Host OS	RAID 1	Simple; Entire Volume
	2	E:\	Data VHDs	RAID 5 (23 drives)	Simple; GPT Partition Table
	3	F:\	OS and Log VHDs	RAID 5 (10 drives)	Simple; GPT Partition Table

5.3 Setting end point antivirus exceptions on your host machines

Configure your desktop anti-virus of choice installed on the server to scan only incoming files and exclude drives E and F on the host machines as appropriate. The end point anti-virus software should only be scanning the host machine's C drive.

5.4 Configuring page files

Page files will be configured to by system managed for all host machines.

1. Navigate to **Start | Control Panel | System | Advanced system settings**.
2. Click the **Advanced** tab**| Performance | Settings**.
3. Click the **Advanced** tab **| Virtual memory | Change**.
4. Choose drive C:\ in the **Drive** list and select the **System managed size** option, and click **Set**.

5.5 Checking for Windows updates

1. Ensure that all the Windows updates have been applied to the machine.

5.6 Disabling Recycle Bin

1. Right click the **Recycle Bin** icon on desktop and choose **Properties**.
2. For each drive choose **Don't move files to the Recycle Bin**.

5.7 Disabling IE ESC

1. Navigate to **Start | Control Panel | Administrative Tools | Server Manager**.
2. Click Security Information | Configure IE ESC link
3. Turn off for both Administrators and Users.

5.8 Disabling User Account Control (Done per User)

1. Navigate to **Start | Control Panel | User Accounts | Change User Account Control Settings** link
2. Open **Control Panel**, click **User Accounts**, and then click **User Accounts**.
3. Change to **Never Notify**.

5.9 Configuring Network Connections

1. Open **Network Connections**.
2. Ensure that there are two connections named MGMT and Trunk and that both are enabled.
3. For the Trunk connection (if using trunk porting), clear all check boxes and ensure the configuration is **Connected: None (No IP Address)**. If not using trunk porting, select all check boxes except **Internet Protocol Version 6 (TCP/IP v6)**, and ensure that the configuration is **Connected: <<MGD forest>>**
4. For the MGMT connection, select all the options except **Internet Protocol Version 6 (TCP/IP v6)**, and ensure that the configuration is **Connected: <<MGMT forest>>**
5. Note which adapter (Name of NIC not connection) corresponds to **TRUNK**.
6. With the **Network Connections** window selected choose < **ALT key > | Advanced| Advanced Settings**. Ensure the **MGMT** connection is at the top of the list above **TRUNK**.
7. Navigate to **Start | Control Panel | Administrative Tools | Server Manager | Roles**.
8. Add the **Hyper-V** role and restart the machine.
9. Open **Server Manager**.
10. Navigate to **Start | Control Panel | Administrative Tools | Hyper-V Manager** and select the host name.
11. From the **Actions Pane | Virtual Network Manager|** choose **Trunk**
12. Set the Name to **TRUNK.**
13. Set the connection type to **External** and select the Trunk adapter from 5. Ensure **Allow management operating system to use this network adapter** is unchecked.

Repeat this configuration for each Host Machine.

6 Creating Virtual Machines

In this section, you will create and configure virtual machines. There is no recommended order in terms of the creation and the configuration of the machines: you may create all the machines first and then configure them one by one or complete the creation and configuration of each individual machine at once. Note: all machines should be created before SharePoint is installed.

VMs should be built out with the following distribution of services and VMs across host machines:

Figure 6: Service Distribution for Illustration Purposes

The VMs have the following HD configuration:

VM Role	Drive Configuration	Notes
SP WFE and Host	1 VHD - C Drive	The VHD is larger for the Search role than other WFE/App roles. Size this based on the amount of crawling you plan to do. The storage needs to account for the index size for both crawl and query needs.
SQL VM	5 VHDs - C, E, F	The C drive (1 VHD) includes program files and windows. The E drive (3 VHDs) is used for SQL DB Storage (Should be twice the size of the log drive) The F drive (1 VHD) is used for SQL Log Storage Plan your SQL storage based on the size of the test/development databases. We recommend and our build documents assume a SCSI controller for the VM and adding 2 fixed SCSI VHDs for the E and F Drives.

For SQ, create new disks in the available SCSI Channel.

VM name	Category	Type	Size	File name
SQ	Data	Dynamic	xxxx GB	SPSQ*XX*_disk_1
SQ	Data	Dynamic	xxxx GB	SPSQ*XX*_disk_2
SQ	Data	Dynamic	xxxx GB	SPSQ*XX*_disk_3
SQ	Logs	Dynamic	xxxx GB	SPSQ*XX*_disk_4

6.1 Creating VMs in Hyper-V

1. On the local Host machines, use Hyper-V to create a new VM. VM configuration files and the C drive VHD should be created on the host machine's E Drive for the App SKU and the F drive for the Back End SKU. For the SQL VMs, place the data VHDs on the host machine's E drive and the log VHDs on the F drive.
2. VMs should be built with Windows 2008 R2 (Standard or Enterprise).
3. All VMs should have a single NIC connected to the virtual network (physical NIC is connected to the trunk network adapter). If using trunk porting set the VLAN ID in the network adapter settings for the VM within Hyper-V. If not using trunk porting then there should be nothing additional to configure for the virtual network adapter.
4. As noted above, this guide assumes 2 VMs per host. Your distribution may vary depending on the resources available to you.

7 Configuring Virtual Machines (Common Steps)

7.1 Changing the network settings

1. Navigate to **Start | Control Panel | Network and Sharing Center | Change adapter settings** link
2. Right-click the **Local Area Connection** network adapter.
3. Uncheck **Internet Protocol Version 6 (TCP/IPv4).**
4. Select **Internet Protocol Version 4 (TCP/IPv4) | Properties**.
5. Specify the **IP address**, **subnet mask**, **default gateway**, and the preferred and alternate **DNS servers** per the IP Excel Worksheet referenced in the To Build record.

7.2 Verifying the connectivity for default gateway (If using Trunk)

Now that we've assigned an IP address to the VM, we can test that the VLAN settings for the Trunk Adapter and Trunk Network are correct. If not using Trunk ports, you can skip this step.

1. Open the command prompt, and ping the default gateway.
2. Verify that you get a reply. If you don't get a reply, check the network settings and confirm a VLAN was assigned to the VM prior in the previous step.

7.3 Configuring page files

Page files will be configured to by system managed for all host machines.

1. Navigate to **Start | Control Panel | System | Advanced system settings**.
2. Click the **Advanced** tab**| Performance | Settings**.
3. Click the **Advanced** tab **| Virtual memory | Change**.
4. Choose drive C:\ in the **Drive** list and select the **System managed size** option, and click **Set**.

7.4 Checking for Windows updates

1. Ensure that all the Windows updates have been applied to the machine.

7.5 Disabling Recycle Bin

1. Right click the **Recycle Bin** icon on desktop and choose **Properties**.
2. For each drive choose **Don't move files to the Recycle Bin**.

7.6 Disabling IE ESC

1. Navigate to **Start | Control Panel | Administrative Tools | Server Manager**.
2. Click Security Information | Configure IE ESC link
3. Turn off for both Administrators and Users.

7.7 Disabling User Account Control (Done per User)

1. Navigate to **Start | Control Panel | User Accounts | Change User Account Control Settings** link
2. Open **Control Panel**, click **User Accounts**, and then click **User Accounts**.
3. Change to **Never Notify**.

7.8 Disabling loopbackcheck

1. Navigate to **Start | Search Dialog Box |** type regedit | click **regedit.exe**
2. Navigate to: **HKLM\SYSTEM\CurrentControlSet\Control\Lsa**

3. Right-click **Lsa** |**New DWORD Value** called DisableLoopbackCheck
4. Right-click **DisableLoopbackCheck | Modify** | **Value data = 1**
5. Restart the VM.

