CHESAPEAKE PUBLIC SCHOOLS
Purchasing Department
School Administration Building
312 Cedar Road
Chesapeake, Virginia 23322

April 1, 2010

To All Interested Parties:

Please find attached hereto our Request for Proposal **RFP #40-0910 – Microsoft Active Directory Migration.** Please read carefully the information contained herein.

You are requested to submit **one (1) original (clearly identified as "ORIGINAL"), and six (6) copies** of your response **no later than 3:00 pm Eastern Standard Time (EST), April 29, 2010** to Amy P. George, CPPB, Buyer, Chesapeake Public Schools, School Administration Building, 312 Cedar Road, Chesapeake, Virginia 23322. **You are also requested to submit one electronic copy on CD-ROM for document management purposes.**

A pre-proposal conference will be held on **April 16, 2010** at 1:00 PM in the Chesapeake Public Schools Parent Resource Center, 369 S. Battlefield Boulevard, Chesapeake, Virginia 23322, to clarify and answer any questions regarding this RFP. Questions to be addressed at the pre-proposal conference should be sent to Amy George via email at georgam@cps.k12.va.us or fax (757) 547-0279 by **April 12, 2010** at 4:00 PM. Any changes determined necessary as a result of this conference or any other source which may affect the responses to this RFP will be formally addressed by the CPS Purchasing Department via addendum/addenda. Attending this conference is not mandatory, but strongly recommended. After the pre-proposal conference, please direct all questions by phone, fax, mail or email to the contact person, no later than five (5) business days prior to the date of the RFP submittal.Please email your RSVP to the pre-proposal conference to Amy George at georgam@cps.k12.va.us by April 14, 2010.
An envelope template (**Attachment C**) has been provided for your use to be affixed to the outside of the envelope of your firm's RFP response. Failure to utilize the envelope template may result in your proposal not being received in a timely manner, which may result in your proposal not being considered.

If you have any questions concerning this RFP, please call me at (757) 547-0265.

Sincerely,

Amy P. George, CPPB
Buyer

Attachments

LETTER OF TRANSMITTAL
REQUEST FOR PROPOSAL (RFP)

Issue Date:	April 1, 2010
RFP Name:	Microsoft Active Directory Migration
RFP Number:	40-0910
Closing Date:	April 29, 2010
Closing Time:	3:00 pm Eastern Standard Time
Using Department:	Information Technology Department
Commodity Code (s):	918-29, 918-30, 918-32, 920-31, 920-45, 920-46
Issued By:	Amy P. George, CPPB, Buyer

Sealed Proposals Must Be Received by 3:00 pm Eastern Standard Time, April 29, 2010

All Inquiries For Information Should Be Directed To:
Amy P. George, CPPB, Buyer
Chesapeake Public Schools
Purchasing Department
312 Cedar Road
Chesapeake, VA 23322
Phone: (757) 547-0265, Fax: (757) 547-0279,
Email: georgam@cps.k12.va.us

If necessary, an addendum will be posted on DemandStar (www.demandstar.com) as well as the Chesapeake Public Schools' website (www.cpschools.com).

Proposals may be mailed or delivered to the Purchasing Department address listed above.

In compliance with this request for proposal and to all the conditions imposed therein and hereby incorporated by reference, the undersigned offers, and agrees to furnish services requested in the solicitation. By signing below, the undersigned attests that the offeror is not under debarment as stated in Part 2 and have complied with Ethics in Public Contracting guidelines as stated in Part 2.

THIS SECTION MUST BE COMPLETED AND SIGNED BY AN AUTHORIZED REPRESENTATIVE OF YOUR FIRM AND RETURNED AS PART OF YOUR PROPOSAL. SUBMITTALS WITHOUT SIGNATURES WILL BE DEEMED NON-RESPONSIVE.

Date: _____

Vendor Name: _____

Street Address: _____City_____State:_____Zip:_____

Name of Authorized Signor: _____**Signature:**_____

FEI/FIN No: _____Phone: _____Fax: _____

E-Mail Address: _____

Website Address: _____

Acknowledge receipt of Addendum #1 _____ #2 _____ #3 _____ #4 _____ #5 _____ (Please Initial)

TABLE OF CONTENTS

Part 6: Attachments

CHESAPEAKE
PUBLIC SCHOOLS

Microsoft Active Directory Migration
#40-0910

Request for Proposal

Part 1
Project Introduction/Background

A. PROJECT INTRODUCTION/BACKGROUND

Chesapeake Public Schools (hereafter referred to as 'the Division') is the seventh largest school system in the Commonwealth of Virginia, with 56 schools, centers and administrative buildings, and approximately 40,000 students and approximately 5,700 full-time employees.

The Division has selected Microsoft Active Directory (AD) as the application standard for their hierarchical directory services. A development, quality assurance (QA), and production environment must each be established and best practices for change control within the AD environment provided for this implementation. The vendor must propose roles and assist with CPS technical staff allocation that will be needed to assist during the implementation.

CPS recently performed a Novell Netware to Microsoft Active Directory migration analysis. **Appendix A** of this document provides the results of that analysis. This Active Directory Design Document should be used as a guide when responding to this RFP.

It can be assumed that the division will purchase the software and hardware recommended in this document utilizing contracts outside of this proposal. However, it is under the scope of this RFP that this software and hardware will be deployed.

This solicitation is subject to the provisions of the Division's purchasing procedures as well as the Virginia Public Procurement Act, which are hereby incorporated into this RFP by reference.

It is the intent to award a contract no later than July 1, 2010. It is the intent of the Division for the successful vendor's proposal, any additional information requested, and negotiated changes to be incorporated by reference into this agreement. The Division will issue a Letter of Intent, Purchase Order, and/or Contract Agreement for the services procured.

B. CONTACT PERSONS

PRE-AWARD
Amy George, Buyer
Purchasing Department
312 Cedar Road
Chesapeake, VA 23322
Telephone: (757) 547-0265
Fax: (757) 547-0279
georgam@cps.k12.va.us

All questions should be submitted in writing to Amy P. George, Buyer. All questions requiring clarification to the specifications will be answered to the extent possible in the form of addenda. The addenda will be published on DemandStar (www.demandstar.com) and the Division's website (www.cpschools.com). Any oral responses are not official. Vendor is encouraged to check DemandStar or the Division's website daily up to 48 hours prior to proposal closing to check and secure any addenda. Receipt of addenda must be acknowledged on the letter of transmittal.

POST-AWARD
Kathleen R. Pitchford, Director
Information Technology Department
369 S. Battlefield Blvd.
Chesapeake, VA 23322
Telephone: 757-482-5635

C. TENTATIVE PROCUREMENT SCHEDULE

April 1, 2010	Proposal Posted
April 12, 2010	Pre RFP Questions Due
April 16, 2010	Pre RFP Meeting
April 29, 2010	Due Date
May 7, 2010	Vendor Interviews
May 24, 2010	School Board Consideration for Approval
July 1, 2010	Contract begins

CHESAPEAKE
PUBLIC SCHOOLS

Microsoft Active Directory Migration
#40-0910

Request for Proposal

Part 2
General Terms and Conditions

Chesapeake Public Schools

General Bid Conditions
For Equipment and Supplies

The conditions set forth herein apply to all equipment, supplies, and contracted services bid to the Chesapeake Public Schools. All vendors are bound, will adhere to and comply with these conditions. **Please read these conditions carefully** as they are an integral part of the agreement and contract awarded to the successful vendor.

A. **Bid Procedure**

1. In the event a vendor finds either discrepancies or omissions in the specifications, drawings and/or bid documents, he shall notify the Purchasing Department, Chesapeake Public Schools, at once. If it is found necessary, a written addendum will be sent to each vendor. All addenda issued shall become a part of the bid documents and should be acknowledged on the letter of transmittal. **Important:** No interpretation of the meaning of the specifications, drawings and/or bid documents (except for procedural clarification) will be made orally to any potential vendor. All requests for such interpretation will be in writing and submitted no later than five (5) days prior to the date fixed for the opening of the bid.
2. The bid response must be:
    a. Sealed and submitted in a plain opaque envelope clearly marked with the bid number, date and time of bid opening as indicated in the Invitation to Bid.
    b. Submitted utilizing the envelope template provided in "**Attachment C**" in packaging your proposal for submission. Failure to do so may result in your proposal not being received in a timely manner, which may result in your proposal not being considered.
    c. Submitted in a separate envelope and not submitted or concealed within any package or envelope that may contain bid samples.
    d. Vendors who choose to utilize an overnight mailing service to deliver bid submittals should be mindful to indicate the bid number, bid due date and time of bid opening on the outside of the package. Failure to do so may affect the proper and timely receipt of bid responses.
3. All proposals will be opened and read aloud at the time and date set forth in the Invitation to Bid. Vendors or their representatives are invited to be present at the opening of bids. All bid openings will be at the School Administration Building, 312 Cedar Road, Chesapeake, Virginia unless otherwise stated in the bid. Bids received after the date and time of bid registration will not be considered.
4. Bids are to be submitted on and in accordance with forms provided by the Chesapeake Public Schools.
5. All information requested on the Letter of Transmittal and the Vendor's Response/Bid Proposal Form must be completed in order to constitute a valid bid offer.
6. Any deviations from the specifications must be set forth in the bid documents.
7. Prices and information required, except for the signature of the vendor, should be typewritten for legibility. Illegible or vague bids will be rejected. **Note:** The signature of the person submitting the bid must be handwritten. Any bid submitted with corrections must have the corrections initialed by the person who signed the bid or his designee. No bid changes will be permitted after the bid is due.
8. The use of a brand name, make or manufacturer within the specifications does not restrict the vendor solely to that specified. Instead, it serves to convey to the vendor the general style, type, character, and quality of the item desired. Any item which the Chesapeake Public Schools in its sole discretion determines to be the equal of that specified, considering quality, workmanship, economy of operation, and suitability for the purpose intended, shall be accepted.
9. When bidding an item other than that specified, the vendor will give the trade designation of the item, manufacturer's name, and detailed specification on the item he proposes to furnish. **The absence of this information** on the Vendor's Response/Bid Proposal Form will be construed as submitting a price on the identical item specified.
10. Bids on equipment must be standard new equipment, of latest model and in current production, unless otherwise specified.
11. All manufactured stock must be certified to meet all federal, state, and local codes.
12. When bids are requested on lump sum basis, vendor must enter the price for each item and also the lump sum
13. All prices quoted must be "per unit" as specified. All prices quoted will include all materials, labor, and any incidental expense incurred by the vendor in performing the contract as per the bid documents. No other charges may be added.
14. Enter the price per unit and the extensions for each item bid. In case of a discrepancy, the lowest price will govern.
15. All bid prices are to be F.O.B. destination unless otherwise indicated. If the award is made on any other basis, transportation charges will be prepaid by the successful vendor and added to the invoice as a separate item. In any case, title shall not pass until items have been delivered and accepted. Delivery alone does not constitute acceptance.

16. The vendor expressly warrants that the price or prices quoted herein are not the result of an agreement or understanding expressed or implied with any other vendor or vendors.
17. Withdrawal of bid due to error: A vendor may withdraw his bid from consideration if it contains a mistake provided that:
    a. The bid was submitted in good faith.
    b. The mistake was a clerical mistake as opposed to a judgment mistake.
    c. It was due to an unintentional arithmetic error or unintentional omission of a quantity of work, labor, or materials made in the compilation of the bid.

    Chesapeake Public Schools reserves the right to require proof from original sources of compilation that would verify the withdrawal's validity. It is preferred that notice of intent to withdraw to be given in writing within two (2) business days after conclusion of the bid opening procedure and must state the reason for withdrawal.
18. For all contracts:
    a. The vendor will not discriminate against any employee or applicant for employment because of race, religion, color, sex, national origin, age, disability, or any other basis prohibited by federal or state law relating to discrimination in employment, except where there is a bona fide occupational qualification reasonably necessary to the normal operation of the vendor. The vendor agrees to post in conspicuous places, available to employees and applicants for employment, notices setting forth the provisions of this nondiscrimination clause.
    b. The vendor will, in all solicitations of advertisements for employees placed by or on behalf of the Vendor, state that such Vendor is an equal opportunity employer; provided, however, that notices, advertisements and solicitations placed in accordance with federal law, rule or regulation shall be deemed sufficient for the purpose of meeting the requirements of this section.
    c. The vendor will include the provisions of the foregoing paragraph in every subcontract or purchase order of over $10,000, so that the provisions will be binding upon each sub vendor or vendor.
    d. During the performance of this contract, the vendor agrees to (i) provide a drug-free and tobacco-free workplace for the vendor's employees; (ii) post in conspicuous places, available to employees and applicants for employment, a statement notifying employees that the unlawful manufacture, sale, distribution, dispensation, possession, or use of a controlled substance, marijuana, or tobacco product is prohibited in the vendor's workplace and specifying the actions that will be taken against employees for violations of such prohibition; (iii) state in all solicitations or advertisement for employees placed by or on behalf of the vendor that the vendor maintains a drug-free and tobacco-free workplace; and (iv) include the provisions of the foregoing clauses in every subcontract or purchase order so that the provisions will be binding upon each sub vendor or vendor.
19. Chesapeake Public Schools is exempt from federal, state, local and excise taxes. The bid price shall be net and not include the amount of any such tax. Exemption certificates, if required, will be provided upon request. The vendor shall pay all sales, consumer, use and other similar taxes for work or portions thereof provided by the vendor which are legally enacted at the time bids are received, whether or not yet effective. The vendor shall also pay for and obtain all permits (includes all federal, state, and local) necessary to complete the project as indicted in the bid documents.
20. Sales to school boards are not affected by any fair trade agreements.
21. Prompt payment discounts will be considered in awarding the bid. However, no prompt payment discounts will be considered if offered for a period of less than twenty (20) days. Time allowed for cash discounts will be figured from date of receipt of a **properly** executed invoice form or date of delivery, whichever is later.
22. In submitting a bid, the vendor signifies that he is fully informed as to the extent and character of the supplies, material, equipment and services required and a representation that the vendor can furnish the supplies, materials, equipment, and services satisfactorily in complete compliance with the specifications. Further, the vendor signifies that he has inspected the site when deemed necessary by the vendor on which the work shall be done and is aware of all conditions affecting the execution of the work contained within the bid documents.
23. Under penalty of perjury, the vendor certifies that the bid price or prices quoted have been arrived at by the vendor independently and has been submitted without collusion with any other vendor of supplies, equipment or services of the type bid: the contents of the bid have not been communicated by the vendor, or, to his knowledge and belief, by any of his employees or agents, to any person not an employee or agent of the vendor or its surety on bond furnished herewith, prior to the official opening of the bid.
24. **No faxed bids will be accepted.**

B. **Bid Contract**

1. The Chesapeake Public Schools reserves the right to reject any or all bids in whole or in part, to waive any informalities such as technical defects, qualifications, irregularities, and omissions if in its judgment the best interest of the Chesapeake Public Schools System will be served.
2. Unless otherwise stipulated, the right is reserved to award the bid in total, by individual item, or by category (compatibility of items), whichever is in the best interest of Chesapeake Public Schools.

3. Award will be made to the lowest responsive and responsible vendor, as will best promote the public interest, taking into consideration the reliability of the vendor, the quality of the materials, warranty of the product, conformity with the specifications, purposes for which required, and terms of delivery.
4. All other factors being equal such as quality, service, cost etc., award preference shall be given in the following order: Chesapeake City firms, area firms, state firms, and out-of-state firms, if such a choice is available; otherwise, a tie shall be decided by a random drawing. Whenever any vendor is a resident of any other state and such state under its laws allows a resident vendor of that state a preference, a like preference may be allowed to the lowest responsive and responsible vendor who is a resident of Virginia.
5. The Chesapeake Public Schools reserves the right to make awards within ninety (90) days after the date of the bid opening during which period bids may not be withdrawn unless the vendor distinctly states in his bid that acceptance thereof must be made within a shorter specified time. Any bid on which the vendor shortens the time specified for acceptance, **may**, in the discretion of Chesapeake Public Schools be rejected.
6. Vendors may be notified in writing of the bid accepted.
7. In submitting a bid, the vendor obligates himself and/or his company to furnish goods or services at price bid, and that written notice from Chesapeake Public Schools constitutes a contract between the vendor and Chesapeake Public Schools. (When a written contract as a separate document is required, this will be prepared and/or approved by Chesapeake Public Schools and submitted to the successful vendor.) An award letter does not constitute official notification unless agreed to by both parties. When circumstances warrant, quantities may be adjusted by mutual consent of Chesapeake Public Schools and the successful vendor.
8. When the Chesapeake Public Schools notifies a vendor in writing of its acceptance of the vendor's price, this contract will become effective on the date acceptance is written. Notification to the vendor can be in the form of a formal contract, purchase order, award letter, or a letter of intent. Public notice of award or the announcement of the decision to award shall be provided in the form of an award letter sent to all participating vendors after final evaluation of bids have occurred. Additionally, award notification shall be posted on the Bid Board located within the Purchasing Department.
9. At its sole discretion, Chesapeake Public Schools reserves the right to accept or reject any decrease in the bid price offered by the successful vendor, as long as all conditions, specifications, etc. remain unchanged, and at any time during a contract period, if determined that it is in the best interest of the school division.
10. If the successful vendor fails to either perform within the time specified, or within a reasonable time, or fails to perform satisfactorily in accordance with the specifications, or should market conditions change such that it is not in the best interest of the Chesapeake Public Schools to continue to purchase from the contract, Chesapeake Public Schools may take the appropriate action to satisfy the contract, including cancellation of the contract. In the event a vendor fails to perform satisfactorily, and the contract has been canceled for poor or nonperformance, any cost incurred in excess of the contract amount may be back charged to the original vendor. Should the difference be less, the successful vendor shall have no claim to the difference. Additionally, the original vendor may be removed from the bid list. The vendor may be allowed to apply for reinstatement to the bid list after a period of one year or one bid cycle, which ever is longer. If reinstatement is possible, it can only occur after a meeting with a purchasing administrator in which the original vendor must demonstrate that the original unsatisfactory actions or conditions have been corrected.
11. When materials, equipment or supplies are rejected, they must be removed by the successful vendor from Chesapeake Public Schools property within ten (10) days from notification. Materials, equipment, or supplies left longer than ten (10) days will be considered as abandoned by the successful vendor and may be disposed of as if it were property of Chesapeake Public Schools.
12. The successful vendor shall not assign, transfer, convey, sublet, or otherwise dispose of the contract or his right, title, or interest therein, or his power to execute such contract to any other person, company, or corporation, without the previous written consent of the Chesapeake Public Schools.
13. The Chesapeake Public Schools reserves the right to make multiple awards from bids, if applicable, and is within the best interest of the school division.