7.9 Setting end point antivirus exceptions on your host machines

Configure your desktop anti-virus of choice installed on the VM to scan specific directories. For simplicity, setup the same rules for all virtualized servers:

- C:\Program Files\Microsoft Office Server
- C:\inetpub
- C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions
- C:\ProgramData\Microsoft\SharePoint
- C:\windows\Microsoft.Net
- C:\windows\temp
- C:\Program Files\Microsoft SQL Server
- E:\
- F:\

7.10 Adding the VM to the domain

1. Navigate to **Start | Control Panel | System | change settings** link |**Change**
2. Provide <customer managed domain>
3. Restart the VM..

7.11 Adding service accounts to local admin group

1. Navigate to **Start | Control Panel | Administrative Tools | Server Manager | Configuration | Local Users and Groups | Groups | Administrators**
2. For FE/AP Servers
    a. Add **managed\ms-svc-sca**
    b. Add **managed\ms-svc-sps**
    c. Add **mgmt\Admin Group** (the admin group you defined for Farm Admins)
3. For SQ Servers
    a. Add **managed\ms-svc-sca**
    b. Add **managed\ms-svc-sql**
    c. Add **mgmt\Admin Group** (the admin group you defined for Farm Admins)

8 Configuring SQ VM Settings

REMOTE-DESKTOP INTO THE SQL VIRTUAL MACHINE.

8.1 Configuring inbound firewall rules

1. Navigate to **Start | Control Panel | Administrative Tools | Windows Firewall with Advanced Security | Inbound Rules**
2. Create a new rule
    a. **Inbound rule | Port | TCP | 1433 | Allow the Connection| Domain | SQL Server 1433**

The appendix has more information about all firewall rules.

8.2 Configure disk layout for SQL

The VHDs were created previously but we need to span and format the volumes

1. Navigate to **Start | Control Panel | Administrative Tools | Server Manager |Storage | Disk Management | (C:)**
2. Right click on all disks and set to **Online**.
3. Create a spanned volume for Data drive
    a. Right click **Disk 1** | **Initialize disk** | select all available disks
    b. Ensure format used is **MBR**
    c. Right click **Disk 1 | New Spanned Volume |** select all data drives | Assign Drive Letter **E |** Clear **New Volume Name**
4. Create and format Log Drive
    a. Right click **Disk 4 |** click **new Simple Volume |** Assign Drive Letter **F |** Clear **New Volume Name**
5. Restart VM

8.3 Installing SQL Server

1. Browse to your SQL installation path (we recommend an ISO image mounted to the VM) and double-click **setup.exe**.
2. Navigate to **Installation** section and select **New Installation or add features to an existing installation.**
3. Use your product key or specify a trial.
4. On the Setup Support Rules page, if the status of all rules appears as **Passed**, click **Next**.
5. On **License Terms** select **I accept the license terms** and clear **Send features usage…** checkboxes.
6. Complete Setup Support Files step.
7. On **Setup Role** choose SQL Server Feature Installation
8. On Feature Selection select the following components:
    - Database Engine Services
    - SQL Server Replication
    - Client Tools Connectivity

- Client Tools Backwards Compatibility
- Management Tools - Basic
- Management Tools – Complete

9. On the **Server Configuration** page set **SQL Server Agent** startup type to **Automatic** then press **Use the same account for all SQL services** and type in **managed\ms-svc-sql** and its password.
10. On the **Database Engine Configuration** page on **Account Provisioning** tab add the following:
    - managed\ms-svc-sca
    - managed\ms-svc-sql
    - mgmt\Admins Group
11. On the **Database Engine Configuration** page navigate to **Data Directories** tab and set/confirm the following settings:
12.

Data root directory	E:\Program Files\Microsoft SQL Server\
User database directory	E:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA
User Database log directory	F:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA
Temp DB directory	E:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Data
Temp DB log directory	F:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Data

13. On **Error Reporting** page clear **Send Windows and SQL Server Error Reports…**
14. Complete installation with default settings on the rest of the pages.

8.4 SQL server configuration

8.4.1 Security

1. Navigate to **Start | All Programs | Microsoft SQL Server 2008 R2 | Configuration Tools | SQL Server Configuration Manager** | **SQL Server Network Configuration**
2. Right-click **Protocols for MSSQLSERVER | Properties |** set **Hide Instance** to **Yes**

8.4.2 Allow Lock Pages in Memory (Set by GPO)

Give SQL server process account rights to lock pages in memory.

1. Navigate to **Start | Control Panel | Administrative Tools | Local Security Policy**.
2. Expand **Local Computer Policy | Computer Configuration | Windows Settings | Security Settings | Local Policies**
3. Select **User Rights Assignment** | double-click **"lock pages in memory"** policy **| add user to group**
4. Enter the SQL Server service account in the form domain\user

8.4.3 Modify Temp DB

Execute to following script to create additional Temp DB files, one for each core. You may need to change temp db sizes based on available storage.

settempdb.sql

```
ALTER DATABASE tempdb MODIFY FILE (NAME = 'TempLog',FileGrowth = 0, FILENAME =
'F:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Data\TempLog.ldf')

ALTER DATABASE tempdb MODIFY FILE (NAME = 'TempDev',FileGrowth = 0, FILENAME =
'E:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Data\TempDev.mdf')

ALTER DATABASE tempdb MODIFY FILE (NAME = 'TempLog',FileGrowth = 0, Size= 130947000 KB
)

ALTER DATABASE tempdb MODIFY FILE (NAME = 'TempDev',FileGrowth = 0, Size= 98210250 KB
)

ALTER DATABASE tempdb ADD FILE (NAME = 'TempDev2',FileGrowth = 0, Size= 98210250
KB,FILENAME = 'E:\Program Files\Microsoft SQL
Server\MSSQL10_50.MSSQLSERVER\MSSQL\Data\TempDev2.ndf')

ALTER DATABASE tempdb ADD FILE (NAME = 'TempDev3',FileGrowth = 0, Size= 98210250
KB,FILENAME = 'E:\Program Files\Microsoft SQL
Server\MSSQL10_50.MSSQLSERVER\MSSQL\Data\TempDev3.ndf')

ALTER DATABASE tempdb ADD FILE (NAME = 'TempDev4',FileGrowth = 0, Size= 98210250
KB,FILENAME = 'E:\Program Files\Microsoft SQL
Server\MSSQL10_50.MSSQLSERVER\MSSQL\Data\TempDev4.ndf')
```

8.4.4 Setting the max degree of parallelism Option

Set the max degree of parallelism option to 1.

```
sp_configure 'show advanced options', 1;
GO
RECONFIGURE WITH OVERRIDE;
GO
sp_configure 'max degree of parallelism', 1;
GO
RECONFIGURE WITH OVERRIDE;
GO
```

8.5 Service startup states

1. Run services.msc.
2. Ensure the following service startup states:

Service	State
SQL Server Agent and SQL Server Database Engine	Automatic
SQL Server Browser	Disabled

9 Configuring SharePoint Web Front End and App Server VMs (Common Steps)

REMOTE-DESKTOP INTO THE FRONT END OR APP VIRTUAL MACHINE.

NOTE: THE SHAREPOINT SERVER MUST HAVE OUTBOUND INTERNET CONNECTIVITY. IF THE PREREQUISITE INSTALLER FAILS, CONFIRM THE SERVERS CAN CONNECT TO THE INTERNET.

9.1 Configuring inbound firewall rules

1. Navigate to **Start | Control Panel | Administrative Tools | Windows Firewall with Advanced Security | Inbound Rules**
2. Create a new rule
   a. **Inbound rule | Port | TCP | 443 | Allow the Connection| Domain | SharePoint 433**
   b. **Inbound rule | Port | TCP | 8888| Allow the Connection| Domain | Central Admin 8888**
   c. **Inbound rule | Port | TCP | 32843| Allow the Connection| Domain | SharePoint 32843**
   d. **Inbound rule | Port | TCP | 32844| Allow the Connection| Domain | SharePoint 32844**
   e. **Inbound rule | Port | TCP | 32844| Allow the Connection| Domain | SharePoint 32844**
3. The appendix has more information about all firewall rules.