C. **Delivery and Installation**

1. No items are to be shipped or delivered, nor any work proceed until receipt of purchase order or confirming purchase order number from an agent of the Chesapeake Public Schools Department of Purchasing.
2. Delivery must be made as stipulated on the purchase order. If for reasons beyond the control of the company the delivery cannot be made by the specified date, it will be the company's responsibility to notify the authorized representative of Chesapeake Public Schools of the reason for the delay and the new delivery date. Failure of this notification may be justification for removal of a vendor from the bid list.
3. All deliveries are to be made between 8:00 a.m. and 3:00 p.m. Monday through Friday unless otherwise stipulated in the bid.

4. No deliveries may be made on Saturday, Sunday, or a legal holiday except when the delivery is an emergency; in which event, the convenience of Chesapeake Public Schools shall govern.
5. Item shall be properly packed for shipment, storage, and stocked in new shipping containers and in accordance with accepted commercial practices.
6. The successful vendor shall be responsible for the delivery of items in good condition to the point of destination. He shall file with the carrier all claims for breakage, imperfections, and other losses, which will be deducted from invoices. The receiving representative for each participant will note for the benefit of successful vendors when packages are not received in good condition.
7. The successful vendor will be required to furnish signed proof of delivery in every instance.
8. All deliveries shall be accompanied by delivery tickets/packing slips. Tickets shall contain the following information for each item delivered:
    a. Purchase Order number and/or Contract Number.
    b. Name of Article.
    c. Item Number.
    d. Quantity.
    e. Name of Successful Vendor.

    Cartons shall be labeled with purchase order or contract number, successful vendor's name and general statement of contents. Failure to comply with this condition shall be considered sufficient reason for refusal to accept the goods at no cost to the receiving participant.
9. When installation is required, the successful vendor will be required to unload and place the material, equipment or supplies in the school or building as directed. The Chesapeake Public Schools accepts no responsibility for unloading and placing of the aforementioned. Any cost incurred due to the failure of the successful vendor to comply with the requirement will be back charged. No help for unloading will be provided by Chesapeake Public Schools; therefore, the successful vendor should have their suppliers notify their truckers accordingly. The successful vendor shall acquaint himself with the conditions to be found at the site to reduce any delivery and installation concerns and shall assume all responsibility for placing and installing the equipment in the locations required.
10. All materials, equipment, etc., are to be installed in accordance with the manufacturer's recommended installation instructions and acceptable industry practices. All work is to be performed in a quality, workmanlike manner for the purpose intended.
11. The successful vendor shall remove all debris and rubbish resulting from his work in an acceptable manner off school grounds on a daily basis. Upon completion of the work, the premises shall be left in a neat, unobstructed condition, the buildings and grounds cleaned, and everything in proper repair, and working order.
12. Equipment and supplies shall be stored at the site only on approval of the Chesapeake Public Schools and at the successful vendor's risk. In general, such on-site storage should be avoided to prevent possible damage or loss.
13. Installation shall progress in such a manner as to cause the least inconvenience to Chesapeake Public Schools and with proper consideration for the rights of other successful vendors or workmen in cases of concurrent operations. The successful vendor shall keep in touch with the entire operation and install his work promptly. He shall remain on the job site until all work is completed.
14. Equipment for trade-in shall be dismantled by the successful vendor and removed at his expense. The condition of the trade-in equipment at the time it is turned over to the successful vendor shall be the same as covered in the specifications, except as affected by normal wear and tear from use up to the time of trade-in. All equipment is represented simply "as is". Equipment is available for inspection only at the delivery point listed for new equipment, unless otherwise specified.

D. **Samples**

1. The Chesapeake Public Schools reserves the right to request a representative sample of the items bid prior to the award. If the sample fails to meet specifications, the bid will be disqualified.
2. If samples are requested subsequent to bid opening, they shall be delivered within ten (10) days of the request, or as directed, for the bid to have consideration. Samples must be furnished at no expense to the Chesapeake Public Schools and must be accompanied by a descriptive memorandum invoice indicating if the vendor desires their return provided they have not been used or made useless by tests. Award samples will be held for comparison with deliveries. The Chesapeake Public Schools will not be responsible for any samples destroyed or mutilated by examination or testing. The vendor will be advised when the sample may be picked up. Samples not remove within fifteen (15) days after written notice to the vendor will be regarded as abandoned, and the Chesapeake Public Schools shall have the right to dispose of them as its own property.
3. If specifications state that an item to be bid must equal a sample on display, the sample will be made available to all vendors by the Chesapeake Public Schools personnel. Failure of a vendor to examine the sample shall not relieve him from complying with the specifications.

4. All specifications are minimum standards, In the case of an offered bid sample being of superior quality and receiving the bid award, the delivered must be the same as sample submitted.

E. **Guarantee-Warranty**

1. The successful vendor guarantees:
   a. Against defective or faulty material or workmanship, or as stipulated in the bid document, for a period of one year from date of the rendering of the final payment.
   b. To furnish adequate protection from damage for all work and to repair damages of any kind for which he or his workmen are responsible, to the building grounds, or equipment, to his own work, or to the work of other workmen.
   c. Any merchandise provided under the contract, which is or becomes defective during the guarantee period shall be corrected or replaced to the satisfaction of Chesapeake Public Schools by successful vendor free of charge with the specific understanding that all replacements shall carry the same guarantee (on year from the date of acceptance of the replacement) as the original equipment. The successful vendor shall make any such replacement immediately upon receiving notice from Chesapeake Public Schools. Only original parts and/or equipment are to be used unless otherwise approved in writing by the Chesapeake Public Schools.
   d. All deliveries will be equal to the accepted bid sample.
   e. The equipment or furniture offered is standard, new, and of the latest model or regular stock product or as required by the specifications with parts regularly used for the type of equipment or furniture offered; also that no attachment or part has been substituted or applied contrary to manufacture's recommendations and standard practice. Every unit delivered must be guaranteed against faulty material and workmanship for a period of at least one (1) year from the date of acceptance. If during this period such faults develop, the successful vendor agrees to replace the unit or part affected without cost to the Chesapeake Public Schools.

F. **Insurance**

1. The successful vendor will be required to carry adequate insurance to protect the Chesapeake Public Schools from loss in case of accident, fire, theft, etc., prior to acceptance by a responsible person representing the Chesapeake Public Schools. Additionally, the Chesapeake Public Schools reserves the right to require bid, performance, labor, and material payment bonds. This requirement will be stated in the original bid documents if it is applicable. Bonds, if required, must be obtained from a surety company that is on both the State Corporation Commission and the Treasury Department's most recent listing of approved licensed surety companies. Insurance requirement include the following:
   a. General Liability: Liability coverage for bodily injury and property damage shall be a minimum of $1,000,000. An umbrella form of coverage may be required in some cases.
   b. Automotive Liability: The successful vendor will provide a certificate of insurance showing a minimum of $1,000,000 for automotive liability insurance to include bodily injury and property damage.
   c. Workmen's Compensation and Employer Liability: Workmen's compensation shall be required of any vendor that has employees prior to beginning work.
2. Prior to undertaking performance of the contract hereunder, the vendor shall be required to furnish certification in a form acceptable to Chesapeake Public Schools that the successful vendor possesses a valid liability insurance policy issued by an insurance company licensed to do business in the Commonwealth of Virginia with effective dates and limits of liability as required by the Chesapeake Public Schools. This certification shall insure the successful vendor's legal liability for injury to or destruction of property (real or personal) and bodily injury or death caused in whole or part by any act of omission of the successful vendor, sub vendors and the agents and employees of either, occasioned directly or indirectly in the performance of the contract. The insurance company will be required to provide thirty (30) days written notice to Chesapeake Public Schools Purchasing Department in the event of a change or cancellation of any policy. In addition, Chesapeake Public Schools **must** be listed as an additionally named insured party with respect to the contract.
3. The successful vendor shall protect, defend, and save harmless the Chesapeake Public Schools, Chesapeake School Board, City of Chesapeake, and Chesapeake City Council from and against all claim, damages, losses, judgments, and expenses (including attorney's fees) arising out of or resulting from the performance of the work provided that any such claim, damage, loss or expense (a) is attributable to bodily injury, sickness, disease, or death, or to injury or destruction of property (real or personal) including loss of use resulting there from, and (b) is also caused in whole or in part by any act of omission of the vendor, any sub vendor anyone directly or indirectly employed or controlled by any one of them regardless of whether or not said claims, damage, loss or expense is caused in part by the Chesapeake Public Schools. In any and all claims against the above aforementioned or any of its agents or employees by any employee of the vendor or any sub vendor, or anyone directly or indirectly employed by any of them or anyone for whose acts any one or more of them may be liable, the indemnification obligation of the vendor hereunder shall not be limited in any way to limits on the amount or type of damages, compensation or benefits payable to or for the vendor

or any sub vendor under the Workmen's Compensation Act, or any disability benefit acts or any other employee benefit act of the Commonwealth of Virginia or nay other state.

4. The successful vendor shall not be held responsible for losses resulting from wars, acts of public enemies, strikes, fires, floods, acts of nature, or for any other acts not within the control of the successful vendor and which by the exercise of reasonable diligence he is unable to prevent.

G. **Licenses**

1. Each vendor must be properly licensed in the locality in which their business office resides and in compliance with all pertinent state (Virginia) and local regulations. Each vendor will make himself aware of the City of Chesapeake codes and regulation relevant to business licenses and should be in compliance with said codes and regulations.

H. **Payments**

1. Payment of invoices will be certified promptly for items received in accordance with specifications and bid.
2. Payment shall not preclude Chesapeake Public Schools from making a claim for adjustment on any item later found not to have been in accordance with General Conditions, Special Conditions and Specifications of Bid.
3. Partial payments against a total order will be made upon presentation of a **properly** executed invoice and in accordance with Chesapeake Pubic Schools' accounting procedures and practices.
4. Finance charges, if incurred, can only be assessed at a rate not to exceed one percent (1%) per month or as mandated by the Virginia Public Procurement Act, Section 2.2-4352.

I. **Bid Response**

Your failure to respond to any two (2) consecutive bids will indicate disinterest, and your name may be removed from the bid list. **No faxed bids will be accepted**.

J. **Asbestos Free Statement**

The General Vendor or Prime Vendor shall be responsible for furnishing and transmitting to either the Architect/Engineer, if applicable or the Owner or his agent, notarized letters, in triplicate, of "asbestos free" certification covering all materials and equipment to be used in this project.

In the event that this General Vendor or Prime Vendor should encounter or discover asbestos related materials in connections with existing work to be altered, connected to, or to remain he shall promptly advise the Architect or Engineer for the Owner or his agent and shall not proceed with the work until receiving notice with instructions to do so.

K. **Lead Free Statement**

The General Vendor or Prime Vendor shall be responsible for furnishing and transmitting to either the Architect/Engineer, if applicable, or the Owner or his agent, notarized letters, in triplicate, of "lead free" certification covering all materials and equipment to be used in this project.

In the event that this General Vendor or Prime Vendor should encounter or discover lead containing materials in connection with existing work to be altered, connected to, or to remain he shall promptly advise the Architect or Engineer for the Owner or his agent and shall not proceed with the work until receiving notice with instruction to do so.

L. **Minorities Statement**

"Chesapeake Public Schools encourages the use of minority firms, vendors, vendors and sub vendors to provide goods and services, including construction projects."

M. **Internet Access**

Bids may be viewed and downloaded by accessing our webpage at http://www.cpschools.com/departments/purchasing/index.html and clicking on "Bids - Current."

N. **Inspection of Records**

The successful vendor/vendor shall maintain, during the course of the work/contract, and retain, not less than five years after final payment for completion thereof, complete and accurate records of all costs chargeable to Chesapeake Public Schools regarding any work or contract awarded. Additionally, Chesapeake Public Schools, or its authorized agents, shall have the right, at any reasonable time, to inspect and audit those records. The records to be maintained and retained by the work/contract shall include, without limitation, all payroll records accounting for the total time distribution of the vendor's employees working full or part time on the work (to permit tracing to payrolls and related tax returns) as well as canceled checks or signed receipts for payroll payments in cash; invoices for purchases, receiving and issuing documents, and all other unit-inventory records for the vendor's stores stock or capital items; and paid invoices and canceled checks for material purchased and for the sub vendor's and any other third-parties' charges.

0. **Faith Based Statement**

Chesapeake Public Schools does not discriminate against "Faith-Based Organizations" as that term is defined in VA. Code § 2.2-4343.1(b) of the Virginia Public Procurement Act.

P. **Debarment Status**

By submitting their proposals, vendors certify that they are not currently debarred by the Commonwealth of Virginia, or any locality in the state of Virginia, from submitting bids or proposals on contracts for the type of goods and/or services covered by this solicitation, nor are they an agent of any person or entity that is currently so debarred. Vendors under debarment should attach documentation explaining the circumstances and nature of the debarment.

Q. **Certificate of Compliance**

Effective July 1, 2006, amendments made to the Code of Virginia § 22.1-296.1 require that prior to awarding a contract, the vendor and the vendor's employees who may be in direct contact with students in the performance of the contract certify that both the vendor and the vendor's employees have not been convicted of a felony or any offense involving the sexual molestation or physical or sexual abuse or rape of a child. This certificate shall be attached to the contract document, if applicable.

R. **Certificate of Compliance with Immigration Laws and Regulations**

The Federal Immigration Reform and Control Act makes it unlawful for a person or other entity to hire, recruit, or refer for a fee for employment in the United States, an alien, knowing the alien is unauthorized to work in the United States. Section 40.1-11.1 of the Code of Virginia makes it unlawful for any employer to knowingly employ an alien who cannot provide documents indicating that he or she is legally eligible for employment in the United States. These laws place an affirmative duty on employers to ensure that aliens have proof of eligibility for employment. In addition, Section 54-72.2 of the Chesapeake City Code requires that any person or entity doing business with the City of Chesapeake, including its boards and commissions, shall provide a sworn certification by the vendor or vendor of compliance with all federal immigration laws and regulations. **Chesapeake Public Schools requires a completed Certificate of Compliance with Immigration Laws and Regulations for transactions that total more than $5,000**.This certificate shall be attached to the contract document, if applicable.

05/08/2009ag

CHESAPEAKE
PUBLIC SCHOOLS

Microsoft Active Directory Migration
#40-0910

Request for Proposal

Part 3
Scope of Work and Methodology

A. PROJECT DESCRIPTION

The Division wishes to be clear in its expectations of this project. The Division expects the successful vendor to provide essentially all of the required staff and services for the successful migration from Novell Netware to Microsoft Active Directory (AD). Division staff will assist in an advisory capacity and as the Division determines the need and availability. The Division expects to assign a Project Manager to act in concert with the successful vendors Project Manager to assure a seamless working team on this project. The Division expects that the vendor will completely turn over the project to division personnel so that the division can be self supporting of the system and have the vendor remain as a consultant after a successful migration.

Vendors will create an architectural structure, implement that structure, assist with establishing governance and work with in-house resources to design appropriate frame works and standards for a complete Microsoft Active Directory solution. A qualified vendor is a Microsoft Certified Partner with expertise in creating an architectural design for and then the implementation of the aforementioned Microsoft product offerings.

The successful vendor will be responsible for identifying the specific licensing required, the installation, implementation, consulting, integration, configuration, programming, training and ongoing support and maintenance.

The overall objective is to provide a unified, flexible solution to the Division's network operating services. It is the vision of the Chesapeake Public School's Department of Information Technology that the end product of such a migration will provide the staff and students of the Chesapeake Public Schools with a highly reliable, highly secure network operating system.

The Division has multiple schools and departments in geographically diverse locations that act as unique business units. Each department/school has different and specific application needs. The migration should have the flexibility to achieve the business objectives of each unit with maximum flexibility and least burden. The migration should also provide flexible and efficient scalability for future expansion and must provide for future growth of users and application integration.

The Division reserves the right to purchase future consulting and services from this RFP on as needed basis for supporting, maintaining and/or adding onto the system.

The Division reserves the right to have the final authority in the design and implementation of the project.

B. VENDOR REQUIREMENTS:

1. Vendors must have a minimum of 3 years experience migrating from Novell Netware to Microsoft Active Directory in environments of similar scale and complexity. Two of those years should be with in the last two years and include a Windows 2008 migration. K-12 environments are preferred.
2. Vendors must have extensive knowledge of Microsoft Windows 2008 Advanced Server, Active Directory, and Windows 2008 Forest/domain design.
3. Vendors must have knowledge of Storage Area Networks (SANS) and Network Attached Storage (NAS) technology.
4. Vendors must have experience in technical writing and editing with an ability to develop, write, and edit material for technical documentation including security design documents, group policies, guidelines, standards and related project documentation.
5. Vendors must have solid understanding of the security aspects of Windows 2008 server including NTLM/Kerberos authentication, Group Policy, Active Directory and secure server builds.

6. Vendors must have experience with firewalls, intrusion detection systems and corporate network security practices.
7. Vendor must have extensive knowledge of network architecture design and deployment.
8. Vendor must have experience with Novell Netware servers and the ability to have both servers functioning in the same environment.
9. Vendor must be a Microsoft Certified Partner and have access to Microsoft Consulting Services.

C. FUNCTIONAL/TECHNICAL REQUIREMENTS:

While utilizing the Active Directory Design Document (**Appendix A**) as a guide for responding to this RFP, the Division wants to be flexible in the design so as to take advantage of new technologies. Should the vendor see something that may have been omitted or in error they are asked to add these items as an option to the response.

The selected Vendor will:

1. Provide the architecture as well as facilitate planning, testing, migration, for implementation of Microsoft Active Directory at all CPS sites (This migration should be well documented and meet or exceed best-practices for Microsoft Active Directory security.)
2. Develop and document AD Object attribute policies, group policies, procedures and standards.
3. Design, document and implement shared file and print services.
4. Provide both Enterprise and Departmental migration plans.
5. Identify key roles and players, and establish CPS and vendor responsibilities.
6. Ensure that during and after the migration that critical CPS applications are still functioning properly. Minimize the impact to users, servers, and applications during the migration. Work performed is to have the least amount of disruption to operations and instructional programs. This will require work to be performed after normal business hours and on weekends. There will be blackout periods when work cannot be performed on the operational network, such as during SOL testing periods. Goal is zero impact.
7. Appropriate notification and mitigating strategy must be provided and deployed in cases where user impact may be unavoidable.
8. Validate existing DNS, DHCP, WINS to new AD architecture and environment.
9. Vendor must review our current Novell structure to ensure any implicit requirements are addressed.
10. Create a development environment and a Quality Assurance (QA) environment for AD.
11. Provide and document capacity planning and recommendations for a backup and storage solution.
12. Provide “lessons learned” meetings and documentation from installations.
13. Maintain an issues register and document appropriate action plan/actions taken.
14. Provide Migration planning for Enterprise and Departments, including a roadmap to simplify migrations of other departments and schools.
15. Provide maintenance and support for the Microsoft AD network for three years post installation to allow CPS staff to fully learn and understand the system.
16. Build into the proposal time for the vendor to completely turn over the support and maintenance of the systems to division personnel.
17. Describe their proposed methods for conducting a system test of all software. These described methods should include proposed benchmarks.
18. Provide a proposed implementation timeline, including proposed training schedule, installation, project management, meeting schedules, Division staff requirements, milestones and a project charter document.
19. Be responsible for providing a Migration Project Plan. The plan will outline the high level tasks as they pertain to the specific phases of the migration in appropriate chronological order (estimated timeline).

20. Provide a risk and vulnerability assessment document outlining and detailing the potential risks of the project based on experience. This shall be provided in Microsoft Project 2008 .mpp file and saved on compact disk.

During the discovery process the selected vendor will:

1. Discuss the impact on users to migrate workstations into Active Directory – The goal is zero Impact.
2. Discuss desktop and server functionality during migration, and expected downtime.
3. Discuss contingency plans during migration.

D. MAINTENANCE AND SUPPORT

1. The division will require 3 years onsite maintenance and support of the system and the software required. This will allow time to train and turn over to staff.

E. TURN OVER

1. The vendor will assist in developing a governance plan for supporting and maintaining the system by in-house staff.
2. The vendor will be responsible for providing and implementing a Turn-Over Plan for technical staff.
3. The vendor will work with the Desktop Support team, guiding them towards a standardized desktop architecture and establish PC and server system requirements needed to use AD.

F. DOCUMENTATION

1. The vendor will be responsible for providing sample documentation of system set up and design. This sample will be representative of what CPS can expect to receive upon project completion and turn-over.
2. The vendor shall provide documentation that includes diagrams showing how major solution components are interconnected.
3. The vendor will provide at least one hard copy of the documentation and one machine-readable format for the system.

CHESAPEAKE
PUBLIC SCHOOLS

Microsoft Active Directory Migration
#40-0910

Request for Proposal

Part 4
Detailed Submittal Requirements

A. PROPOSAL FORMAT

In order to be considered for selection, potential vendors must provide a complete response to this RFP. **One (1) original and six (6) copies of each proposal must be submitted no later than 3:00 p.m., Eastern Standard Time, April 29, 2010 to Amy P. George, CPPB, Chesapeake Public Schools, School Administration Building, 312 Cedar Road, Chesapeake, Virginia 23322. You are also requested to submit one electronic copy on CD-ROM for document management purposes.**

Proposals received prior to the time of the opening will be securely kept, unopened. No responsibility will be attached to the Purchasing Department for the premature opening of a proposal not properly addressed and identified. Utilize the envelope template provided in **Attachment C** in packaging your proposal for submission. Failure to do so may result in your proposal not being received in a timely manner, which may result in your proposal not being considered. The Division cautions vendors to assure actual delivery of mailed or hand-delivered proposals directly to the Purchasing Department prior to the date and time established as the deadline. Late proposals will be unopened and available for pick-up for thirty (30) days by the vendor.

Submittals shall be signed by an authorized representative of the vendor making submission. All information requested shall be submitted. Failure to submit all information required may result in submittals being rejected or a lowered evaluation of your submittal.

In order to facilitate the analysis of responses to this RFP, vendors are required to prepare their proposals in accordance with the instructions outlined as follows. Proposals should be prepared as simply as possible and provide a straightforward, concise description of the vendor's capabilities to satisfy the requirements of the RFP. Emphasis should be concentrated on accuracy, completeness, and clarity of content. All parts, pages, figures, and tables should be numbered and clearly labeled.

All vendors hereby certify that they have carefully examined all of the documents for the project, have carefully and thoroughly reviewed this RFP, and understand the nature and scope of the work to be done; and that their submittal is based upon the terms, specifications, requirements, and conditions of the RFP.

Vendors are required to follow the outline below when preparing their proposals:

i. **Signed Letter of Transmittal including acknowledgement of any Addenda.**

ii. **Table of Contents**

Section 1. **Title Page** – Show the Request for Proposal subject, the name of your company, address, telephone number, fax number, e-mail address, name of contact person and the date.

Section 2. **Table of Contents** – Clearly identify material provided by section and page number.

Section 3. **VENDOR REQUIREMENTS/EXPERIENCE**

3.1 Company Information

3.1.1 Provide a general overview of company history, stability, and technical expertise.

3.1.2 The vendor must provide financial statements applicable to the firm. If publicly held, the vendor must provide a copy of the firm's audited financial statements for the past two years. If the firm is not publicly held, the vendor must provide sufficient information to document the organization's financial stability and capability to perform the services of this RFP.

3.1.3 The vendor shall disclose any contract terminations or stop-work orders involving the vendor or any proposed subcontractor, that were stated to be the result of non-performance or poor performance that occurred within the past five (5) years. This disclosure shall include an explanation of the circumstances surrounding the termination/stop-work order, the vendor's position on the matter, dates of occurrence and the outcome. If no such default is known to exist, so declare.

3.2 Company Qualifications

3.2.1 Provide a summary statement of your firm's qualifications and experience in providing Migrations from Novell to Microsoft network operating system emphasizing the qualifications and experience of the firm.

3.2.2 Indicate resources available to your firm from Microsoft and Microsoft consulting service contract level.

3.2.3 Indicate resources available to your firm from Novell.

3.2.4 Indicate the number of 2000/2008 MCSE consultants that are available through your organization.

3.2.5 Indicate the number of Novell CNE consultants that are available through your organization.

3.2.6 Indicate how many years your business has provided migration services from Novell Netware to Microsoft Active Directory for government entities with 45,000 or more end users.

3.3 References

3.3.1 The vendor shall provide references of five (5) organizations for which it has completed services of similar size, scope and complexity as that described herein. Two (2) references must be K-12 public school systems that have successfully migrated from a Novell environment to a Microsoft AD environment. (Please specify) Two (2) references must be within the last two years and a Microsoft AD 2008 migration is preferred. (Please specify)

3.3.2 For each of the five (5) references/projects, the vendor must address the following:

- Name of the organization.
- Name of person to contact at the organization as a reference include a name, title, current phone, fax and email address.
- Provide a comprehensive and detailed description of the scope of services provided, project start and end dates, vendor's responsibilities, methodology followed and resulting deliverables.
- State whether the vendor provided services as the prime contractor or subcontractor and the percentage of work performed by vendor's staff in either case.
- State whether the project was completed on time and within budget.
- State which of the vendor's staff members assigned to this referenced project will also be assigned to the Division's project, if any. If none, so declare.

3.4 Knowledge, Skills and Abilities

3.4.1 Provide additional relevant information to further demonstrate the firm's industry knowledge, credentials, certifications, etc.

3.4.2 Provide additional relevant information to further demonstrate the firm's specialization and in-house expertise in the functional areas required of this project.

3.4.3 Provide additional relevant information to further demonstrate the firm's scope and breadth of resources (internal and/or external), available to the vendor.

3.4.4 Provide additional relevant information to further demonstrate the firm's established record of successful performance installing, integrating and maintaining similar systems.

3.4.5 Provide additional relevant information to further demonstrate the firm's experience working cooperatively with other contractors on a project site.

3.5 Personnel Management and Staff Qualifications

3.5.1 Provide a narrative which will describe the composition of the workgroup that will be directly committed to the performance of this contract and their qualifications and recent relevant experience.

3.5.2 Provide a description of the team leadership, support personnel and reporting relationships. Special mention shall be made of direct supervisors and key personnel and the percentage of total time each will be available for this project.

3.5.3 Indicate each member's primary role in the project and describe that individual's experience in performing the work to be assigned.

3.5.4 Clearly identify the person in charge of the overall project and the individual(s) accountable for the completion of each component and deliverable of the RFP.

3.5.5 Indicate experience of any members of the workgroup in performing projects of similar size and scope for other educational institutions.

3.5.6 Provide an organization chart, as it relates to this project, indicating full-time personnel, job titles, locations, and whether each individual works out of an office or is in the field.

3.5.7 Provide a resume for each individual directly committed to work on the project. Resumes shall include, at a minimum:

- Name, Job Title and Phone Number.
- Academic Background.
- Professional Certifications.
- Description of relevant industry experience with the current and previous firms.

3.6 Subcontractor Information

3.6.1 If the vendor intends to subcontract any part of its performance of this contract, provide the subcontractors' company information, level of effort, and relevant experience.

3.6.2 Provide the following information for each subcontractor:

- Subcontractor company name, address and phone number.
- List of specific tasks to be performed by subcontractor.
- Narrative of the subcontracting company's background and

capability to perform the work to be assigned.
- Percentage of performance hours intended for each subcontract.
- Total percentage of subcontractor(s) performance hours.

Section 4. **PROPOSED MIGRATION PROJECT PLAN /METHODOLOGY USED FOR THE PROJECT**

4.1 Understanding of Scope of Work and Methodology

4.1.1 Provide a statement of project understanding, affirming the vendor's comprehension of the scope of work, objectives, and desired results and the vendor's intent to comply with the RFP requirements.

4.1.2 Provide a narrative of how your organization plans to have the Microsoft environment coexist with the Novell environment until the project is complete and the Novell Netware servers have been decommissioned.

4.1.3 Provide a narrative of the requirements as they are analyzed by the vendor, to include a discussion of an awareness of the difficulties or challenges in the completion of this undertaking and a plan for surmounting them. Describe any phases, standards, procedures or best practices to be utilized. Special attention should be given to the methodological issues that will be encountered in such a project.

4.1.4 Describe problems encountered with similar clients and the approach used to resolve the issues.

4.1.5 Provide an operational management plan describing the standards and procedures to be used for successfully providing all the services required in this RFP in efficient and timely manner.

4.1.6 Provide project management objectives and plan.

4.1.7 Provide client service procedures, including communication, coordination and client satisfaction guarantees.

4.1.8 Provide the method of status reporting.

4.1.9 Provide contingency plans for problem correction, cost and schedule controls and emergency response.

4.1.10 Provide quality control policies and procedures.

4.1.11 Explain the process that will be used to manage and monitor changes to configurations and any standards established.

4.1.12 Describe the proposed methods for conducting a system test of all software. These described methods should include proposed benchmarks.

4.2 Assumptions

The vendor shall describe any assumptions upon which its proposal is based, such as:

- Division resources required.
- Division responsibilities.
- Scope of Work requirements/limitations.
- Schedule.
- If the vendor makes no assumptions, so declare.

4.3 Schedule

The vendor shall submit a detailed schedule proposed for completion of all work specified herein, noting all milestones; time required to complete each milestone; and completion of the entire project. Identify task relationships, overlap, and dependencies and start/end dates for each task.

4.4 Maintenance and Support

Describe in detail how the vendor will provide ongoing maintenance and support of the system. Specifically detail what methods are available to CPS for notifying the vendor of problems, hours of support, guaranteed response time.

4.5 Turn Over

Describe the process for providing and implementing a Turn-Over Plan for technical staff.

4.6 Documentation

Provide sample documentation of system set up and design. This sample will be representative of what CPS can expect to receive upon project completion and turn-over.

Section 5. PRICE PROPOSAL

The vendor shall present the total price to perform all of the requirements of this Request For Proposal. This shall include an itemized list of ALL costs associated with the performance of the contract, including but not limited to:

- Hourly billing rate for all personnel assigned work on this project. Provide name and job classification for each, and number of hours assigned.
- Out-of-pocket expenses.
- Full training costs for project.

The vendor shall present costs for any additional products or services proposed for the completion of the project that were not requested. The Division reserves the right to review all aspects of the Cost Proposal for reasonableness and to request clarification of any proposed cost where additional information is required or the cost component shows significant and unsupported deviation from industry standards.

An itemized list of ALL costs associated with the performance of the contract must be included in your proposal.

Section 6. EXCEPTIONS AND DEVIATIONS - If any aspects of the vendor's proposed services deviate from the requirements as described herein, provide a brief explanation to identify the Section Number and the portion of work proposed that deviates from specification. If no such deviations exist, so declare. Cite any exceptions you may have regarding any of the general and/or special conditions, requirements or any other facet of this RFP. The vendor should keep in mind that while allowance is made for you to state exceptions to this RFP, it does not in any way imply that Chesapeake Public Schools will accept or be willing

to accept any deviations from the specifications or conditions required by this RFP.

Section 7. ADDITIONAL INFORMATION

7.1 Presentation

Chesapeake Public Schools may require a presentation to be made of your services to a selection committee. Would that be acceptable?

7.2 Limitations

Include any specific terms or limitations regarding your company's ability to meet any stated requirements.

7.3 Additional Information

Include any additional information deemed pertinent for consideration as it applies to the requirements stated herein.

7.4 CERTIFICATE OF COMPLIANCE - Attachment A - See part Q, page 10 of the general bid conditions.

7.5 CERTIFICATE OF COMPLIANCE WITH IMMIGRATION LAWS AND REGULATIONS - Attachment B - See part R, page 10 of the general bid conditions.

ABSOLUTELY NO TELEPHONE, FAX, E-MAIL, OR VERBAL OFFERS WILL BE ACCEPTED.