9.2 Installing the SharePoint prerequisites

- With **Windows Explorer** | browse to **prerequisitesinstaller.exe**

9.3 Installing ADO.NET Data Services v1.5 CTP2

To enable REST services in SharePoint we must install the ADO.Net Data Services. This is not installed as a part of the prerequisites.

- Install ADO.NET Data Services v1.5 CTP2 by clicking http://go.microsoft.com/fwlink/?LinkId=158354.

9.4 Deleting the default IIS sites and application pools

1. Navigate to **Start | Control Panel | Administrative Tools |Internet Information Services (IIS) Manager**
2. Delete all default IIS sites and application pools

9.5 Configure IIS Logging

1. Navigate to **Start | Control Panel | Administrative Tools |Internet Information Services (IIS) Manager**
2. Select the **Machine Name** from left pane **| Logging**
   a. One log file per: **Server**

   b. Format: **W3C**
   c. Select fields: **check all fields**
3. Open **Windows Explorer | c:\inetpub\logs** | right click on **LogFiles** folder **| Properties | Advanced |** check **Compress contents to save disk space**
4. Run **IISReset**.

9.6 Configure IIS Logs maintenance job

Copy the following scripts to FE servers and schedule **logsdel.cmd** to run daily with **task scheduler**

logsdel.cmd

```
powershell -command "& 'logsdel.ps1' "
```

logsdel.ps1

```
$lgs = Get-ChildItem C:\inetpub\logs\LogFiles -recurse
foreach($f in $lgs)
    {
        $d = ((Get-Date) - $f.CreationTime).Days
        if ($d -gt 60 -and $f.PsISContainer -ne $True)
            {$f.Delete()}
    }
```

9.7 Installing the SharePoint Server

1. Browse to your SharePoint installation path (we recommend an ISO image mounted to the VM), and click **setup.exe**.
2. Type your product key.
3. Choose a **Server Farm** installation.
4. Don't launch PSConfig.exe yet.

9.8 Installing Microsoft Office Web Apps (If purchased)

1. Browse to your Office Web Apps installation path (we recommend an ISO image mounted to the VM) and click **setup.exe**.
2. Type your product key.
3. Don't launch PSConfig.exe yet.

9.9 Installing language packs

1. Browse to the path that contains the language packs, and install the language packs.
2. Select the **I accept the license terms** check box, and then click **Continue**.
3. Follow the instructions in the wizard to install the language packs.

9.10 Managing Certificates

We recommend an actual SSL certificate issued either by a corporate domain certificate authority or a third party authority. You can run into problems if you choose to use a self-signed certificate and will need to export the private key to install a self-signed certificate on other machines.

9.10.1 SSL Binding for First Machine

9.10.1.1 Requesting certificates (For first machine)

The following process is required to generate a request that can be submitted to a certificate authority (CA) to issue the SSL certificate. Use AP-01.

1. Navigate to **Start | Control Panel | Administrative Tools |Internet Information Services (IIS) Manager**
2. Select the **Machine Name** from left pane **| Server Certificates | Create certificate request**

   Using values from the to-build record:

   a. Common Name: ***.<customerdomain>.com**
   b. Organization: **<Customer Name>**
   c. Organization Unit: **<Customer OU>**
   d. City: **<Customer City>**
   e. State: **<Customer State>**
   f. Country: **<Customer Country>**
   g. Cryptographic service provider: **Microsoft RSA SChannel Cryptographic Provider**
   h. Bit length: **1024**
   i. File Name: Navigate to **My Documents** folder and create file called **<customer name> SSL certificate request.txt**
3. The request should now be submitted to the CA that is issuing the SSL certificate.

9.10.1.2 Completing Certificate Request

When a response is returned by the CA, perform the following steps on the same machine used to request the certificate. This should be AP-01.

1. Navigate to **Start | Control Panel | Administrative Tools |Internet Information Services (IIS) Manager**
2. Select the **Machine Name** from left pane **| Server Certificates | Complete certificate request**
   a. File Name: **provide path to the file that contains response from certificate authority**
   b. Friendly Name: **<customer name> Wildcard SSL certificate**

9.10.1.3 Exporting certificates for use on other machines (For First Machine)

Now that we have a complete SSL certificate, the next step is to export the certificate so we can install on all other FE machines. Use default values if not otherwise specified.

1. Launch mmc.exe; **Start | Run | mmc.exe**
2. Click **File | Add/Remove snap-in | Certificates | Computer Account | Local Computer**
3. **Certificates (Local Computer) | Personal | Certificates**
4. Right-click the SSL Certificate **| All Tasks | Export**
   a. Export Private Key: **Yes, export the private key**
   b. Format: **Personal Information Exchange #12 (.pfx)**
      i. Select **Include all certificates in the certification path if possible**
      ii. Select **Export all extended properties**
   c. Specify a strong password
   d. Navigate to **My Documents** folder and create file called **<customer name> SSL certificate request.pfx**

9.10.2 Import Certificates (Other SharePoint VMs)

Copy the certificate request from the previous step to all SharePoint VMs.

1. Navigate to **Start | Control Panel | Administrative Tools |Internet Information Services (IIS) Manager**
2. Select the **Machine Name** from left pane **| Server Certificates | Import**
    a. File Name: **provide path to the file for the exported pfx certificate**
    b. Password: **provide password from previous step**

9.11 Updating the host file (for AP servers)

1. Browse to **C:\windows\system 32\drivers\etc**, and then open the hosts file as an administrator.
2. Add the IP address and the names of the hostnames on the farm you will be creating based on the following pattern (adding an entry for team, my, etc.) as per the to-build record:

    Internal Virtual IP (VIP) Address <TAB> *Host name of application URL*

    131.107.40.230 <TAB> my.contoso.com

    131.107.40.230 <TAB> team.contoso.com

    131.107.40.230 <TAB> portal.contoso.com

9.12 Updating the host file (for FE servers)

1. Browse to **C:\windows\system 32\drivers\etc**, and then open the hosts file as an administrator.
2. Add the internal loopback IP address and the names of the Web application URL on the farm you will be creating based on the following pattern as per the to-build record:

    127.0.0.1 <TAB> *Web application URL*

    127.0.0.1 <TAB> my.contoso.com

    127.0.0.1<TAB> team.contoso.com

    127.0.0.1<TAB> portal.contoso.com

10 Building the SharePoint Online 2010 farm

REMOTE-DESKTOP INTO THE MACHINE THAT WILL CONTAIN CENTRAL ADMIN (AP-01).

10.1 Creating databases and launching the SharePoint Configuration wizard

We are running PSConfig via the cmd line to control how the tool is run. We will use a common passphrase on all servers of **PassPhrase** (feel free to use a passphrase of your own choosing). Use default values unless otherwise specified.

1. Within a **cmd window |** cd *to* **C:\Program files\Common files\Microsoft shared\Web Server Extensions\14\BIN\ |** Execute the following:

```
psconfig –cmd configdb –create –server < SQL Machine Name > -database
SharePoint_Config –user managed\ms-svc-sca -password <ms-svc-sca password> –
passphrase PassPhrase–admincontentdatabase SharePoint_CA_Content
```

2. Wait until step 1 is completed.
3. Navigate to **Start | All Programs | Microsoft SharePoint 2010 Products | SharePoint 2010 Products Configuration Wizard**.

REMOTE-DESKTOP INTO THE MACHINE THAT CONTAINS THE CENTRAL ADMIN.

4. Select the **Specify port number | 8888**

10.2 Generic step for joining servers to the farm (Other than VM running CA)

Now that you've created the farm with the central admin server, you must add all other machines to the farm via the PSConfig wizard. After you set up the SharePoint Configuration wizard on all FE and AP VMs, these VMs will be listed in the Central Admin site.