CHESAPEAKE
PUBLIC SCHOOLS

Microsoft Active Directory Migration
#40-0910

Request for Proposal

Part 5
Selection Process

A. SELECTION PROCESS

Submittals will be reviewed by a committee and selection shall be made of one or more vendors deemed to be fully qualified and best suited to perform the services requested. The selection process shall be in accordance with the Virginia Public Procurement Act, on the basis of the following criteria:

1. **VENDOR REQUIREMENTS/EXPERIENCE**

2. **PROPOSED MIGRATION PROJECT PLAN /METHODOLOGY USED FOR THE PROJECT**

3. **PRICE PROPOSAL**

B. AWARD

The award of any contract shall be at the sole discretion of the Division. The award shall be based upon the evaluation of all information submitted, and any subsequent information required or solicited that may be necessary in clarifying or understanding information provided by the vendor in their proposal and the criteria established.

The Division intends to award a contract to the vendor(s) whose proposals are most advantageous to the Division with respect to price, conformity to the conditions, specifications and other factors as outlined herein. The Division reserves the right to accept or reject any or all proposals in whole or in part and to waive any informality, and to negotiate any prices or services offered by the vendor.

The Division shall not be required to furnish a statement of the reason why a proposal was not deemed to be fully qualified or best suited to provide the requested services.

CHESAPEAKE
PUBLIC SCHOOLS

Microsoft Active Directory Migration
#40-0910

Request for Proposal

Part 6
Attachments

ATTACHMENT A

Certificate of Compliance
Code of Virginia §22.1-296.1

I, the undersigned certify that no individual holding an office in the company and/or corporation has been convicted of a felony or any offense involving the sexual molestation or physical or sexual abuse or rape of a child.

List Officers and Titles:

Further, the following individuals will, on behalf of my firm, assist in the performance of this contract and they have not been convicted of a felony or crime as described above.

Listing of individuals assisting in the performance of this contract:

Attach additional names to this form if the space is not adequate.

I understand that should there be any change to this certification of officers, or individuals assisting in the performance of this contract, during any time of this contract, the Chesapeake Public Schools' central office/school issuing this contract/PO will be notified immediately, and an updated certification will be provided to them within five (5) days of such change.

Company

Print Name

Title

Signature

Date

FOR OFFICE USE ONLY

Acknowledged by: _____ Date:_____

If Applicable:
Project Name: _____ PO # :_____

ATTACHMENT B

CHESAPEAKE PUBLIC SCHOOLS

Certificate of Compliance
With Immigration Laws and Regulations

*****For Transactions That Total More Than $5,000*****

Return this form to the school/department responsible for finalizing your agreement.

VENDOR: FORM MUST BE NOTARIZED PRIOR TO SUBMISSION

The Federal Immigration Reform and Control Act makes it unlawful for a person or other entity to hire, recruit, or refer for a fee for employment in the United States, an alien, knowing the alien is unauthorized to work in the United States. Section 40.1-11.1 of the Code of Virginia makes it unlawful for any employer to knowingly employ an alien who cannot provide documents indicating that he or she is legally eligible for employment in the United States. These laws place an affirmative duty on employers to ensure that aliens have proof of eligibility for employment. In addition, Section 54-72.2 of the Chesapeake City Code requires that any person or entity doing business with the City of Chesapeake, including its boards and commissions, shall provide a sworn certification by the contractor or vendor of compliance with all federal immigration laws and regulations.

This certificate shall be attached to the contract document, if applicable. In any case where a purchase order will serve as the contract, this certificate shall be completed and returned to the Chesapeake Public Schools. The Contract/Purchase Order will not be issued prior to submittal of a completed Certificate of Compliance With Immigration Laws and Regulations. No performance may take place until the completed certificate is provided to the school/department responsible for finalizing your agreement. Failure to submit a certificate shall render the pending contract and/or purchase order void.

Type or print legibly when completing this form.

Legal Name of Contractor or Vendor (Note: This is your name as reported to the IRS. It should match your Social Security card or Federal Identification Number.)

TYPE OF BUSINESS ENTITY

Check one (attach additional pages to this form if the space below is not adequate):

- ❑ **Sole Proprietorship**—provide full name and address of owner
- ❑ **Limited Partnership**—provide full name and address of all partners
- ❑ **General Partnership**—provide full name and address of all partners
- ❑ **Limited-Liability Corporation**—provide full name and address of all managing members
- ❑ **Corporation**—provide full name and address of all officers

Full Name

Address

City, State and Zip

( ) Business Telephone # ( ) Business Fax #

Certificate of Compliance
With Immigration Laws and Regulations

For Office Use Only: _____ Buyer

PO #: _____

Bid/RFP Project Name: _____

Doing Business As (If Applicable) (Note: This is the name that appears on your invoices, but is not used as your reporting name.)

Name and Title of Person Completing this Certificate

Physical Business Address

Number of Employees

Are All Employees Eligible for Employment in the United States?

Under penalty of perjury, I declare on behalf of the contractor/vendor listed above that to the best of my knowledge and based upon reasonable inquiry each and every one of the contractor's employees is eligible for employment in the United States as required by the Federal Immigration Reform and Control Act of 1986 and Section 40.1-11.1 of the Code of Virginia. I further declare on behalf of the contractor/vendor that due care and diligence shall be used to ensure that all employees hired in the future will be eligible for employment in the United States and that I agree to remain in compliance throughout the duration of the contract. I affirm the information provided herein is true, correct, and complete. I also agree to permit the Chesapeake Public Schools to inspect records and documentation to ensure that all persons hired by the contractor/vendor are eligible for employment under the laws referenced in this certificate when deemed necessary by Chesapeake Public Schools. I agree that the contractor/vendor will fully cooperate in any such audit.

Sworn this _____ day of _____, 20_____

on behalf of _____
(Name of Contractor/Vendor)

as evidenced by the following signature:

Printed Name of Signatory:_____

Signature:_____

Date:_____

Please have a Notary Public complete this section (Form is invalid unless notarized)

CITY/COUNTY OF: _____

COMMONWEALTH/STATE OF:_____

The foregoing document was acknowledged before me this_____ day of _____, 20_____.

by _____.

_____
Notary Public Signature

Registration No.:_____

My commission expires:_____

Notary Seal:

Attachment C

Please complete the following "return envelope template," affix to the outside envelope of your agency's Bid/RFP response, and return to Chesapeake Public Schools. Failure to do so may affect the proper and timely receipt of your Bid/RFP response.

VENDOR'S NAME: _____

_____

_____

RFP: #	**RFP #40-0910**
BID NAME:	**MICROSOFT ACTIVE DIRECTORY MIGRATION**
CLOSING:	**3:00 P.M. EASTERN STANDARD TIME, APRIL 29, 2010**

AMY P GEORGE, CPPB, BUYER
CHESAPEAKE PUBLIC SCHOOLS
PURCHASING DEPARTMENT
312 CEDAR ROAD
CHESAPEAKE, VA 23322

CHESAPEAKE
PUBLIC SCHOOLS

Microsoft Active Directory Migration
#40-0910

Request for Proposal

Part 8
Appendix A – ACTIVE DIRECTORY DESIGN DOCUMENT

Chesapeake Public Schools

Department of Information Technology

Active Directory Design Document
Version 1.0

Date: October 2009

Chesapeake Public Schools
312 Cedar Road
Chesapeake, VA 23322

Introduction

Purpose

The purpose of this document is to provide a comprehensive description of the Chesapeake Public Schools Enterprise Infrastructure Architecture for the planning of Windows 2008 and Active Directory. This document provides descriptions on the fundamental services provided through the next generation computing environment.

Scope

The scope of this project is to create the design for an Active Directory (AD) environment that will include group policy implementation, server management, server system monitoring, and directory and data replication to remote sites. The environment will initially be implemented for current campus servers and desktops only, but should be designed to be expandable to meet the need of the district as a whole. Implementation of the AD environment for IT servers and desktops is included within the scope of this project; implementation beyond that is not. Replication between Kerberos/LDAP and Active Directory is required. SCCM 2007, SQL, and SCOM 2007 will be considered in the design of Active Directory as supported applications.

Objectives

The objective of this project is to create a Windows Active Directory environment that will meet the District's business needs for information technology management as well as better utilization of resources required to manage these technologies. Centralized management of server resources is envisioned within this project, along with improved security and improved access to resources within Active Directory. This Active Directory will provide authentication and authorization of all participating resources.

The following bullets outline the technical objectives for the Chesapeake Public Schools infrastructure project:

- Design an enterprise architecture encompassing Active Directory and supporting DDNS.
- Design a directory service architecture which will provide a single logical view of all Chesapeake Public Schools users as well as white page information for other services and agencies.
- Design a comprehensive enterprise infrastructure architecture that will serve as the foundation for consolidation and collaboration for the Chesapeake Public Schools staff.

Design Goals

The overall architectural design goals seek to implement standardization of process, procedures and technology for the Chesapeake Public Schools Enterprise Infrastructure Architecture. Specifically, the following Chesapeake Public Schools procedures, processes, and techniques will be standardized throughout the enterprise:

- Object naming conventions and standards
- Foundational Organizational Unit (OU) design

- Global group design
- Standard equipment suite to support domain hubs and network services
- Improve the current user experience through increased services, and applications
- Improve system availability, and overall system reliability
- Consolidation of servers and storage where appropriate
- Improve system recovery time should a failure occur and overall system resilience

A primary tenant of the Chesapeake Public Schools architecture is tightly controlled change management procedures. Chesapeake Public Schools will evaluate, and test any architectural and/or technological change prior to introduction into the operational environment to achieve a consistent, controlled and predictable computing environment. Change management is guided through the change management committee, extensive regression testing and limited field pilot implementations as a final validation prior to introduction into the Chesapeake Public Schools Enterprise Infrastructure Architecture operational environment.

The standardization of the organizational unit (ou) and global group structure is designed to facilitate locating objects within the Global Catalog as well as consistent access control definition throughout the enterprise. A failure to strictly enforce directory object naming standards will result in multiple objects serving the same purpose and objects with similar function having entirely dissimilar names, thus making name resolution and unambiguous object location virtually impossible. The creation of additional global groups will require a process and technology (possible web based interface to build additional appropriate groups) to determine suitability and eliminate redundancy.

Business Drivers

- Provide a solid Microsoft infrastructure to prepare for Active Directory aware applications that assist in collaboration and increased productivity
- Increase the level of security to meet FERPA requirements
- Lower Total Cost of Ownership by implementing an infrastructure that provides a foundation for consolidation
- Lower administrative responsibilities with an infrastructure that allows for automation of resources

Current Environment

CPS currently has a Novell Netware 6.x based network, with GroupWise as the supporting messaging system. Novell's Linux based products are not in production anywhere in the production network.

There are 54 remote sites, with a total of 45,000 users system wide. The sites range in size from 500 to over 3,000 users, with varying needs based on the type of location (Elementary School requirements, High School requirements, etc...), with greater requirements defined for high school and middle school users as opposed to elementary school users.

The main directory servers are located at the Battlefield Boulevard site, with replicas residing on at least one server at each location.

File and print services are provided at each location on by at least one locally placed Netware System. Further, all applications required reside locally, also on local Netware servers.

GroupWise is centrally installed at the Battlefield Boulevard location, and is installed on Novell Netware servers.

Windows 2008 Active Directory

The Active Directory is comprised of the following entities:

- Forest / Tree / Domain Architecture
- Organization Units (OU)
- Sites
- Global Catalog (GC)
- Trusts
- Groups
- Domain Operation Mods
- Naming Conventions

Background

Windows 2008 Active Directory (AD) is made up of a collection of domains. This collection of domains is known as a forest. A forest can be organized into parent-child relationships to form a hierarchy known as a tree. A *parent* domain is the domain directly superior in the hierarchy to one or more subordinate, or *child,* domains. A child domain can also be the parent of one or more child domains, and so on, as shown in Figure 1.

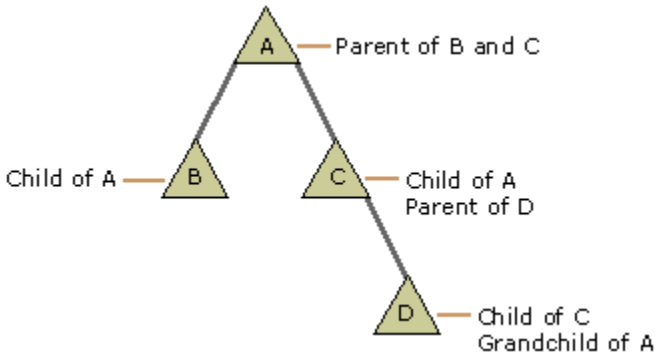


Figure 1 - Active Directory Tree

Each domain defines both an administrative boundary and a unit of replication for a collection of objects. These objects include items such as user information, printer resources, and file server shares. To provide delegated management of day-to-day tasks, each domain can be further subdivided into logical containers known as Organizational Units (OU).

Within the domain, all servers holding a copy of the domain information are known as domain controllers. Domain controllers can accept updates and replicate these changes to other domain controllers within the same domain. In order to make domain information available to users in

other domains within the forest, a subset of the most commonly needed information from all domains is stored and replicated to specified domain controllers. These domain controllers are called global catalog (GC) servers.

Selecting Forest Model

Based on the CPS requirements and current operation the AD design team came to conclusion that a single forest for the CPS will be an adequate solution. This assumption required all participants in the forest to agree about a Change Control policy for the forest. Specifically, there needs to be agreement on the changes made to the Schema and Configuration containers. The Schema Container is owned by the security group Schema Admins, and the Configuration Container is owned by the Enterprise Admins security group. Note that all containers in the Active Directory can be delegated so that other users and groups can be granted rights to operate on any containers in the AD.

Extending the Schema

It will be required to extend the schema to add classes for a particular application. Applications such as Exchange 2010, System Center Configuration Manager 2007, System Center Operations Manager 2007, and Internet Security and Acceleration (ISA) Server will require schema changes. **Schema Extensions are not reversible.**

Goals

The design must permit change without re-engineering, meet the demands of 7 by 24 operations, and be scalable.

The administration of the system must provide for centralized policy management while at the same time allowing for the delegated execution of day-to-day tasks in accordance with CPS standards.

Forest Model

The AD design team decided that CPS AD root should be implemented based on a single production forest. However, a non-production lab forest will be created for the purpose of testing proposed changes to the production forest. The changes that will be tested in this environment include things like schema changes, configuration changes, implementing new group policies, etc.

CPS.LOCAL should be considered as the primary production forest root for the Chesapeake Public Schools.

Namespace

The namespace for the Windows 2008 Active Directory will be based on a single tree structure. This provides the required functionality for the Active Directory design. The Forest root domain which is also the first logical tree structure will be called ***CPS.LOCAL*** and this namespace will be created as a dedicated Windows 2008 DNS ZONE.

Domains

The Domain Model for the CPS forest will be a single root domain for the Battlefield Boulevard campus and all outlying CPS facilities. This domain will be implemented as a pristine (i.e., brand new) domain. In Windows 2008, a security administration group will limit administrative rights within the domain. This group will use Organizational Units to delegate the rights for the performance of day-to-day tasks within the domain. The implementation of trust relationships should not be required.

Goals

- Enable the new user groups available in Native mode.
- Provide administrators the ability to nest user groups.
- Since the CPS domain will be a new Windows 2008 domain, it will be implemented as a Native mode Windows 2008 domain. To activate the new domain features, all domain controllers in the domain must be running Windows Server 2008.
- Maintain a domain structure to ensure consistency and simplicity.
- Provide a single sign-on infrastructure to access resources within the infrastructure

Windows Server 2008 Architecture Design

The CPS.LOCAL Root domain is intended to be the functional domain for all objects in the Battlefield Boulevard campus. Modifications to the AD schema will require that the person doing the modification will need to log into the CPS.LOCAL domain with an account that has schema admin rights. The domain consists of four to five DCs, and for ease of recovery, each will host a portion of the Operations Masters (OMs).

Initially, the CPS.LOCAL domain (CPS) will consist of several Windows Server 2008 DCs. Four to five DCs will be located at the main campus site. These DCs will also host any and all required DNS functionality. Additionally, as required, Read Only Domain Controllers (RODCs) should be installed to provide a local login authority at the larger remote sites.

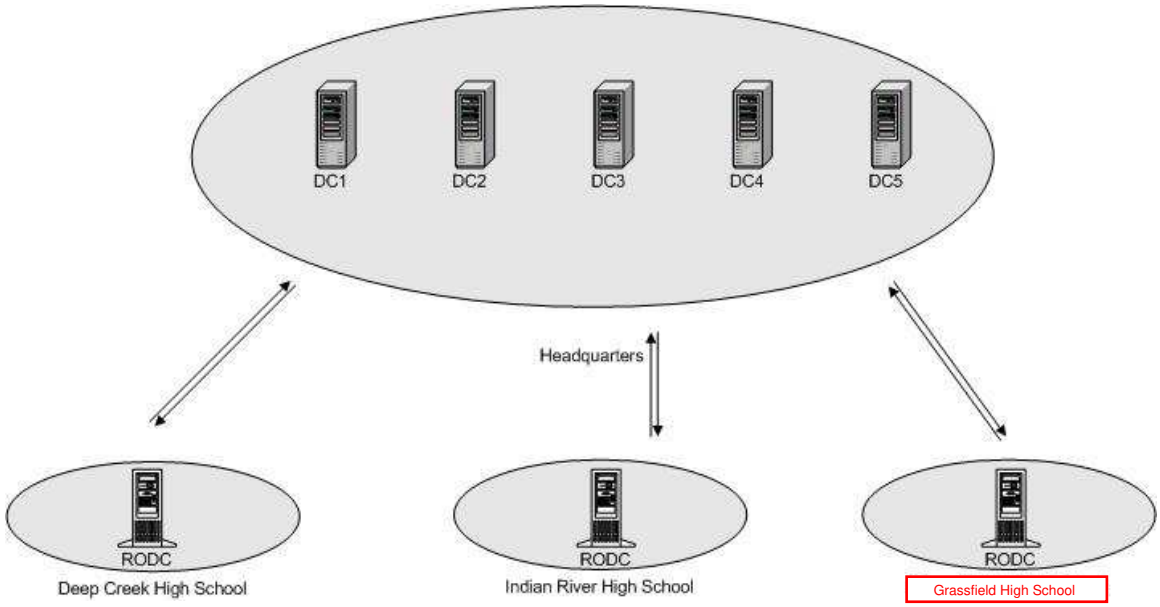


Figure 2 – Domain Controller Placement Example

CPS.LOCAL Infrastructure Services

Dynamic Domain Name System (DDNS)

The Domain Name System (DNS) is the de facto naming system for TCP/IP-based networks. Its primary role is to translate user-friendly domain names into computer-friendly TCP/IP (Transmission Control Protocol/Internet Protocol) addresses. All Windows 2008 domains are identified by a DNS name. Active Directory uses the DNS as the locator service to allow users and systems to locate resources in the network.

The DNS was originally designed to support queries of a statically configured database. While the data was expected to change, the frequency of those changes was expected to be fairly low, and all updates were made manually to a text file. With the introduction of automated IP addressing using DHCP, the process of manually updating address records became insufficient, and Dynamic DNS was developed as defined in the Internet RFC 2136.

The DNS appliance must support the following functionality.

- **Dynamic updates:** This allows DNS servers to receive incremental, dynamic updates, rather than requiring that changes be created in a static file, the whole of which must be reloaded by the server. Windows 2008, Windows 2008, and XP domain member systems can register their name and reverse address information, while a Windows 2008 DHCP server will perform these functions for down level clients. Compared to the previous methods of loading static information periodically (intervals of hours to days), zones allowing dynamic updates will change much more frequently, so these zone's data will be more consistent than static ones. Windows 2008 also supports periodic scavenging of the DNS zones to remove stale entries.
- **SRV records:** These are used to find servers by location, function or other criteria. Servers dynamically register records in sub domains of the Windows 2008 domain (named _msdcs, _sites, _tcp, _udp) to identify what services they provide. Typically, these sub domains are part of the same zone as the parent Windows 2008 domain.
- **Domain Address records:** Each Windows 2008 domain controller registers its address as an address record for the domain itself. The main purpose of these entries is to identify them as LDAP directory servers for the domain. This allows clients to contact any directory server for the domain without having to know the individual host names.

Goals

- Provide DNS services on the Windows 2008 platform
- Reduce the dependencies on Microsoft WINS in favor of a more industry standard approach for name resolution, such as DNS.
- Accommodate the existing DNS infrastructure needs within the new Windows 2008 environment.

The Domain Name System (DNS) is an integral part of Windows 2008 Active Directory. Each domain in Windows 2008 registers its services with the DNS and uses the DNS to locate other resources and services. Therefore, the CPS Windows 2008 design will include a well-designed DNS architecture. This domain will be called CPS.LOCAL and will be the authority to that domain structure.

The DNS reverse look-up zones (PTR records) should be implemented as well. All versions of Windows 2008 will register theses records automatically via DDNS by default. Integrating these zones will provide a level of resiliency and redundancy.

- The final configuration of DNS will be
- All Zones will be hosted on the DNS appliance currently in use.
- Only 2 zones should exist for each domain – one based on the FQDN and one reverse lookup zone.

Windows Internet Name Service (WINS)

When using TCP/IP to communicate on a network, a "friendly" computer name, such as *mycomputer,* must be resolved to a TCP/IP address. This is necessary because TCP/IP requires an address, such as 172.16.48.1, to establish a connection to a network device. Several different methods of name resolution exist. These methods include:

- TCP/IP broadcasts
- Static mapping files (HOSTS files)
- Using WINS to provide the computer name–to–address resolution
- DNS (in Windows NT–based networks, this is the Microsoft DNS Server)

A friendly computer name identifies computers in a Windows NT–based network. The computer name is exposed to users through Windows Explorer, and other utilities.

WINS is designed to prevent the administrative difficulties that are inherent in the use of NetBIOS broadcasts, static mapping files such as LMHOSTS files, and dynamic assignment of TCP/IP addresses. Microsoft WINS eliminates the need for IP broadcasts, while providing a dynamic, distributed database that maintains computer name–to–IP address mappings. WINS also provides facilities for centralized configuration and management

WINS servers use a replicated database that contains friendly computer names and TCP/IP address mappings (database records). When Windows-based computers log on to the network, their computer name and TCP/IP addresses are automatically registered with a specified WINS server. The WINS server database is replicated among multiple WINS servers in a local area network (LAN) or WAN.

Goals

If required, the WINS solution for the CPS will include establishing a new Windows 2008 WINS server at the Battlefield Boulevard campus site. This service will be installed and configured on a domain controller. It will function as the primary WINS for the CPS enterprise.

- DHCP Scopes will need to be modified in order to provide the client workstations participating in the IOC with the proper WINS servers.

A number of parameters will be adjusted to minimize the impact of WINS replication. To reduce the chance of a client receiving different WINS servers for the same TCP/IP subnet, all of the DHCP servers servicing a particular scope should be configured to use the same WINS server and provide the WINS server addresses in the same order.

WINS Tuning Parameters

The following table lists the recommended configuration parameters that will be used with the WINS within CPS environment.

Parameter	Setting	Comments
Logging Enabled	Enabled	
Log Detailed Events	Enabled	
Replicate Only with Partners	Enabled	Note 1
Back Up On Termination	Disabled	

Migrate On/Off	Enabled	Note 2
Database Backup Path	C:\WINNT\SYSTEM32\WINS\WINSBACKUP	Note 3

Table 1 - Recommended WINS Configuration Parameters

Note 1: To prevent unauthorized WINS servers from participating in the CPS WINS replication strategy, it is necessary to enable the Replicate Only with Partners option.

Note 2: Some TCP/IP devices do not support WINS. Therefore DNS will be used to maintain the names and TCP/IP addresses for these devices. If this is not an option, it is recommended that all static TCP/IP entries always be managed from the master WINS servers. As static devices are migrated to use WINS, it is important to enable the Migrate On/Off option. This parameter will allow for the replacement of static entries with dynamic WINS entries.

Note 3: The WINS database will automatically back up its data on a daily basis; however, it is necessary to provide a path.

Sites

Background

A Windows 2008 s*ite* is a collection of one or more IP subnets that are interconnected using a high-speed network. Sites are independent of domains, where sites map the physical structure of your network and domains typically map a logical structure of the organization. Sites are used by client computers to efficiently find network resources such as domain controllers and global catalog servers. Sites are also used to provide administrators with the ability to control replication traffic that needs to traverse WAN boundaries. There is little benefit to creating a site that does not contain at least one domain controller.

Goals

- Minimize the administrative effort required to build and maintain a Windows 2008 site topology.
- Provide administrators with the ability to closely control both the flow of replication traffic, as well as to direct client computers to infrastructure resources in an efficient manner.

The initial site topology within CPS will be modeled after the physical network infrastructure. This will result in a manageable number of sites being created, and each site will potentially contain at least one domain controller (Read Only). Having a domain controller (RODC) in the same site as the client enables faster logon, reduces WAN traffic, and enables the link generation service to properly construct the replication topology.

The sites design for the CPS regions will include initially forty seven sites. The CPS site topology will result in sites defined for all Chesapeake Public Schools locations.

This CPS site topology will provide administrators with the ability to control replication traffic within the CPS forest. In order to achieve this control, *site links* will be used to connect sites together and model the amount of available bandwidth between two sites. Site links are used to

control the network path and frequency of replication between domain controllers in the forest. There are four parameters to site links that need to be considered: cost, replication schedule, replication interval, and transport. The cost value of a site link helps the replication system determine when to use the link as compared to other links. Cost values will determine what paths replication will take through the network. The replication schedule associated with a site link indicates at what times of the day the link is available to carry replication traffic. The replication interval indicates how often the system will poll domain controllers on the other side of the site link for replication. Transport indicates whether RPC or SMTP will be used as the transport for replication. CPS should use the RPC transport exclusively.

Note*:* To improve WAN traffic first the site replication interval between the sites DCs must be set to higher number. Second it is possible to enable the Universal Group membership caching which mitigates the need for having global catalog reside at each site.

Core Site Map

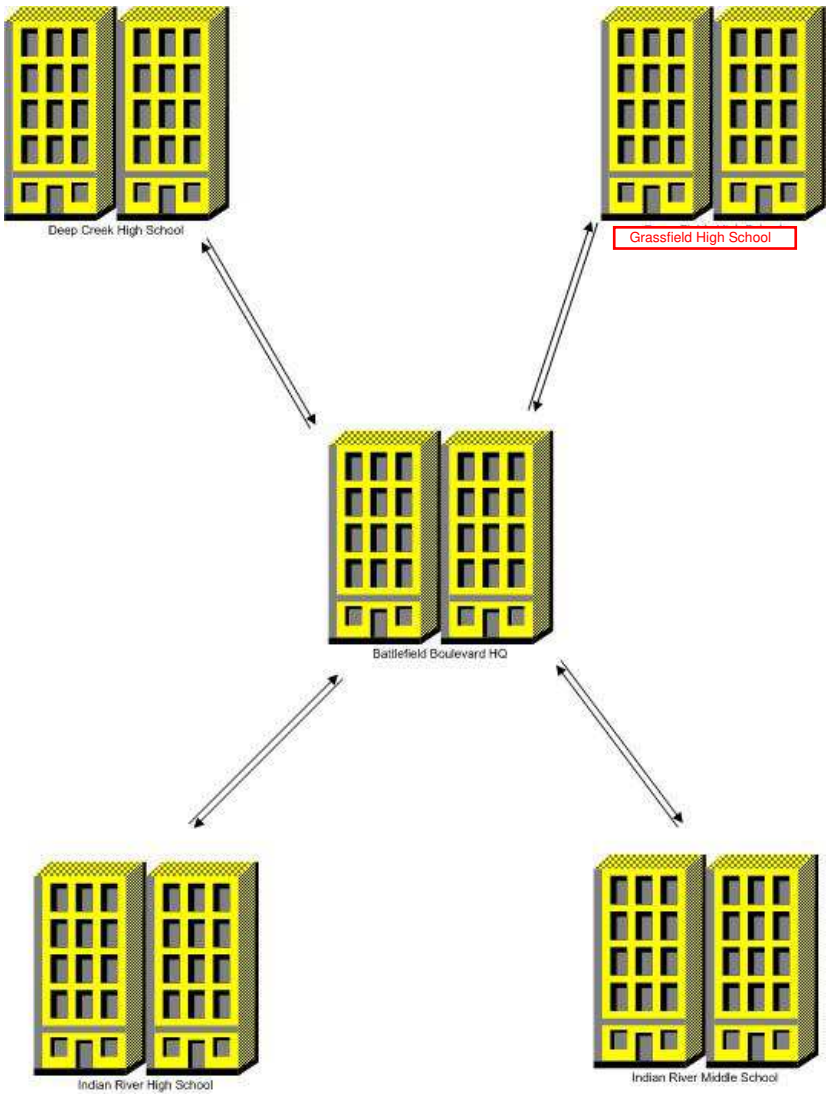


Figure 2 - Core Site Map

Standard Site Configuration

All other locations with local domain controllers will be defined as small, medium and large sites. Site connectors will be required for each site and replication and link cost calculated on a site-by-site basis.

Note: Figure 3 does not represent all sites that will be created during the site definition process.

Site Link Costs

Goals

Site Links are used to control the flow of inter-site replication traffic. The configuration of site links will directly follow the detailed network topology, and the desired paths for replication. Exchange 2010 utilizes Active Directory sites as mechanism for mail flow within the organization. Should CPS decide to implement Exchange 2010, this will allow for efficient mail routing between each site.

Once site and site link objects have been established, it is necessary to build a replication topology for the tree from this information. This replication topology provides for the exchange of information between domain controllers. Every domain controller has a built-in process known as the *Knowledge Consistency Checker* (KCC) that generates this replication topology automatically. The KCC generates and maintains the replication topology for replication within sites and between sites. Settings on the site links are the factors that the KCC considers in the process.

A "preferred" server is the server from a site selected to act as the connection point to other sites. As the KCC constructs the inter-site topology, the servers in each site are evaluated as "preferred" servers. While the KCC can automatically select the "preferred" servers, it is recommended that these servers be manually assigned to each of the site links.

Organization Units

Background

Organizational Units are directory objects that serve as a container for other directory objects. OUs can contain users, groups, computers, printers, shared folders, and other Organizational Units within a single domain. Organizational Units provide logical containers for objects in the domain.

There are two primary reasons for using OUs within an Active Directory domain. The first is to provide a model for delegating administrative tasks, and the second is a way of applying group policies to users and computers. These policies are applied at the OU level and take the form of locking down the desktop environment or assigning logon/logoff scripts to a group of users.

Goals

- Local administrators need the ability to manage resources within their geographies for which they are responsible such as computers and groups.
- Security administration is performed on a local basis for the management of user accounts and access control lists.
- Organize group policy objects on an enterprise level.

An example of how the Windows Server 2008 Active Directory (AD) will represent the CPS.LOCAL domain the top organizational unites can be seen in figure 5. The CPS Installations OU structure will consolidate the Chesapeake Public Schools user community in a several departmental OUs and distribute the local objects such as computers and groups to provide further granular separation as necessary for each organization.

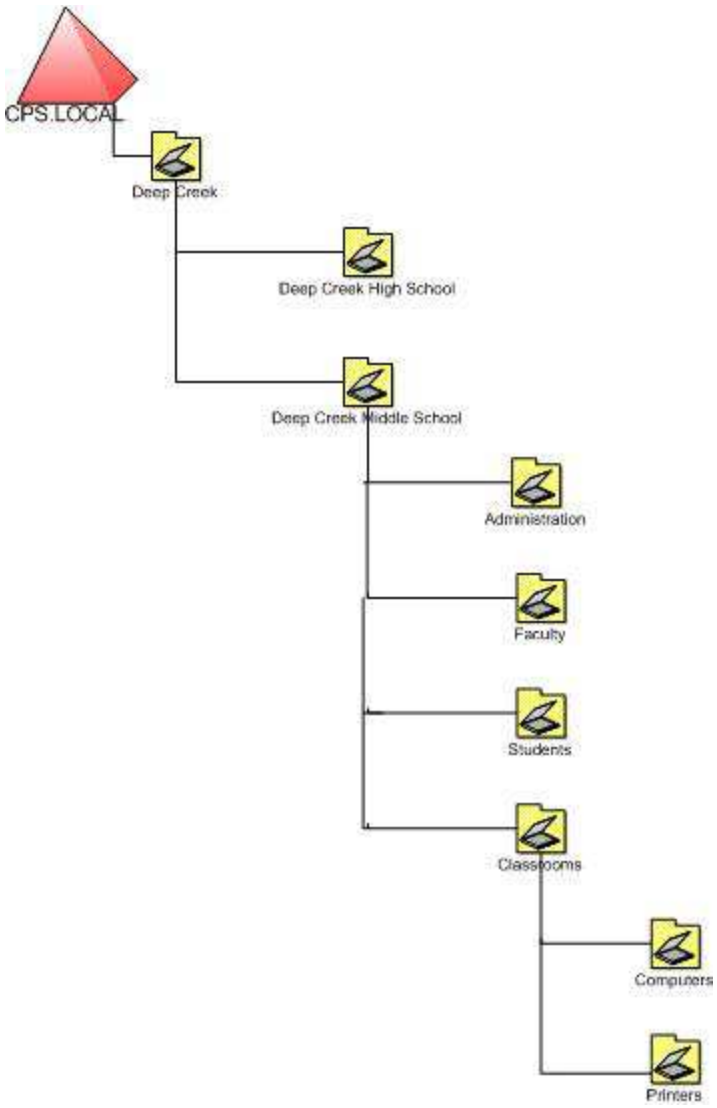


Figure 3 - AD and OU Structure

OU(s) and Group Policies

At client logon time, the local computer must enumerate the OU hierarchy that exists for both the computer account and the user account. This hierarchy is then evaluated to determine the applicable group policies to be applied. Because of this, it is recommended that group policies be used in a manner that minimizes the time needed to evaluate the effective group policy for a client. Within CPS, group policies will be applied at either the domain level or the OU that directly contains the user or computer object. In addition, group policies will be filtered by setting permissions on the objects. For example, a group can be a member of a particular OU, but can be excluded from a particular policy be removing the "READ" permissions. This will

minimize the effect that group policies have on client logon time, while still providing the ability for both centralized and localized policy management.