1. Navigate to **Start | All Programs | Microsoft SharePoint 2010 Products | SharePoint 2010 Products Configuration Wizard**.
2. Select the **Connect to an existing server farm** option.
3. Specify the SQ-01 server.
4. Use passphrase **PassPhrase.**

10.3 Registering managed accounts

Under **Central Administration**, click **Security**, click **Register Managed Account**.

Ensure that the following accounts are listed. If they are not, register them.

- managed/ms-svc-sca

- managed/ms-svc-sps
- managed/ms-svc-spa

10.4 Order we shall follow to configure services

The following instructions are organized to get the farm up and running as fast as possible. It is recommended you follow them in the order laid out so nothing is missed.

10.5 Generic steps for configuring services using the Central Admin Web site

1. Under **Central Administration | System Settings | Servers | Manage services on server**
2. A drop down at the top of the list allows you to switch from server to server, so all servers previously added to the farm can be configured from AP-01.
3. Start the service machine by machine as noted in the table below:

Following is a table describing the distribution of the services based on roles. It assumes AP-01 for Central Admin App Role (CA) and for Search App Server.

Server	Secondary
FE	Foundation Web Application
	Foundation Sandboxed Code Service
AP (generic)	Access database Service
	Application Registry Service
	Business Data Connectivity Service
	Excel Calculation Services
	Managed Metadata Web Service
	Foundation Workflow Timer Service
	PowerPoint Service
	Secure Store Service
	Visio Graphics Service
	Word Automation Services
	Word Viewing Service
AP (CA)	Central Administration
	Foundation Web Application
	Foundation Workflow Timer Service
	User Profile Service
	User Profile Synchronization Service**
	SharePoint Server Search
	Search Query and Site Settings Service
	Foundation Search*

* These services require certain prerequisites before they can be started.

** Do not start the User Profile Synchronization Service right now; you'll be notified further in the document when to start the service.

10.6 Creating quota templates

We need to create the quota templates before we create the web applications.

1. Under **Central Administration | Application Management | Site Collections | Specify quota templates**
   Create five new quota templates using the **[new blank template]** as per the table below:

Name	Limit site storage to a maximum of:	Send warning E-mail when Site Collection storage reaches:	Limit maximum usage per day to:	Send warning e-mail when usage per day reaches :
< *Customer Name* > 2 GB	2000 MB	1800 MB	300 pt	250 pt
< *Customer Name* > 5GB	5000 MB	4800 MB	300 pt	250 pt
< *Customer Name* > 10 GB	10000 MB	9800 MB	300 pt	250 pt
< *Customer Name* > 100 GB	100000 MB	80000 MB	300 pt	250 pt
Personal Sites	100 MB	80 MB	300 pt	250 pt

10.7 Configuring Outgoing Email

1. Under **Central Administration | System Settings | E-Mail and Text Messages (SMS) | Configure outgoing e-mail settings**.
2. Configure
   - Provide an outbound SMTP server address (either from the MGD or customer forest) that will accept routing requests from all SharePoint servers.
   - Provide a From address from to build record: e.g., donotreply@microsoft.com
   - Provide a Reply-to address from to build record: e.g., donotreply@microsoft.com

10.8 Creating Web applications using Central Admin

The following table outlines what web applications to create.

Web Application	Existing Customers	New Customers	Notes
My Sites	Create	Create	https://my.contoso.com
Portal	Skip	Create	https://portal.contoso.com
Team	Create	Create	https://collab.contoso.com
Partner	Skip	Reference to-build record	https://extranet.contoso.com
DR	Create	Create	https://drtest.contoso.com

All existing customers will be provisioned with classic authentication. For new customers refer to the to-build-record to determine whether the customer should be deployed with classic or claims authentication. If not specified in the to-build-record then the default is to build out with claims.

Authentication	Classic Mode Authentication	Claims Based Authentication
IIS Web Site : Port	443	
IIS Web Site **:** Host Header	URL provided by the customer	
IIS Web Site **:** Path	<<default path>>	
Security Configuration: Authentication Provider	NTLM	
Security Configuration: Allow Anonymous**,**	No	
Security Configuration: Use Secure Sockets Layer (SSL)**,**	Yes	
Public URL	<<default values>>	
Application Pool	When creating the first web application, create an application pool called **SharePoint Content Applications** and use the managed/ms-svc-sps account. For all other web applications reuse this App Pool.	
Database Name and Authentication: Database Server	SQ-01	
Database Name and Authentication: Database Name	The default naming scheme for databases is <application>_content_<##>.	
Failover Server	Leave Blank	
Service Application Connections	<<defaults>>	
Customer Experience Improvement Program	No	

10.9 Configuring Web application common settings

The following common settings must be applied to each content web application (My, Portal, Team, DR, and Partner Access).

10.9.1 General Settings

1. Under **Central Administration | Application Management | Web Applications | Manage web applications | General Settings**
2. Make the following settings:
    a. Time Zone: reference **to-build** record
    b. Default Quota (My Web App): **Personal Sites**
    c. Default Quota (Other Web Apps): **<name> 2 GB**
    d. Browser File Handling: **Permissive**
    e. Security Validation: **60** minutes
    f. Maximum Upload Size: **250 MB**
3. Repeat step 2 for each content web application.

10.9.2 Enable the BLOB cache

By default, the disk-based BLOB cache is off and must be enabled on each content web application of each FE server.

4. Navigate to **Start | Control Panel | Administrative Tools |Internet Information Services (IIS) Manager**
5. Expand the **Machine Name** from left pane **|** expand **Sites |** right click on first content web application (My, Portal, Team, DR, and Partner Access) **| Explore**
    - Open **web.config |** select **Notepad.exe**
    - Find the element called <BlobCache /> it should resemble the following :

```
<BlobCache location="C:\BlobCache\14"
path="\.(gif|jpg|jpeg|jpe|jfif|bmp|dib|tif|tiff|ico|png|wdp|hdp|css|js|asf|avi|flv|m4v|mov|mp3|mp4|mpeg|mpg|rm|rmvb|wma|wmv)$" maxSize="10" enabled="false" />
```

    - location attribute: **C:\BlobCache\14**
    - path attribute: keep default
    - maxSize attribute: **20**
    - enabled attribute: **true**
    - Save web.config
6. Repeat step 2 for each content web application.

10.9.3 Deskless Worker Restrictive Permissions Web App Policy and User Policy

For customers that have purchased the deskless worker USL option, it is necessary to create a web application policy to restrict what they can do in SharePoint. In addition to this web app policy, we need to create a user policy to associate this web app policy with a Role Claim or AD Group.

1. Under **Central Administration | Application Management | Web Applications | Manage web applications | Permission Policy | Add Permission Policy Level**
    - Name: **Deskless Worker Deny Policy**
    - Description: **Deny policy for deskless workers**
    - Manage Lists: **Deny**
    - Override Check Out: **Deny**
    - Approve Items: **Deny**
    - Manage Permissions: **Deny**
    - View Web Analytics Data: **Deny**
    - Create Subsites: **Deny**
    - Manage Web Site: **Deny**
    - Add and Customize Pages: **Deny**
    - Apply Themes and Borders: **Deny**
    - Apply Style Sheets: **Deny**
    - Create Groups: **Deny**
    - Use Self-Service Site Creation: **Deny**
    - Enumerate Permissions: **Deny**
    - Manage Alerts: **Deny**
    - Use Client Integration Features: **Deny**
    - Manage Personal Views: **Deny**
    - Add/Remove Personal Web Parts: **Deny**

- Update Personal Web Parts: **Deny**

2. Under **Central Administration | Application Management | Web Applications | Manage web applications | User Policy | Add Users**
   - Zones: **(All zones)**
   - Users: **Add the AD group(s) specified in the build document for deskless workers.**
   - Permissions: **Deskless Worker Deny Policy**
   - Account operates as System: **leave unchecked.**
3. Repeat steps 1 and 2 for each content web application.

10.9.4 Setting Up Super User and Super Reader Accounts

Publishing sites depend on the object cache for maximum performance. This is also a required setting for claims authentication where the default users don't resolve correctly and users will get "Access Denied" error messages when navigating to the site.

1. Run **ConfigurePortalAccountsInteractive.ps1**
   - Select number of the web application
   - Super Reader Account: managed\ms-svc-rea
   - Super User Account: managed\ms-svc-sup
2. Repeat for each content web application

ConfigurePortalAccountsInteractive.ps1

```
function Prompt($s)
{
  Write-Host
  Write-Host $s
  $r = Read-host
  return $r
}

function ConfigureAccounts($application, $readerAccountString, $userAccountString)
{
  $superReaderPropertyString = "portalsuperreaderaccount"
  $superUserPropertyString = "portalsuperuseraccount"

  $fullReadRoleName = "Full Read"
  $fullControlRoleName = "Full Control"

  Write-Host

# Super Reader
       Write-Host "Adding policy user for Super Reader $readerAccountString"
       $superReaderPolicy = $application.Policies.Add($readerAccountString, "Object Cache
Super Reader")

       Write-Host "Getting Policy Role: $fullReadRoleName..."
       $role = $application.PolicyRoles | where {$_.Name -like $fullReadRoleName}

       Write-Host ("Assigning Policy Role: " + $role.Name + "...")
```

```
       $superReaderPolicy.PolicyRoleBindings.Add($role)

       Write-Host "Setting $superReaderPropertyString property..."
       $application.Properties[$superReaderPropertyString] =
[System.String]$readerAccountString

  Write-Host

# Super User
       Write-Host "Adding policy user for Super User $userAccountString"
       $superUserPolicy = $application.Policies.Add($userAccountString, "Object Cache Super
User")

       Write-Host "Getting Policy Role: $fullControlRoleName..."
       $role = $application.PolicyRoles | where {$_.Name -like $fullControlRoleName}

       Write-Host ("Assigning Policy Role: " + $role.Name + "...")
       $superUserPolicy.PolicyRoleBindings.Add($role)

       Write-Host "Setting $superUserPropertyString property..."
       $application.Properties[$superUserPropertyString] = [System.String]$userAccountString

  Write-Host
       Write-Host "Updating Web Application..."
       $application.Update() | Out-Null
}

$windowsAuthName = "Windows Authentication"
$formsAuthName = "Forms Authentication"
$genevaAuthName = "Geneva"

if(((Get-PSSnapin | foreach {$_.Name}) -contains "Microsoft.SharePoint.PowerShell") -eq
$false)
{
  Add-PSSnapIn Microsoft.SharePoint.PowerShell
}

$webAppCollection = @(Get-SPWebApplication)
$i = 1
foreach($webApp in $webAppCollection)
{
  Write-Host "[$i]:" $webApp.Name
  $i = $i + 1
}
$appIndex = [System.Int32](Prompt "Enter the number of the application to configure")

if($appIndex -gt $webAppCollection.Length -or $appIndex -lt 1)
{
  Write-Host "Invalid Index"
  Exit
}

$app = $webAppCollection[$appIndex - 1]
```

```
$zone = $app.IISSettings.Item("Default")

$authProviderNames = $zone.ClaimsAuthenticationProviders | foreach {$_.DisplayName}

$isMultiAuth = ($zone.ClaimsAuthenticationProviders.Count -gt 1)
$superReaderString = ""
$superUserString = ""

Write-Host
Write-Host "################################################################################"
Write-Host
Write-Host "Information about the default zone:"
Write-Host "  Name:" $app.name
Write-Host "  Using Claims:" $zone.UseClaimsAuthentication
Write-Host "  Is Multi Auth:" $isMultiAuth
write-Host "  Providers Enabled:" $authProviderNames
Write-Host
Write-Host "################################################################################"
Write-Host

if($zone.UseClaimsAuthentication -eq $false)
{
  Write-Host "Windows Auth is enabled, creating portal accounts with Windows users"
  Write-Host
  Write-Host -ForegroundColor Red "Default Users Accounts:"
  Write-Host -ForegroundColor Red "  Super Reader | managed\ms-svc-rea"
  Write-Host -ForegroundColor Red "  Super User   | managed\ms-svc-sup"
  Write-Host
  Write-Host "################################################################################"
  Write-Host
  $superReaderString = Prompt "Enter a Windows user name to use for the super reader account"
  $superUserString = Prompt "Enter a Windows user name to use for the super user account"
}
  else
{
  if($authProviderNames -contains $windowsAuthName)
  {
    Write-Host "Windows Auth is enabled, creating portal accounts with Windows users"
    Write-Host
    Write-Host -ForegroundColor Red "Default Users Accounts:"
    Write-Host -ForegroundColor Red "  Super Reader | managed\ms-svc-rea"
    Write-Host -ForegroundColor Red "  Super User   | managed\ms-svc-sup"
    Write-Host
    Write-Host
"################################################################################"
    Write-Host
    $superReaderString = Prompt "Enter a Windows user name to use for the super reader
account"
    $superUserString = Prompt "Enter a Windows user name to use for the super user account"
```

```
    $superReaderPrincipal = New-SPClaimsPrincipal -Identity $superReaderString -IdentityType
WindowsSamAccountName
    $superReaderString = $superReaderPrincipal.ToEncodedString()

    $superUserPrincipal = New-SPClaimsPrincipal -Identity $superUserString -IdentityType
WindowsSamAccountName
    $superUserString = $superUserPrincipal.ToEncodedString()
  }
  elseif($authProviderNames -contains $formsAuthName)
  {
    $formsProvider = $zone.FormsClaimsAuthenticationProvider
    $formsPrefix = "Forms"
    if($formsProvider -eq $null)
    {
      Write-Host "Error getting claims forms provider, defaulting to prefix `'Forms`'"
    }
    else
    {
      $formsPrefix = $formsProvider.MembershipProvider
    }

    Write-Host "Forms Auth is enabled, creating portal accounts with Forms users"
    Write-Host "Forms usernames will be prefixed with this provider:" $formsPrefix
    $superReaderString = Prompt "Enter a forms user name to use for the super reader account"
    $superUserString = Prompt "Enter a forms user name to use for the super user account"

    $superReaderPrincipal = New-SPClaimsPrincipal -Identity ($formsPrefix + ":" +
$superReaderString) -IdentityType FormsUser
    $superReaderString = $superReaderPrincipal.ToEncodedString()

    $superUserPrincipal = New-SPClaimsPrincipal -Identity ($formsPrefix + ":" +
$superUserString) -IdentityType FormsUser
    $superUserString = $superUserPrincipal.ToEncodedString()
  }
  elseif($authProviderNames -contains $genevaAuthName)
  {
    $tokenIssuer = Get-SPTrustedIdentityTokenIssuer

    Write-Host "Geneva Auth is enabled, creating portal accounts with Geneva users"
    Write-Host "Geneva usernames should not have a domain or provider in the string e.g.
testuser"

    $superReaderString = Prompt "Enter a geneva user name to use for the super reader account"
    $superUserString = Prompt "Enter a geneva user name to use for the super user account"

    $superReaderPrincipal = New-SPClaimsPrincipal -Identity $superReaderString -
TrustedIdentityTokenIssuer $tokenIssuer
    $superReaderString = $superReaderPrincipal.ToEncodedString()

    $superUserPrincipal = New-SPClaimsPrincipal -Identity $superUserString -
TrustedIdentityTokenIssuer $tokenIssuer
    $superUserString = $superUserPrincipal.ToEncodedString()
  }
```

```
  else
  {
    Write-Host "This application cannot be configured with this script"
    Exit
  }
}

if($superReaderString -eq $superUserString)
{
  Write-Host
  Write-Host "You must use different accounts for Super User and Super Reader!  Exiting..."
  Exit
}

ConfigureAccounts $app $superReaderString $superUserString
Write-Host
Write-Host "You need to IISReset on each WFE to complete the operation"
```