Groups

Background

Active Directory services provide two types of groups: *security groups* and *distribution groups*. Security groups are used to assign or deny rights and permissions to groups of users and computers so that they can gain access to resources. A security group has all the capabilities of a distribution group. Distribution groups can only be used for non-security related functions, such as e-mail lists. Security and distribution groups have a scope attribute. The scope of a group determines who can be a member of the group and where that group can be used to permission resources in the CPS.LOCAL forest.

Local Group - Local groups are security groups that can contain users and global groups from any domain in the forest. Local groups are specific to a computer and are not recognized elsewhere in the domain. Local groups are typically used to grant access to resources on a specific computer.

Domain Local Group (Native mode only) - A domain local group can be used to permission resources only within its own domain. A domain local group can contain users and global groups from any domain in the forest and can also contain other domain local groups from its own domain.

Domain Global Group - A domain **global group** can be used to permission resources anywhere in the tree. When operating in Mixed mode, a domain global group can contain users, global groups, and universal groups from other domains in the forest operating in Native mode. When operating in Native mode, a domain global group can also contain other domain global groups from its own domain.

Universal Group (Native mode only) - A **universal group** is the simplest form of group. Universal groups can be used to permission resources anywhere in the forest, and can contain other universal groups, global groups, and users from anywhere in the forest. Universal group memberships are maintained in the global catalog.

Goals

Provide Administrators with the ability to permission resources with the lowest amount of administrative and replication overhead, while providing users the required and appropriate level of access to resources.

Delegating group management to local administrators with limited access to user accounts

Recommendations

The Chesapeake Public Schools Microsoft Infrastructure Planning Committee will determine the actual groups and their roles. Windows 2008 security groups should be used to assign permission to resources instead of directly granting permissions to individual users. The

recommended strategy for using both global and domain local groups is to put user accounts into global groups and then to put global groups into domain local groups and assign resource permissions to the domain local groups. This strategy provides for the most flexibility and reduces the complexity of assigning access permissions to the network resources.

Global Catalog

Background

The g*lobal catalog* holds a replica of every object in a Windows 2008 domain. In order to keep the size of global catalog data to a minimum, each object contains only a subset of its attributes. The attributes in the global catalog are those most frequently used in search operations (such as a user's first and last names) and those attributes that are required to locate a full replica of the object. The global catalog enables users and applications to find objects in Active Directory given one or more attributes of the target object, without knowing which domain in the tree holds the object. Active Directory replication automatically builds the global catalog after an administrator has designated the server as a global catalog server. The attributes replicated into the global catalog include a base set defined by Microsoft. Administrators can specify additional properties to meet the needs of their installation. For this reason, the global catalog plays a critical role in the operations of Active Directory.

Goals

- Reduce the time required to find information about other users and resources anywhere within the network.
- Reduce the time required for client logon when operating in Native mode.

For every Active Directory site, a minimum of one global catalog server will be implemented. This will facilitate faster tree-wide directory searches and improve client logon response time when operating in Native mode. It is further recommended in this design that every domain controller be designated as a global catalog.

Directory Synchronization

Recommendations

A one way synchronization should be performed to populate the Microsoft Active Directory to replicate the user accounts already existing in Novell. Novell should remain the authoritative directory service until such a time as it is ready to be removed entirely from the CPS infrastructure.

Novell offers free tools to perform synchronization with Active Directory called "Novell's Account Management for Active Directory" which is a suite of applications that ensure information is replicated between directories.

Guidance from Novell Support should be sought before bringing the available Novell tools into the production environment. Failure to correctly configure synchronization tools can lead to the corruption of data in the target directory.

Naming Conventions

Background

Establishing a naming convention early in the process helps ensure a consistent approach for deploying a new infrastructure. The nature of the Chesapeake Public Schools requires that naming conventions be sensitive physical location. In addition, it is better to select names that are unlikely to change.

Recommendations

It is recommended that the name of a new machine reflect the physical location of the machine, the version of the operating system, and the purpose of the machine.

For instance, a Windows 2008 Server running as an domain controller located in headquarters could be named HQW2K8DC01, denoting that it is the domain controller installed in that site.

FSMO Roles

Background

Active Directory defines five operations master roles: schema master, domain naming master, relative identifier (RID) master, primary domain controller emulator, and infrastructure master. (FSMO stands for Flexible Single Master Operations). The schema master and domain naming master are per-forest roles, meaning that there is only *one* schema master and *one* domain naming master in the entire forest.

Schema Master (Forest Level FSMO)

The domain controller that holds the schema master role is the only domain controller that can perform write operations to the directory schema. Those schema updates are replicated from the schema master to all other domain controllers in the forest.

Domain Naming Master (Forest Level FSMO)

The domain controller that holds the domain naming master role is the only domain controller that can add new domains to the forest and remove existing domains from the forest.

RID Pool Master (per Domain FSMO)

A new security principal object (User, Group, or Computer) can be created on any domain controller. However, after creating several hundred security principal objects, a domain controller must communicate with the domain controller holding the domain's RID master role before creating the next security principal object. Then, another several hundred security principal objects can be created, and when this set of objects has been created, the process of contacting the RID master repeats. If a domain controller's RID pool is empty, and the RID

master is unavailable, you cannot create new security principal objects on that domain controller.

PDC Emulator (per Domain FSMO)

The domain controller holding the PDC Emulator provides backward compatibility to down-level Backup Domain Controllers (when running in Mixed Mode). The PDC emulator also provides time synchronization and password latency control. Changes to security account passwords present a replication latency problem wherein a user's password is changed on domain controller A (perhaps by an admin at a core site) and the user subsequently attempts to log on, being authenticated by domain controller B (in his local branch office). If the password has not replicated from A to B, the attempt to log on fails. Active Directory replication remedies this situation by forwarding password changes immediately to a single domain controller in the forest, the PDC emulator. If authentication fails at a backup domain controller, the authentication request is passed immediately to the primary domain controller, which is guaranteed to have the current password. The urgent replication of password changes to the PDC Emulator occurs immediately without respect to schedules between sites on site links.

Infrastructure Master (per Domain FSMO)

The domain controller holding the infrastructure master role for the group's domain is responsible for updating the cross-domain group-to-user reference to reflect the user's new name. The infrastructure master updates these references locally and uses replication to bring all other replicas of the domain up to date. If the infrastructure master is unavailable, these updates are delayed.

Locating Roles

Infrastructure Master

Infrastructure Master should not be a global catalog server in a multiple domain forest unless every domain controller is a global catalog server.

When an object on one domain controller references an object that is not on that domain controller, it represents that reference as a record containing the GUID, the SID (for references to security principals), and the DN of the object being referenced. If the referenced object moves, its GUID does not change. Its SID changes if the move is cross-domain, and its DN always changes.

The infrastructure master for a domain periodically examines the references, within its replica of the directory data, to objects not held on that domain controller. It queries a global catalog server for current information about the DN and SID of each referenced object. If this information has changed, the infrastructure master makes the change in its local replica and also replicates the new values to other domain controllers within the domain.

Domain-Naming Master

The Domain Naming Master should also be a global catalog server.

When the domain-naming master creates an object representing a new domain, it must make sure that no other object-domain object or otherwise-has the same name. The domain-naming

master achieves this by running on a global catalog server, which contains a partial replica of every object in the forest.

Role integrity and Recovery

When a role transfer takes place, it updates the current role owner before it updates the desired new role owner. If the desired new role owner fails before making its update, it does not yet hold the role. The desired new role owner can gain ownership of the role in the following ways:

Typically, you would repeat the role transfer attempt.

- Allow replication to update the desired new role owner with the change made at the current role owner. (This does not require any action on your part, but it does take more time than repeating the role transfer attempt.)
- Backing up Roles masters. When you back up a domain controller, you back up the roles it owns. When a domain controller is restored from backup media, the roles are restored also.
- Roles during the DCPROMO demotion process. When you remove Active Directory from the domain controller that owns the operations master roles, the domain controller attempts to "abandon" its roles. For each role the domain controller holds, it locates another available domain controller for the role and transfers the role to it. If another domain controller is not available during the demotion, the demotion process will not succeed.
- Do not rely on the transfer feature when removing Active Directory from a domain controller. Instead, transfer any roles before you begin the removal process so that role placements are as they should be.

The FSMO locations described in the Services Locations section above, offer the best configuration for where the roles should live. A clear set of procedures should be established on how to manage them.

The Battlefield Boulevard Campus will contain the core of the CPS.LOCAL domain. Flexible Single Masters Operations (OM) roles will all be located on the DCs.

Table 2 - Master Operation Placement

Domain / Domain Controller	Global Catalog	Schema Master	Domain Naming	PDC Emulator	RID Pool	Infrastructure Master
DC01.CPS.LOCAL	☑	☑		☑		☑
DC02.CPS.LOCAL	☑		☑		☑	
DC03.CPS.LOCAL	☑					

Time Synchronization

Background

Windows 2008 includes the W32Time (Windows Time) time service that is required by the Kerberos authentication protocol. Windows 2008 implements RFC 1361, the Simple Network Time Protocol (SNTP). The purpose of the time service is to ensure that all computers using Windows 2008 within an enterprise use a common time.

Goals

Maintain all the clocks of all Microsoft Windows computers within Chesapeake Public Schools in synchronization with an authoritative time source with a minimal amount of administrative effort.

The PDC FSMO role owner in the Chesapeake Public Schools domain will be configured to synchronize its clock with an authoritative time source. The PDC operations master at the root of the forest is DC01. As the PDC emulator, this server becomes authoritative for the enterprise and will be configured to access an external time source for enterprise time configuration

- All desktops and member servers nominate their authenticating DC as their in-bound time source.
- DC nominates the PDC emulator as the in-bound time source within the domain and time is determined by the hierarchy of domains tracing back to the root.

The following Table identifies the Public Time Services that can be used to provide time synchronization for the CPS.LOCAL domain.

Table 3 - Public Time Sources for all Domains

DNS Name	IP Address
tock.usno.navy.mil	192.5.41.40
tick.usno.navy.mil	192.5.41.41

NOTE: SNTP (Note: Simple Network Time Protocol (SNTP) uses User Datagram Protocol (UDP) port 123. Therefore, this port must be opened at the appropriate places in the TLA stack and at the firewalls protecting the AD/Windows Server 2008/Exchange 2007 enclave.

Macintosh Integration

Overview

Macintosh computers can be added to an existing Active Directory network without additional software or any changes to the Active Directory server schema. Mac OS X Tiger includes built-in support for Microsoft Kerberos (MSK) authentication and Active Directory authentication policies, such as password changes, expiration and forced password changes, as well as Active Directory replication and failover.

Services for Macintosh lets Apple Macintosh clients share files and printers and remotely connect to a Microsoft® network. The three components of Services for Macintosh are: File Server for Macintosh, Print Server for Macintosh, and the AppleTalk Protocol.

Configuration

Goals

- Allow Macintosh users to access resources within the Active Directory forest such as File and Print

Recommendation

If required, install Services for Macintosh within the Active Directory environment which includes File Server for Macintosh, Print Server for Macintosh, and the AppleTalk Protocol. This will allow clients to access the resources necessary within the Active Directory environment.

An authentication client may be needed on the clients to ensure they are able to interact with the Macintosh services within Active Directory.

File servers will require new extension associations for Macintosh files. Unless all the Macintosh clients support TCP/IP, the Appletalk protocol may need to be installed to support communication.

Windows 2008 Server

Overview

The Windows 2008 Server section examines common baseline configurations to support a Windows 2008 Active Directory environment. A baseline configuration includes hardware configuration, software configuration as well as service configurations. A baseline configuration will streamline maintenance and support for Chesapeake Public Schools. The Active Directory environment will support a Windows 2008 server configuration and it is recommended to replace the Windows 2008 domain controllers with Windows 2008. This will ensure the infrastructure will support applications that may leverage new features in Windows 2008.

Hardware Configuration

Goal

Standardizing the server hardware configurations will streamline support and maintenance procedures. Server hardware configurations consist of the following entities:

- Processor/CPU: Single or Multiple
- Memory
- Disk Subsystems: Raid Levels
- Network Interface Cards
- Backup Hardware
- Other Hardware Considerations

Recommendation

Processors

Windows 2008 fully supports symmetrical multiprocessing (SMP) servers and 64 bit technology. It is recommended that x64 bit SMP servers be used for domain controllers that are deployed.

Memory

Domain controllers that are deployed should have at least 8GB of RAM.

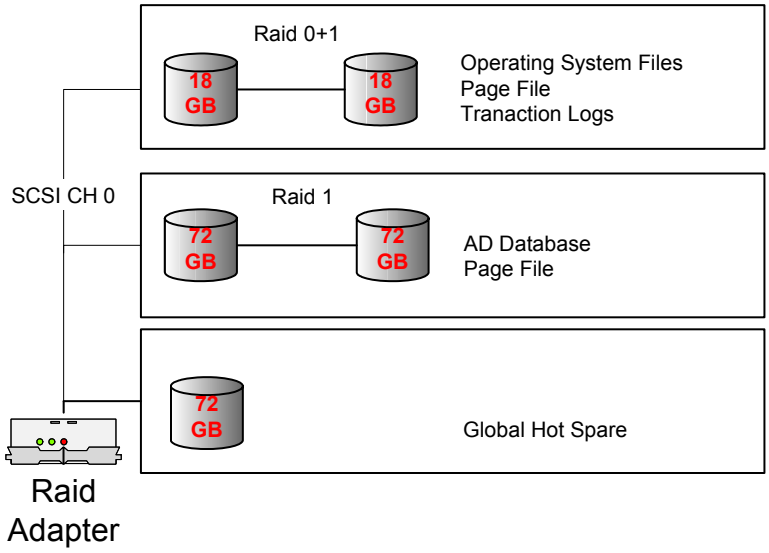
Disk Subsystems

The standard configuration should include hardware-based raid controllers using a combination of raid levels depending on the server type. The raid controller will require on-board cache, battery backup and multiple channels. Since AD has built-in read-caching, raid controllers should be configured as 75-100 % write, 25 – 0 % Read for the caching policy. Rebuild times should be set to **MEDIUM**. For application servers, this setting should be set to **HIGH**.

Dedicated Domain Controllers (Core Sites)

Dedicated domain controllers are used exclusively to provide infrastructure services (i.e., authentication, name resolution and directory lookups). These servers should be configured as follows:

Figure 4 - Drive Configuration



Network Interface Cards (NIC's)

All servers will have a 100/mb or 1/GB Ethernet adapter installed. These NIC's should be configured to operate in Full Duplex mode when this configuration is possible.

Backup Hardware

Since domain controllers will all have a duplicate copy of the active directory database, restores will be performed over the network (permitted bandwidth is available).

Other Hardware Considerations

For dedicated domain controllers, additional server hardware fault tolerance measures should be taken. This includes having ECC (error checking and correcting) Memory, hot swappable disk drives, dual fans, and dual power supplies.

Software Configurations

Directory Structure

Drive 1 – Primary Boot (Partition 1 on the RAID 1 or RAID 0+1 Array)

- C:\windows - Windows 2008 Operating System
- C:\i386 - Copy of Windows 2008 Installation Directory
- C:\DRLogs - Dr. Watson Log files
- C:\Dumps - Crash Dumps
- C:\Temp - Temporary Files
- X:\ = CD Rom

Drive 2 – AD Database (Partition on the RAID 1 Array)

- E:\NTDS - Active Directory Database
- E:\ntdslog - Active Directory Transaction Logs

- E:\perflogs – Windows 2008 Baseline Performance Logs

Drive 3 – Global Hot Spare drive that will be available for use in case if hardware failure occur at the above Raid1 drives.

System Monitoring, Tuning and Optimization

Background

Windows 2008 has many parameters that can be customized to fit Chesapeake Public Schools requirements. These parameters are considered "Best Practices" based upon field experience and support feedback. This section will focus on settings for monitoring using the event viewer and tuning and optimization settings for the operating system.

Event Log Settings

The Event Viewer maintains several separate event logs on the server:

- System Log
- Security Log
- Application Log
- DNS Server Log
- File Replication Service Log
- Directory Service Log

The log files are a critical feature for the monitoring of Windows 2008 operations. Each log can be set to a maximum file length and a write policy.

In the implementation event log properties will be changed from 512k to 10mb for maximum size, and will be configured to "Overwrite as needed" from "Overwrite every 7 Days".

Performance Options

Windows 2008 has a self-tuning function that allows the operating system to configure runtime parameters for memory and processor contention. These parameters allow an administrator set priority for different processes based on the server's function. The two categories are Application Response and Virtual Memory.