10.10 Setting up People Picker for each URL

Our service accounts are not trusted by the customer AD because of our one-way trust. We must specify

1. **Command Prompt |** navigate to **C:\Program Files\Common files\Microsoft Shared\Web Server Extensions\ 14\BIN**
2. Execute the following:

```
stsadm –o setapppassword – password <KeyPhrase>;
```

   Where the password is a KeyPhrase provided from our account/password spreadsheet for encrypting the login/passwords for step 3.
3. Repeat step 2 on all SharePoint VMs
4. Execute the following for all URLs including central admin, don't run unless step 2 has been run:

```
stsadm -o setproperty -url <URL> -pn peoplepicker-searchadforests -pv <list of
forests/domains>

ex: stsadm -o setproperty -url https://portal.contoso.com -pn "peoplepicker-
searchadforests" -pv
"forest:emea.contoso.com,emea\spaccount,*****;forest:na.contoso.com,na\spaccount,*****
;domain:apac.contoso.com,apac\spaccount,*****"
```

Name	Value
pv	A valid list of forests or domains. The format of the list of forests or domains value includes the following: • forest:*DnsName,LoginName,Password;* • domain:*DnsName,LoginName,Password;*
url	The URL of the Web application, in the form https://*my.contoso.com*

10.11 Creating site collections

1. Under **Central Administration | Application Management | Site Collections | Create site collections**
2. Create root site collections for each web application using the parameters listed in the following table:

Parameter	My Site	Portal*	Team	DR	Partner**
Web Application	Customer Provided URL	Customer Provided URL	Customer Provided URL	Customer Provided URL	Customer Provided URL
Template	Enterprise | MySite Host	Enterprise | Portal	Collaboration | Team Site	Collaboration | Team Site	Collaboration | Team Site
Primary Site Collection Admin	Managed\ms-svc-sps	Customer provided User	Customer Provided User	Customer Provided User	Customer Provided User
Quota	No Quota	100 GB	5 GB	5 GB	5 GB
Members Group	All IW Users	Customer Defined	Customer Defined	Customer Defined	Customer Defined
Visitors Group	All Authenticated Users	Customer Defined	All IW Users	Customer Defined; Likely All Authenticated Users	Customer Defined

***** Don't create portal root site collection for existing customers
****** Only create Partner Access root site collection if the web app was created as per to-build record for new customers

3. Under **Central Administration | Application Management | Site Collections | Create site collections**
4. To support service applications, two site collections are created as per the following table:

Parameter	Content Hub*	Broadcast site
Web Application	Team URL\sites\contenthub	Team URL\sites\Broadcast
Template	Collaboration | Team Site	PowerPoint Broadcast site
Primary Site Collection Admin	Customer Provided User	Customer Provided User
Quota	5 GB	5 GB

Parameter	Content Hub*	Broadcast site
Members Group	Customer Defined	
Visitors Group	Customer Defined; Likely All Authenticated Users	
Broadcast Presenters Group		Customer Defined
Broadcast Attendees Group		Customer Defined

5. After creating the content hub, navigate to the site collection and enable the following site collection feature: **Content Type Syndication Hub**

10.12 Creating additional content databases for each web application

1. Navigate to **Central Admin | Application Management | Databases | Manage Content databases**
2. Set the **Site Collection Level Warning** to 0 and the **Maximum Number of Site Collections** to the number of site collections in each database.
3. Repeat step 2 for each **Web Application.**
4. Click **Add a content database**
    - Database Server: **SQ-01**
    - Database Name: <application>_content_<##>.

    Note: If the customer has multiple SQL pairs for content, create **4 content databases** on the first SQ pair and the other **4 content databases** on the second SQ Pair.
5. Repeat step 4 a total of **6** more times so you have a total of **8 databases** for each **Web Application**.
6. Repeat steps 4 and 5 for each **Web Application.**

10.13 Configuring Self-service site collection

1. Navigate to **Central Admin | Application Management |Web Applications | Manage web applications**
2. Select the first content web application and choose **Self-Service Site Creation** from the ribbon.
    a. Enable Self-Service Site Creation: **On**
3. Repeat step 2 for all content web applications (My, Portal, Team, DR, and Partner Access)

10.14 Creating service applications using Central Admin

Most service applications will use default settings. Below we will highlight when configuring the service application what settings to change. If this is a new customer, all settings will be default. If building out an existing customer, build out first with the defaults and the delta (based on change requests) will be applied afterwards.

Following are the generic steps to create service applications:

1. Under **Central Administration | Application Management |Service Applications** | **Manage service applications**.
2. For each service click **New** and select **Service Application**
3. For **Name** choose the title of the type of Service Application. i.e. **Access Services Application**
4. All dbs should be created on SQ-01 and use the provide Database name if the service application has an associated database (not all do).
5. All service applications should use the **SharePoint Service Applications** App Pool, created for Access Services.

NOTE: WE ARE CREATING THE SHAREPOINT SERVICE APPLICATIONS APPLICATION POOL IN THE FOLLOWING STEP. SUBSEQUENT SERVICE APPLICATIONS WILL REUSE IT.

10.14.1 A Service Instance will not be created for the following:

- PerformancePoint Service Application

10.14.2 Configure the Access Service application:

- Name: **Access Service Application**
- App Pool: **SharePoint Service Applications** (create this pool)
- Security account: **managed\ms-svc-spa**

10.14.3 Configure the Business Data Connectivity Service Application:

- Name: **Business Data Connectivity Service Application**
- App Pool: **SharePoint Service Applications**
- Database Name: **BDC_Service_DB**
- Database Server: **SQ-01**

10.14.4 Start the State Service (via PowerShell)

1. On AP-01, navigate to **Start | All Programs | SharePoint 2010 Management Shell**
    - Execute the following PS script in the Management Shell

```
New-SPStateServiceDatabase -Name "SharePoint_State_Service" | New-
SPStateServiceApplication -Name "State Service Application" | New-
SPStateServiceApplicationProxy –DefaultProxyGroup
```

10.14.5 Configure the SharePoint Server ASP.Net Session State Service (via PowerShell)

1. On AP-01, navigate to **Start | All Programs | SharePoint 2010 Management Shell**
    - Execute the following PS script in the Management Shell

```
Enable-SPSessionStateService –DatabaseName “Session_State_Service”
```

10.14.6 Configure the Secure Store Service Application:

- Name: **Secure Store Service Application**
- Database server: **SQ-01**

- Database name: **Secure_Store_Service_DB**
- App Pool: **SharePoint Service Applications**
- Once created navigate to **Central Admin | Application Management | Service Applications | Secure Store Service Application | Manage**
    - Click **Generate New Key** where the pass phrase is **PassPhrase**
    - Click **New** Target Application
        - Target Application ID**: 101**
        - Display Name: **Visio and Excel Unattended Service Account**
        - Contact Email: Use **Email Address** from to-build record
        - Target Application Type: **Individual**
        - Target Application Administrators: **MGMT\ms-csa-admins**
        - After the Target Application is created, select App ID 101 and choose **Set Credentials**
            - Credential Owner**: MGMT\ms-csa-admins**
            - Windows User Name: Provided by customer in to-build record
            - Windows Password: Provided by customer in to-build record
    - Click **New** Target Application (If customer has provided BCS Profile Import credentials)
        - Target Application ID**: 102**
        - Display Name: **BCS Profile Import Account**
        - Contact Email: Use **Email Address** from to-build record
        - Target Application Type: **Individual**
        - Target Application Administrators: **MGMT\ms-csa-admins**
        - After the Target Application is created, select App ID 202 and choose **Set Credentials**
            - Credential Owner**: MGMT\ms-csa-admins**
            - Windows User Name: Provided by customer in to-build record
            - Windows Password: Provided by customer in to-build record

10.14.7 Configure the Excel Service Application

- Name: **Excel Service Application**
- App Pool: **SharePoint Service Applications**

10.14.7.1 Configure a service application

- Once created navigate to **Central Admin | Application Management | Service Applications | Manage Service Applications | Excel Services Application | Manage**
- Change **Trusted File Locations | c**hange address **http://** to **https://**.
- Set **Global Settings | External Data | Application ID** to **101**.

10.14.8 Configure InfoPath Forms Services

Under **Central Administration | General Application Settings | InfoPath Forms Services | Configure InfoPath Forms Services**

- Select **Allow cross-domain data access for user form templates that use connection settings in a data file**

10.14.9 Configure the Managed Metadata Service Application:

- Name: **Managed Metadata Service**
- Database server: **SQ-01**
- Database name: **Managed_Metadata_Service**
- Application Pool: **SharePoint Service Applications**
- Content Hub URL: **https://*team URL*/sites/contenthub** (created earlier)
- Select **Report syndication import errors From Site Collections using this service application**

10.14.10 Configure the PowerPoint Service Application:

- Name: **PowerPoint Service Application**
- Application pool: **SharePoint Service Applications**

10.14.11 Configuring SharePoint Foundation Search

In the primary data center this should be enabled on **AP-02**, in the secondary or PPE this should be placed on **AP-01**. There should only be one instance of SharePoint Foundation Search per farm.

1. Under **Central Administration | System Settings | Servers | Manage services on server**
2. As per table above, start the **SharePoint Foundation Search** service.
    a. Service Account: **managed\ms-svc-spa**
    b. User name: **managed\ms-svc-srh**
    c. Password: **<password for ms-svc-srh>**
    d. Database Server: **SQ-01**
    e. Database Name: **SharePoint_WSS_Search**
    f. In the **Service Account** section, select managed\ms-svc-spa.

10.14.12 Configure the Usage and Health data collection service

Under **Central Administration | Monitoring | Reporting | Configure usage and health data collection**

- Select **Enable usage data collection**
- Select **Enable health data collection**
- Database server: **SQ-R** (Reporting SQL) or **SQ-01** (PPE)
- Database Name: **WSS_Logging**

10.14.13 Configure the User Profile Service Application

- Name: **User Profile Service Application**
- Application pool: **SharePoint Service Applications**
- Database server: **SQ-01**
- Profile database name: **Profile_DB**
- Database server: **SQ-01**
- Sync database name: **Sync_DB**
- Database server: **SQ-01**

- Social Tagging Database name: **Social_DB**
- Profile Synchronization Instance: **AP-01**
- My Site Host URL: **https://<mysite URL>/**
- Site Naming Format: **Domain and user name (will not have conflicts)**

10.14.14 Configure the Search Service Application:

a. Name: **Search Service Application**
b. Fast Service Application: **None**
c. Search Service Account: **managed\ms-svc-spa**
d. Application Pool for Search Admin: **SharePoint Service Applications**
e. Application Pool for Search Query and Site Settings Web Service: **SharePoint Service Applications**

10.14.14.1 ForceClaimACLs for Search Results

A change in the 2010 architecture means that by default search doesn't support returning results in an environment with a one-way trust. After you start the Search Service Application, run the following powershell script to change how ACL permissions are stored in the Index:

```
$searchapp = Get-SPEnterpriseSearchServiceApplication
$searchapp.SetProperty("ForceClaimACLs",1)
```

10.14.14.2 Configuring the Search Service Application:

1. Under **Central Admin | Application Management | Service Applications | Manage Service Applications | Search Service Application | Manage**
    a. **System Status | Default content access account |** set to **managed\ms-svc-srh.**
    b. **System Status | Contact e-mail address** | set to **customer provided address**.
    c. Under **Administration | Farm Search Administration | Ignore SSL Warnings |** change to **Yes**
    d. Under **Crawling | Content Sources**
        i. Edit **Local SharePoint Sites** content source
        ii. From **Start Addresses** remove the reference to **https://<mysite URL>**
        iii. From **Start Addresses** remove the reference to **sps3://<mysite URL>**
        iv. Crawl Schedules | Full Crawl: **Every Sunday 1 am**
        v. Crawl Schedules | Incremental Crawl: **Every Day at 10 pm.**
    e. Click **New Content Source** to create a new content source for MySites
        i. Name: **My Sites**
        ii. Add to Start Addresses: **http://<mysite URL>**
        iii. Add to Start Addresses: **sps3://<mysite URL>**
        iv. Crawl Schedules | Full Crawl: **Every Sunday 3 am**
        v. Crawl Schedules | Incremental Crawl: **Every Day at 12 am.**
2. Modify the Search Topology (Primary Data Center)
    a. The Administration Component should be only on **AP-01**
    b. The Crawl Component should be on **AP-02.**

i. To change **Search Application Topology | Modify | Crawl Component 0 | Edit Properties | Server | AP-02**

c. The Index Partition should be on both **AP-01 and AP-02**

i. To change **Search Application Topology | Modify | Index Partition 0 | Add Mirror | Server | AP-02**

3. Confirm the Search Topology (Secondary Data Center and PPE)
   a. The Administration Component should be only on **AP-01**
   b. The Crawl Component should be only on **AP-01.**
   c. The Index Partition should be only on **AP-01**

10.14.15 Configure the Visio Graphics Service Application:

- Name: **Visio Graphics Service Application**
- Application Pool: **SharePoint Service Applications**

10.14.16 Configure a service application

- Once created navigate to **Central Admin | Application Management | Service Applications | Manage Service Applications | Visio Graphics Service Application | Manage**
- Set **Global Settings | External Data | Application ID** to **101**.

10.14.17 Configure the Web Analytics Service Application:

- Name: **Web Analytics Service Application**
- Application Pool: **SharePoint Service Applications**
- Database server: **SQ-R** (Reporting SQL) or **SQ-01** (PPE)
- Staging Database name: **Web_Analytics_Staging**
- Reporting Database name: **Web_Analytics_Reporting**
- Data Retention Period: **3 months**

10.14.18 Configure the Word Automation Service Application:

- Name: **Word Automation Service**
- Application Pool: **SharePoint Service Applications**
- Add to Default Proxy List**: True**
- Database: **SQ-01**
- Database Name: **Word_Automation_Service**

10.14.19 Configure the Word Viewing Service Application:

- Name: **Word Viewing Service**
- Application Pool: **SharePoint Service Applications**

10.14.20 Start the User Profile Synchronization Service

NOTE: TO SET UP PROFILE SYNCHRONIZATION, IT IS CRITICAL THAT THE FARM ACCOUNT (MS-SVC-SCA) HAVE LOGON ON LOCALLY RIGHTS WITH THE AP-01 SERVER. TO TEST THIS, TRY LOGGING INTO THE SERVER (AP-01) WITH THAT ACCOUNT PRIOR TO THIS STEP.

1. Under **Central Admin | Application Management | Service Applications | Manage Services on server | AP-01 | User Profile Synchronization Service | Start**
    a. Account Name: **managed\ms-svc-sca**
    b. Password: **< password for ms-svc-sca>**
2. Can take a short period of time for Forefront Identity Manager (FIM) to be setup. Wait until status changes from "Starting" to "Started".