Recommendations

These settings can be changed in the following location: Start→Settings→Control Panel → "System" Icon→Advanced Tab. From this menu select "Performance".

Application Response:
All servers should be configured to Optimize performance for "Background Services". A setting of "Applications" would only give benefit for a Terminal Service server running in application mode.

Virtual memory setting:
All servers will pre-define a paging file of RAM times 1.5 on the C: and D: Partitions (if the D partition exists) and set the maximum and minimum page file size to the same value.

Server Performance Monitoring

In order to gather data about a server's performance over time, it is necessary to develop a server's baseline performance metrics. The baseline metrics allows an administrator to know what the server's normal performance levels are during different times of the day or month. Windows 2008 comes with the "Performance Logs and Alerts" feature which provides the ability to monitor and alert on hundreds of different performance metrics. Thus, in order to be able to manage the amount of data that is collected and to avoid negatively impacting the performance of the server, you must be very selective when determining which performance metrics to monitor. The items that you want to include as part of your baseline are metrics that provide data about processor, memory, and disk performance. This provides a complete view as to how the server is performing. Furthermore, a performance baseline is necessary for each individual server because the normal operation levels tend to vary between servers.

Recommendations

It is recommended that Chesapeake Public Schools use the Performance Monitor logs to create a new performance counter log that will create the server performance baseline. This baseline will consist of a data gathering interval of every 15 minutes and will run on a 24 by 7 basis. The performance log files will be located in the E:\perflogs directory and start with the name of servperf. The specific counter data that should be captured in the baseline log file are as follows:

- Memory Object – Pages per Second counter - is the rate at which pages are read from or written to disk to resolve hard page faults. (Hard page faults occur when a process requires code or data that is not in its working set or elsewhere in physical memory, and must be retrieved from disk). This counter is a primary indicator of the kinds of faults that cause system-wide delays. It is the sum of Memory\\Pages Input/sec and Memory\\Pages Output/sec. It is counted in numbers of pages, so it can be compared to other counts of pages, such as Memory\\Page Faults/sec, without conversion. It includes pages retrieved to satisfy faults in the file system cache (usually requested by applications) non-cached mapped memory files.
- Processor Object - % Processor Time counter is the percentage of elapsed time that the processor spends to execute a non-Idle thread. It is calculated by measuring the duration of the idle thread is active in the sample interval, and subtracting that time from interval duration. (Each processor has an idle thread that consumes cycles when no other threads are ready to run). This counter is the primary indicator of processor activity, and displays the average percentage of busy time observed during the sample interval. It is calculated by monitoring the time that the service is inactive and subtracting that value from 100%.
- Physical Disk Object – Average Disk Queue Length counter is the average number of both read and write requests that were queued for the selected disk during the sample interval.

These counters will be used to develop the baseline of the server's performance. Administrators should review these logs on a monthly basis to determine how the server is performing. This can be accomplished by opening the baseline log file with the System Monitor tool.

Dr. Watson Setting:

Settings for the Dr. Watson debugging application can be changed by running drwtsn32.exe from the command line.

Recommendations

- LogFilePath = c:\DRLogs
- CrashDump = c:\dumps
- Number of Instructions: 10
- Number of errors to save: 10
- Options (default)

Startup and Recovery Option

System Failure:

- Write an event to the system log
- Send an Administrative Alert
- Automatically Reboot? YES
- Write debugging info: complete
- Dump file path: c:\dumps
- Checkbox: overwrite existing file

Tuning the System Cache

Windows 2008 can tune the cache allocation for file and print sharing based on the type of services offered by the server. To change these settings:

1. Start→ Settings→ Network and Dialup Connections
2. Right-click on Network Adapter, select “Properties”
3. Right-click on “File and Print Sharing for Microsoft Networks, select “Properties”
4. Select Optimization: Minimize, Balance, File Sharing, Applications

Recommendations

For application servers such as Exchange, SMS, and SQL, this setting will be set to “Maximize data throughput for Applications”. For dedicated file and print servers, this setting will be set to “Maximize data throughput for File Sharing “. For Active Directory domain controllers this setting will be set to “Balance”. Make Browser broadcast should not be checked.

Replication Monitoring

Windows 2008 includes “Replication Monitor” which will monitor Active Directory replication. If further functionality is needed that is not provided by this product, it is recommended that NETPRO’S DirectoryAnalyzer product be evaluated. DirectoryAnalyzer provides proactive monitors for replication, DNS, operations masters, domain controllers, global catalogs and sites; it can also send alerts in the event of a failure

System Center Operations Manager 2007

Microsoft System Center Operations Manager is a software solution to meet the need for end-to-end service monitoring in the enterprise IT environment. Operations Manager provides an easy-to-use monitoring environment that monitors thousands of servers, applications, and clients to provide a comprehensive view of the health of an organization’s IT environment.

If possible be implemented as an follow up to this project for monitoring purposes. It is recommended to replicate the above best practices on monitoring to ensure the proper management of the servers is in place. CPS will have the ability to not only monitor the Active Directory environment, but applications such as Exchange, SQL, SCCM, and ILM.

Server Startup and Recovery Options

Restoring a Domain Controller

If a domain has more than one domain controller, you can restore it in one of two ways. You can either restore Active Directory using replication with another domain controller, or restore Active Directory from backup media. If there are no domain controllers in the domain, then you can only restore Active Directory from backup media.

In order to restore the System State data on a domain controller, you must first start your computer in a special safe mode called directory services restore mode. This will allow you to restore the SYSVOL directory and AD directory service database.

Restoring Active Directory with a Replica

Use the Active Directory Installation wizard to reinstall Active Directory, promoting the server to a domain controller. Active Directory and Sysvol will be brought up-to-date through replication from a domain controller. Before you run the Active Directory Installation wizard, delete any references to the old domain controller using the Sites and Services snap-in.

Restoring Active Directory from Backup Media

Use Backup to restore the System State, which will recover Active Directory, File Replication Service (including Sysvol) and Certificate Services (if installed). If the domain controller computer has been replaced because of malfunctioning or the network adapters have been replaced, you might need to reconfigure the network settings manually.

If you are restoring the System State data to a domain controller, you must choose whether you want to perform an authoritative restore or a non-authoritative restore. The default method of restoring the System State data to a domain controller is non-authoritative.

Non-authoritative Restore

In this mode, any component of the System State that is replicated with another domain controller, such as the Active Directory service or the File Replication service (including the SYSVOL directory), will have their original update sequence number. The Active Directory replication system uses this number to detect and propagate Active Directory changes among the servers in your organization. Thus, after you restore the data, it will be brought up to date by replication. For example, if the last backup was performed a week ago, and the System State is restored using the default restore method (non-authoritative), any changes made after the backup operation was ran will be replicated from the domain controllers.

Authoritative Restore

In some cases, you may not want to replicate the changes that have been made subsequent to the last backup operation. In other words, there may be instances where you want all replicas to

have the same state as the backed up data. To achieve this state, you must perform an authoritative restore.

For example, you have to perform an authoritative restore if you inadvertently delete users, groups, or organizational units from the AD directory service and you want to restore the system so that the deleted objects are recovered and replicated. To do this, you need to run the Ntdsutil utility after you have restored the data but before you restart the domain controller. This utility lets you mark objects as authoritative. When an object is marked for authoritative restore, its update sequence number is changed so that it is higher than any other update sequence number in the Active Directory replication system. This will ensure that any replicated or distributed data that you restore is properly replicated or distributed throughout your organization.

Backup / Restore

Windows 2008 includes functionality that will require existing disaster recovery procedures to be reviewed in order to ensure a high level of recoverability. Data contained on a Windows 2008 Server can be separated into the following classes, each of which needs to be addressed in the disaster recovery procedure:

- Registry: A database repository for information about a computer's configuration.
- Components Services Class Registration database: A database that stores class registrations.
- System startup files: Critical system files that are required in order for the system to boot to a minimal state of functionality.
- Certificate Services database: A database that stores issued certificates. A certificate is a file used for authentication and secure exchange of data on non-secured networks, such as the Internet.
- Active Directory services: The directory that stores information about network resources, as well as all the service that makes the information available and useful. These resources include user data, printers, servers, databases, groups, computers, and security policies.
- SYSVOL folder: The shared system volume, which is a folder structure that exists on all Windows 2008 domain controllers. It stores scripts and some of the group policy objects for both the current domain as well as the enterprise.

In addition to the built-in backup utility, Windows 2008 includes new functionality to aid in the recovery of a Windows 2008 server that will not boot due to a configuration problem. The Recovery Environment is a text-mode command interpreter that is separate from the Windows 2008 command prompt and allows the system administrator to gain access to the hard disk of a computer running Windows 2008, regardless of the file format used, for basic troubleshooting and system maintenance. Since starting Windows 2008 is not a prerequisite for using the Recovery Environment, it can help recover a computer powered by Windows 2008 that does not start properly or at all.

Goals

Provide administrators with the ability to easily manage the backup and recovery of data and configuration information maintained on Windows 2008 servers.

Ensure new functionality of the Windows 2008 product is leveraged to aid in the recovery of Windows 2008 servers in the event that erroneous configuration of a server renders it inoperable.

Recommendations

The proposed architecture of the Windows 2008 environment within Chesapeake Public Schools will result in multiple copies of each domain partition existing on the network. In addition to providing a high level of availability of directory data, this design will allow for the restoration of a domain controller by performing an installation of Windows 2008 and relying on the replication of domain data from an existing domain controller. The need to perform a restoration of an Active Directory database will thus be limited to those situations where directory data has not yet replicated to other domain controllers prior to a server failure, or where the time required performing replication will have a negative impact on the availability of network resources.

It is recommended that the current backup software in use within Chesapeake Public Schools be upgraded to versions that are Windows 2008 logo compliant. This will ensure that the application is capable of performing Active Directory backup and recovery operations on an enterprise level.

It is also recommended that Chesapeake Public Schools incorporate the installation of the Recovery Environment as a standard on every Windows 2008 installation. This will provide administrators with the ability to troubleshoot and potentially solve problems that otherwise will require a restoration of files from tape.

Windows 2008 Security

Authentication in Windows 2008

Overview

The Chesapeake Public Schools information security officer will have the overall responsibility for security policy. Thus, the ISO will ensure that the proposed policies and settings follow the Chesapeake Public Schools security standards.

Windows 2008 has adopted Kerberos as the default protocol for network authentication. An emerging standard, Kerberos provides a foundation for interoperability while enhancing the security of enterprise-wide network authentication.

Windows 2008 implements Kerberos version 5 with extensions for public key authentication. The Kerberos client is implemented as a security provider through the Security Support Provider Interface. Initial authentication is integrated with the Winlogon single sign-on architecture. The Kerberos Key Distribution Center (KDC) is integrated with other Windows 2008 security services running on the domain controller and uses the domain's Active Directory as its security account database.

Windows 2008 supports several protocols for verifying the identities of users who claim to have accounts on the system, including protocols for authenticating dial-up connections and protocols for authenticating external users who access the network over the Internet. But there are only two choices for network authentication within Windows 2008 domains:

Kerberos Policy Options

In Windows 2008, Kerberos policy is defined at the domain level and implemented by the domain's KDC. Kerberos policy is stored in Active Directory as a subset of the attributes of domain security policy. By default, policy options can be set only by members of the Domain Administrators group.

Kerberos policy includes these settings:

Table 4 - Recommended Kerberos Policy Settings

Policy	Description	Default
Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy **Enforce user logon restrictions**	When this option is enabled, the KDC validates every request for a session ticket by examining user rights policy on the target computer to verify that the user has the right either to Log on locally or to Access this computer from network.	Enabled
Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy **Maximum lifetime for service ticket**	Determines the maximum amount of time (in minutes) that a granted session ticket can be used to access a particular service.	600 Min.
Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy **Maximum lifetime for user ticket**	Determines the maximum amount of time (in hours) that a user's ticket-granting ticket (TGT) may be used.	10 Hrs.
Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos **Policy Maximum lifetime for user ticket renewal**	Total lifetime of ticket with possibly many session renewals.	7 Days
Computer Configuration\Windows	Determines the maximum time difference (in minutes) that Kerberos	5 Min.

Settings\Security Settings\Account Policies\Kerberos **Policy Maximum tolerance for computer clocks synchronization**	will tolerate between the time on a client's clock and the time on a server's clock while still considering the two clocks synchronous. Kerberos uses timestamps to prevent replay attacks.	

Goals

All aspects of the Windows 2008 design include security as a required parameter. The Chesapeake Public Schools ISO has overall responsibility for security policy. Thus, the ISO will ensure that the proposed settings follow CPS security standards. A secure platform is critical in order to achieve a successful migration. Specifics in securing a Windows 2008 platform include Security Policies, User and System Policies, Account Policies, Auditing and security setting of the infrastructure services. Specific settings for the domain are listed in the respective sections below.

Recommendations

It is recommended that Chesapeake Public Schools use the built-in Kerberos authentication by using the default settings for all Windows 2008 communications.

Account Password & Lockout Policy Options

Recommendations

The settings below will be reviewed by the Chesapeake Public Schools ISO to ensure that they follow CPS security standards. Note: By default, Account Policies (Password, Lockout, and Kerberos settings) are all defined at the domain level. This ensures a consistent security policy throughout the domain. The CPS domain account password and account lockout policies are defined in the table below.

Table 5 - Recommended Domain Account Password & Account Lockout Policies

Policy	Description	Setting
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy **Enforce password history**	Password history specifies the number of previous passwords remembered.	Remember 24 passwords
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy **Maximum password age**	Specifies the password expiration for the domain.	90 days

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy **Minimum password age**	Prevents the user from changing the password more frequently than once every 3 days.	1 day
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy **Minimum password length**	The password must be at least 8 characters.	8 characters
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy **Passwords must meet complexity requirements of the installed password filter**	The default password filter (passfilt.dll) requires the following: Does not contain all or part of the user's account name ▪ Is at least six characters in length ▪ Contains characters from three of the following four categories: ▪ English upper case characters (A..Z) ▪ English lower case characters (a..z) ▪ Base 10 digits (0..9) ▪ Non-alphanumeric (For example, !,$#,%) ▪ Complexity requirements are enforced upon password change or creation.	Enabled
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy **Store password using reversible encryption for all users in the domain**	This option is available to support applications that use protocols that require knowledge of the user password for authentication purposes. It should NOT be enabled unless such a requirement exists.	Disabled
Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy **Account lockout duration**	Determines the number of minutes a locked out account will remain locked out.	5 minutes
Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy **Account lockout threshold**	Determines the number of failed logon attempts that will cause a user account to be locked out.	5 attempts
Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy **Reset account lockout counter after**	Determines the number of minutes that must elapse after a failed logon attempt before the bad logon attempt counter is reset to 0 bad logons.	21600 minutes

Local Policy & Event Log Options

Recommendations

The settings below will be reviewed by the Chesapeake Public Schools ISO to ensure that they follow CPS security standards. The following local policy and event log settings will be applied at the domain level.

Table 6 - Recommended Local Policy and Event Log Options

Policy	Description	Setting
Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy **Audit account logon events**	Determines whether to audit each instance of a user logging on or logging off of another computer where this computer was used to validate the account.	Success & Failure
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options **Do not display last user name in logon screen**	Determines whether the name of the last user to logon to the computer is displayed in the Windows logon screen	Enabled
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options Message text for users attempting to log on	Specifies a text message that is displayed to users when they log on. This text is often used for legal reasons, such as to warn users about the ramifications of misusing company information or to warn them that their actions may be audited.	Use of Chesapeake Public Schools computing systems is restricted to authorized use only. The use of any Chesapeake Public Schools computing system may be monitored and recorded by Chesapeake Public Schools for administrative and security reasons at any time. Your use of these computing systems constitutes consent to this monitoring. CPS reserves the right to take appropriate action against anyone who accesses or uses, or attempts to access or use, any Chesapeake Public Schools computing system improperly or without the appropriate authorization>
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options **Message title for users**	Allows the specification of a title to appear in the title bar of the window that contains the Message text for users attempting to log on.	<>

attempting to log on		
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options Rename administrator account	Determines whether a different account name will be associated with the security identifier (SID) for the account "Administrator." By associating the Administrator SID with another account, you will no longer have an account named "Administrator," which is often a point of attack by hackers.	Confidential – will be provided at deployment time
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options **Rename Guest account**	Determines whether a different account name will be associated with the security identifier (SID) for the account "Guest." By associating the Guest SID with another account, you will no longer have an account named "Guest," which is often a point of attack by hackers.	Administrator
Computer Configuration\Windows Settings\Security Settings\Event Log\Settings for Event Logs **Maximum application log size**	Specifies the maximum size for the application event log.	10240KB
Computer Configuration\Windows Settings\Security Settings\Event Log\Settings for Event Logs **Maximum security log size**	Specifies the maximum size for the security event log.	10240KB
Computer Configuration\Windows Settings\Security Settings\Event Log\Settings for Event Logs **Maximum system log size**	Specifies the maximum size for the system event log.	10240KB
Computer Configuration\Windows Settings\Security Settings\Event Log\Settings for Event Logs **Retention**	Determines the "wrapping" method for the application log.	Overwrite events as needed

method for application log		
Computer Configuration\Windows Settings\Security Settings\Event Log\Settings for Event Logs **Retention method for security log**	Determines the "wrapping" method for the security log.	Overwrite events as needed
Computer Configuration\Windows Settings\Security Settings\Event Log\Settings for Event Logs **Retention method for system log**	Determines the "wrapping" method for the system log.	Overwrite events as needed

Group Policy Objects

Overview

A Group Policy object contains an extensive profile of security permissions that apply primarily to the security settings of a domain, computer, or users. A single Group Policy object can be applied to all of the computers in an organizational unit. Group Policy gets applied when the individual computer starts up, and periodically is refreshed if changes are made without restarting.