10.14.21 Creating a profile synchronization connection within the User Profile Service Application

1. Navigate to **Central Admin | Application Management | Manage Service Applications | User Profile Service Application | Manage | Synchronization | Configure Synchronization Connections**
2. If the customer has one or more AD connections (forest level). This may include a separate connection for partner users.
    a. Click **Create New Connection**
        i. Connection Name: **<customer> AD Connection**
        ii. Type: **Active Directory**
        iii. Forest Name: **Name of Directory Servicer Forest**
            1. If customer has a co-located **domain controller** specify that here otherwise use **Auto Discover domain controller**.
        iv. Authentication Provider Type: **Windows Authentication**
        v. Account Name: **<customer domain profile import account>** from to-build record, account must have dirsync permissions
        vi. Account Password: **<customer domain profile import account>** from to-build record
        vii. Port: **389** unless customer has provided an alternative.
        viii. Select **Use SSL-secured connection**
        ix. **Populate Containers**
        x. Select Forest and Sync
    b. We prefer to sync at the forest level rather than OU level unless the customer insists differently. We can filter OUs out in a later step.
3. If there are multiple AD connections repeat step 2.

10.14.22 Configuring user synchronization filter

1. Navigate to **Central Admin | Application Management | Manage Service Applications | User Profile Service Application | Manage | Synchronization | Configure Synchronization Connections |** select **Connection | Edit Connection Filters**
2. SharePoint 2010 uses an exclusion model for Users and Groups. Specify the exclusion filter as per to-build record.

10.14.23 Manage User Permissions for the User Profile Service Application

Deskless workers (DW) don't get permission to create My Sites. We are creating permission policies to grant the right to create a My Site to Information Workers (IW) and revoking that right for DW users.

1. Navigate to **Central Admin | Application Management | Manage Service Applications | User Profile Service Application | Manage | People | Manage User Permissions**
2. For DW:
    a. Add each role claim or group for deskless workers (customer may have more than one).
    b. Select:
        i. **Use Personal Features:** Checked.
        ii. **Create Personal Site:** Unchecked.
        iii. **Use Social Features:** Checked.
3. For IW users:
    a. Add each role claim or group for IW users (customer may have more than one).
    b. Select:
        i. **Use Personal Features:** Checked.
        ii. **Create Personal Site:** Checked.
        iii. **Use Social Features:** Checked.
4. Partners have rights to create My Sites at the customer's discretion.
    a. Add each role claim or group for Partners (customer may have more than one).
    b. Select:
        i. **Use Personal Features:** Checked.
        ii. **Create Personal Site:** << Customer Option>>
        iii. **Use Social Features:** << Customer Option>>; default is Checked.
5. Click **Ok**.

10.14.24 Managed Paths

1. Under **Central Administration | Application Management | Web Applications | Manage web applications | Managed Paths**
2. Make the following settings, delete any included paths not called out below:
    - Included Paths (My Web App): **(root) - Explicit inclusion**; **personal – Wildcard inclusion**
    - Included Paths (Other Web Apps): **(root) – Explicit inclusion**; **sites – Wildcard inclusion**
3. Repeat step 2 for each content web application.

10.15 Installing Microsoft Forefront for SharePoint 2010

Note: use the managed\ms-svc-sca account. Download a trial copy here.

1. Browse to your Forefront installation path (we recommend an ISO image mounted to the VM).
2. Double-click **ForefrontSharepointsetup.exe** to launch the Setup Wizard.
3. Click the **I agree to the terms of the license agreement and privacy statement** check box, and then click **Next**.
4. If the **Service Restart** page appears, review the list of services about to be restarted, and then click **Next**.
5. On the Proxy Information page, click **Next**.
6. On the **SharePoint Information** page, specify the managed\ms-svc-sca account and password for database access. This account must be a member of the local Administrators group on the server on which you have installed SharePoint Portal Server, as well as have read/write access to the SharePoint configuration and content databases.

7. Click **Next**.
8. On the **Do you want to join the Customer Experience Improvement Program** page, indicate whether you want to **Join the Customer Experience Improvement Program**, and then click **Next**.
9. On the **Confirm Settings** page, review the data presented to you. If any changes need to be made, click the back icon in order to navigate to the screen to be changed. Otherwise, click **Next** in order to begin the installation. A progress bar indicates that the files are being copied.
10. After the installation is complete, click **Finish**.
11. Browse to **Start | Microsoft Forefront Server Protection | Forefront Protection for SharePoint Console | Policy Management | Global Settings | Advanced Options | Threshold Levels**
    a. Maximum container file size (megabytes): **250**
    b. Maximum compressed file size (megabytes): **250**

10.16 Configuring antivirus settings (Configure Once)

1. Navigate to **Central Admin | Security | General Security | Manage antivirus settings**
2. Antivirus Setting changes:
    1. Unselect **Scan documents on download**

10.17 Disabling selected site templates (perform on each WFE)

For 10.3 we do not offer Record Center and don't want customer's creating My Site Hosts.

1. Within **Notepad** | Edit **C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\TEMPLATE\1033\XML\webtempoffile.xml**
    a. Modify the <Configuration /> element containing **ID="1"** and change to:

```
<Configuration ID="1" Title="Records Center" Hidden="TRUE"
ImageUrl="/_layouts/images/strc.png" Description="This template creates a site
designed for records management. Records managers can configure the routing
table to direct incoming files to specific locations. The site also lets you
manage whether records can be deleted or modified after they are added to the
repository." DisplayCategory="Enterprise" VisibilityFeatureDependency="97A2485F-
EF4B-401f-9167-FA4FE177C6F6" >    </Configuration>
```

2. Within **Notepad** | Edit **C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\TEMPLATE\1033\XML\webtempsps.xml**
    a. Modify the <Configuration /> element containing **ID="0" Title="My Site Host"**

```
<Configuration ID="0" Title="My Site Host" Type="0" RootWebOnly="TRUE"
Hidden="TRUE" DisplayCategory="Enterprise" ImageUrl="../images/perstemp.gif"
Description="A site used for hosting personal sites (My Sites) and the public
People Profile page. This template needs to be provisioned only once per User
Profile Service Application, please consult the documentation for details.">
</Configuration>
```

3. If the customer has language packs installed, repeat steps 1 and 2 for each other locale. Just replace 1033 (English) with the locale for the other language packs. A reference for locale IDs can be found here.

10.18 Configuring the execution of Sandboxed Code to occur locally on machine (WFE)

1. Navigate to **Central Admin | System Settings | Farm Management | Manage User Solutions**
2. Change Load Balancing: **All sandboxed code runs on the same machine as a request**

10.19 Confirming and modifying service accounts assigned to services

We want to ensure that all services are correctly associated with the correct Account.

- Navigate to **Central Admin | Security | General Security | Configure Service Accounts**

Detail	Account
Farm Account	[ms-svc-sca]
Windows Service - Claims to Windows Token Service	[Local System]
Windows Service - Microsoft SharePoint Foundation Sandboxed Code Service	[ms-svc-ptc]
Windows Service - SharePoint Foundation Help Search	[ms-svc-spa]
Windows Service - SharePoint Server Search	[ms-svc-spa]
Windows Service - User Profile Synchronization Service	[ms-svc-spa]
Windows Service - Web Analytics Data Processing Service	[ms-svc-spa]
Web Application Pool - SharePoint Content Applications	[ms-svc-sps]
Service Application pool - SecurityTokenServiceApplicationPool	[ms-svc-sca]
Service Application Pool - SharePoint Service Applications	[ms-svc-spa]
Service Application Pool - SharePoint Web Services System	[ms-svc-sca]

11 Appendix

11.1 Firewall settings

For FE/AP Servers

Name	Profile	Enabled	Action	Override	Protocol	Local Port
SP Central Admin	Domain	Yes	Allow	No	TCP	8888
SP Web Services	Domain	Yes	Allow	No	TCP	32844
SP Web Services	Domain	Yes	Allow	No	TCP	32843
SP Web Services	Domain	Yes	Allow	No	TCP	32845
WWW Services	Domain	Yes	Allow	No	TCP	433

For SQL Server:

Name	Profile	Enabled	Action	Override	Protocol	Local Port
SQL Server Database Service	Domain	Yes	Allow	No	TCP	1433