How Group Policy Works

Group Policy objects are associated with domains and organizational units (folders) in the Active Directory Users and Computers snap-in to MMC. The permissions granted by the Group Policy are applied to the computers stored in that folder. Group Policy can also be applied to sites using the Active Directory Sites and Services snap-in.

Group Policy settings are inherited from parent folders to child folders, which might in turn have their own Group Policy objects. A single folder could have more than one Group Policy object assigned to it. For more information on Group Policy precedence and how conflicts are resolved among multiple policy objects, see Windows 2008 Help.

Group Policy is the complementary component to security groups. Group Policy lets you apply a single security profile to multiple computers. It enforces consistency and provides easy administration.

Group Policy objects contain permissions and parameters that implement multiple types of security strategies.

Considerations about Group Policy

In general, Group Policy can be passed down from parent to child sites and organizational units. If you have assigned a specific Group Policy to a high level parent, that Group Policy applies to all organizational units beneath the parent, including the user and computer objects in each container.

Security templates (described later in this section) could be useful to you as models of security settings appropriate to different types of Group Policy.

Goals

- Provide consistent security throughout the enterprise.
- Provide consistent environment for the desktop user.
- Provide customization flexibility from domain to domain.

Recommendations

Settings will be enforced in the domain GPO. This will provide a consistent domain wide security policy.

All domain policies, except for the account policies, local policies, and event log settings will be implemented at the lowest level of OU possible. The number of group policy objects will be kept to a minimum, preferably one, in order to reduce logon times.

The following non-default settings are recommended, but not required for the typical Windows XP Professional workstation at Chesapeake Public Schools. These settings are broken down into two tables. One table is for computer settings and the other is for user settings.

Other settings can be applied to a group of users or workstations on an as needed basis. All policy changes must be thoroughly tested in a lab environment before implementing them in the production domain. If the number of policies begins to become unmanageable, then third party Group Policy management tools (for example, Fazam 2003 from Full Armor) should be evaluated by Chesapeake Public Schools.

Windows Management Instrumentation (WMI) filters allow you to dynamically determine the scope of Group Policy objects (GPOs) based on attributes of the target computer.

When a GPO that is linked to a WMI filter is applied on the target computer, the filter is evaluated on the target computer. If the WMI filter evaluates to false, the GPO is not applied (except if the client computer is running Windows 2000, in which case the filter is ignored and the GPO is always applied). If the WMI filter evaluates to true, the GPO is applied.

WMI makes data about a target computer available for administrative use. Such data can include hardware and software inventory, settings, and configuration information. For example, WMI exposes hardware configuration data such as CPU, memory, disk space, and manufacturer, as well as software configuration data from the registry, drivers, file system, Active Directory, the Windows Installer service, networking configuration, and application data.

A WMI filter consists of one or more queries based on this data. If all queries are true, the GPO linked to the filter will be applied. The queries are written using the WMI Query Language (WQL), a SQL-like language. Queries can be combined with AND and OR logical operators to achieve whatever effect the administrator wants. Each query is executed against a particular WMI namespace. When you create a query, you must specify the namespace. The default is root\CIMv2, which is appropriate for most WMI queries.

The WMI filter is a separate object from the GPO in the directory. To apply a WMI filter to a GPO, you link the filter to the GPO. This is shown in the WMI filtering section on the Scope tab of a GPO. Each GPO can have only one WMI filter, however the same WMI filter can be linked to multiple GPOs.

Table 7 - Recommended Computer GPO Settings

Policy	Description	Setting
Computer Configuration\Administrative Templates\ Windows Components\NetMeeting **Disable remote Desktop sharing**	Disables the remote desktop sharing feature of NetMeeting. Users will not be able to set it up or use it for controlling their computers remotely.	Disabled
Computer Configuration\Administrative Templates\ Network\Network and Dial-up Connections **Prohibit configuration of connection sharing**	Determines whether administrators can enable, disable, and configure the Internet Connection Sharing feature of a dial-up connection.	Enabled
Computer Configuration\Administrative Templates\ Printers **Pre-populate printer search location text**	Enables the Location Tracking feature of Windows 2008 printers. Location tracking lets you design a location scheme for your enterprise and assign computers and printers to locations in your scheme. Location tracking overrides the standard method of locating and associating users and printers, which uses the IP address and subnet mask of a computer to estimate its physical location and proximity to other computers.	Enabled

Table 8 - Recommended User GPO Settings

Policy	Description	Setting
User Configuration\Windows Settings\Folder Redirection**My Documents**	This setting forces the My documents folder to be redirected to a specific location.	Target folder location
User Configuration\Administrative Templates\ \Windows Components\NetMeeting\Audio&Video **Prevent sending Video**	Prevents users from sending video if they have the hardware. Users will still be able to receive video from others.	Enabled
User Configuration\Administrative Templates\ \Windows Components\Internet Explorer **Do not allow AutoComplete to save passwords**	Disables automatic completion of user names and passwords in forms on Web pages, and prevents users from being prompted to save passwords.	Enabled
User Configuration\Administrative Templates\ Start Menu & Taskbar **Disable and remove links to Windows Update**	Prevents users from connecting to the Windows Update Web site.	Enabled
User Configuration\Administrative Templates\Control Panel\Display **Password protect the screen saver**	Determines whether screen savers used on the computer are password protected. If you enable this policy, all screen savers are password protected. If you disable this policy, password protection cannot be set on any screen saver.	Enabled
User Configuration\Administrative Templates\Control Panel\Display **Screen Saver timeout**	Specifies how much user idle time must elapse before the screen saver is launched.	900 Seconds
User Configuration\Administrative Templates\System\Logon/Logoff **Run logon scripts synchronously**	Directs the system to wait for logon scripts to finish running before it starts the Windows Explorer interface program and creates the desktop. If you enable this policy, Windows Explorer does not start until the logon scripts have finished running. This setting assures that logon script processing is complete before the user starts working, but it can delay the appearance of the desktop.	Enabled

Security Policy Templates

Background

Security settings include Security Policies (account and local policies), access control (services, files, and registry), event log, group membership (restricted groups), Internet Protocol Security policies, and Public Key policies.

A *security template* is a physical representation of a security configuration

- Security configuration tools
- Security Templates snap-in – define and apply Security Templates
- Security Configuration and Analysis snap-in.- configure and analyze security locally
- Group Policy snap-in - configure security centrally in Active Directory
- Predefined Security Templates

A set of security templates is provided for common security scenarios. These can be assigned directly to a computer as is, or modified to suit unique security requirements. Predefined security templates should not be applied to production systems without testing to ensure that the right level of application functionality is maintained for your network and system architecture.

The predefined security templates are:

- Default workstation (basicwk.inf)
- Default server (basicsv.inf)
- Default domain controller (basicdc.inf)
- Compatible workstation or server (compatws.inf)
- Secure workstation or server (securews.inf)
- Highly secure workstation or server (hisecws.inf)
- Dedicated domain controller (dedicadc.inf)
- Secure domain controller (securedc.inf)
- Highly secure domain controller (hisecdc.inf)

By default, these templates are stored in the *systemroot*\security\templates folder. In addition to the predefined templates, a security analysis wizard can be used to evaluate the current local security settings against a desired configuration template.

Legacy Environment and Coexistence Considerations

Overview

Chesapeake Public Schools currently has a Novell Netware infrastructure deployed, and based on the discovered requirements, must be able to coexist with the Windows Infrastructure. Further, CPS has a variety of legacy applications and technologies that are mission critical in day to day operations that must be migrated to the new Active Directory environment as part of the migration process.

Applications

CPS currently employs several hundred applications for both student and faculty/administrative use. Of these, only a small number of applications require that a user log in. Most of these applications have a local user database that does not interface with the Novell LDAP directory (eDirectory). These applications are mostly hosted locally on servers located within each physical school or site. The majority of these will not be directly affected by the Windows Infrastructure migration. However, GroupWise 7, PeopleSoft, and Websense can communicate with Novell's directory for authentication purposes. These applications will require special consideration during the migration process. For instance, the GroupWise migration from Novell to a Windows platform is documented by Novell. The migration of these applications from Novell to Windows should be considered separate projects from the Active Directory Infrastructure build out, and should be completed during the coexistence phase of the Active Directory implementation. Each product's respective vendor should be consulted for guidance on the migration process.

All other applications are run as commands from the directories they reside in on the individual site servers. In order to ensure the least amount of user disruption, it is advised to migrate these applications simply by copying them from their respective Novell directories to a directory located on the local Windows server. This server can be the locally installed Read Only Domain Controller (RODC). After the file copy has happened, the drive letters to the applications should then be remapped via login script to the location on the Windows servers.

Migration

Migration from existing Netware servers to the new Microsoft infrastructure should be accomplished in a phased, site by site fashion.

Initially, after the directory synchronization and workstation domain join, new servers should be installed side by side with at all remote sites to serve as RODCs, DPs, and local file/print servers.

Next, all data, and applications should be copied to the new Microsoft servers. Upon successful data copy, filie shares should be created, permissions should be set, and scripts to map user and data drives should be developed.

Next printer objects should be created for each locally available printer.

Finally, all workstations should be configured by the created scripts to point to the new Microsoft services, and after a successful cool off period, the local Novell server should be decommissioned, and if possible, repurposed.

Depending on technical staff resources, a maximum of two sites per week, per team, should be possible.

Backups

Currently all user data resides locally on servers located at each physical site location. This data is backed up locally by locally at each location. During the coexistence period this should not be changed. However, at the time of this writing, Microsoft Office SharePoint Server is being considered as a collaboration and portal solution. It has been considered by CPS that all user data should be migrated into the proposed SharePoint solution. In the event that this does happen, there will be no further need for local backups at each site, as all user data would reside in the central SharePoint infrastructure, and all backups for SharePoint would be handled in a centralized manner.

Further, the current backup solution should be evaluated to determine if it is the best fit for Microsoft backups. With a new infrastructure, additional vendors should be evaluated as well to determine which solution best fits the needs of CPS.

For the Windows servers, to include Active Directory, all servers requiring backup should be located in the headquarters site, and the backups should be handled centrally. A centralized backup solution will require its own server infrastructure, and has its own design requirements. Products to consider include Symantec's Netbackup.

Antivirus

Currently no antivirus software is running locally on the workstations at CPS. Instead, all systems are running a product called "Deep Freeze" that allows for the machines to be rolled back to a known good state at startup. This configuration is not desirable for the new Active Directory environment. Even though it is possible to restore systems to a known good state, during the actual live operation of these systems, they are susceptible to security breaches due to their patch state, which can lead to infections and issues on systems that are not controlled through deep freeze, such as servers.

With this configuration, patches are not applied to workstations, so that they are susceptible to attacks that the patches protect against. Once a workstation is infected with a virus, even though it goes back to a known good state, it is possible for the workstation to cause damage to

other systems on the network, such as servers, that are not a part of the deep freeze deployment.

A centrally located and managed virus protection solution is recommended for both the workstations and servers in the new environment. Microsoft has released the Forefront product as a centralized virus solution. The Forefront product licensing is often included as part of an enterprise agreement. Other solutions from companies like AVG, Norton, and McAfee should also be considered to determine which solution fits the needs of CPS, both in terms of functionality and cost.

Dedicated servers will be required for any antivirus solution. Based on the size and scope of the CPS infrastructure, an enterprise rollout of Forefront Client Security should be considered. A minimum of four servers should be used. These servers will each host a single role. The four roles are the database role, the management server role, the collection server role, and the reporting server role.

The hardware requirements for these servers are as follows:

Database Server

- Dual Processor, Quad Core, 64 bit
- 16 GB RAM
- System Drive - 2 hard drives, 10k RPM, Minimum 100 GB, RAID 1
- Log Drives - 2 hard drives 15k RPM, 300 GB, RAID 0+1
- Database Drives - 5 Hard Drives, 15k RPM, 300 GB, RAID 5

Other Forefront Client Security Servers

- Dual Processor, Dual Core NIC
- 8 GB RAM
- 2 300 GB HDD, RAID 0+1
- 1 GB NIC

Systems Management

The only systems management solution in place currently is Novell's Zen product. Zen is only being used to facilitate group policy on the workstations. This is being done through the use of administrative registry templates being pushed down to workstations at logon. With the implementation of Active Directory, this functionality will no longer be required from Zen. As such, the Zen product will also no longer be required.

With the implementation of the Microsoft infrastructure, offerings from Microsoft's System Center solutions should be considered.

System Center Configuration Manager 2007 R2

Systems Center Configuration Manager (SCCM) should be considered for the purposes of systems management to include both servers and workstations. SCC M has been used to

significantly decrease the amount of time spent by administrators performing management tasks in their environment.

Some features in SCCM include

- Asset Intelligence - Configuration Manager 2007 gives organizations better control over their IT infrastructure and assets through asset intelligence technologies that provide IT administrators continuous visibility into what hardware and software assets they have, who is using them, and where they are.
- Desired Configuration Manager - With Configuration Manager 2007 Desired Configuration Management, organizations can ensure that IT systems comply with desired configuration states to improve systems availability, security, and performance network-wide.
- Software Update Management - Configuration Manager 2007 Software Update Management simplifies the complex task of delivering and managing updates to IT systems across the enterprise. IT administrators can deliver updates of Microsoft products, third-party applications, custom in-house line-of-business applications, hardware drivers, and system BIOS to a variety of devices—including to desktops, laptops, servers, and mobile devices.
- Software Distribution - Microsoft System Center Configuration Manager 2007 Software Distribution simplifies the complex task of distributing applications and updates to desktops, servers, laptops, and mobile devices across enterprise networks.
- Operating System Deployment - Microsoft System Center Configuration Manager 2007 Operating System Deployment is a highly flexible, automated solution that allows IT administrators to fully deploy and configure servers and desktops from any previous state, including bare-metal deployments.

Furthermore, any system running the SCCM client can be remote controlled by help desk staff, if desired. This can give the help desk staff direct console access to any workstation, eliminating the need for most destop visits and allowing for remote troubleshooting.
The design requirements and implementation steps of SCCM 2007 are beyond the scope of this document. Even so, the installation of a systems management solution should be considered crucial to the success of any Active Directory implementation.

Systems Center Operations Manager 2007

Monitoring the new Active Directory infrastructure should also be considered necessary in order to ensure the stable and consistent operation of all aspects of the Microsoft infrastructure. Microsoft has developed System Center Operations Manger (SCOM) in order to meet these requirements.

SCOM offers the following features:

- Delivers monitoring across Windows, Linux, and Unix servers through a single console.
- Assures the health and performance of Microsoft and non-Microsoft systems and workloads running on and across all platforms.

- Reports detailing IT operational performance and availability metrics for IT services provide rapid identification of where service levels are at risk, as well as the most likely cause of the potential drops in service.
- The interoperability connectors for System Center share and synchronize alerts and status between all management systems that may be in place.
- SCOM can perform automated tasks when certain event thresholds are hit. For instance, if a server's print spooler goes down, SCOM and run a script on the problem system to restart the spooler service without human intervention.

SCOM gives an organization the ability to act proactively rather than reactively to any problem situation that may develop, allowing for better service levels and reducing the workload on IT staff for dealing with issues.

Patch Management

At the time of this writing, there is no patch management infrastructure in place at CPS. It is recommended that an enterprise class patch management system be implemented as part of any Active Directory rollout.

Microsoft provides two possible solutions for patch management. These are the Windows Software Update Service (WSUS), and System Center Configuration Manager 2007 (SCCM). Both technologies will automate the delivery and installation of patches to workstations and servers enterprise wide.

WSUS leverages Active Directory to require that systems use the Windows Automatic Update to point to an internal WSUS server to download CPS approved patches on a set schedule. This technology relies on each individual workstation to pull down patches and does not offer any reporting of success or failure of patch installation.

SCCM, on the other hand, pushes patches to client systems using the same mechanism that it utilizes to distribute software. This allows for the ability to generate reports on patch success and failure, as well as the ability to remotely troubleshoot the cause for any patch installation failures. Also, since this is a push type technology, it can be considered the more reliable of the two available mechanisms.

Authentication

Users currently log into the Novell system in order to access network resources. During the coexistence period, it will be necessary to for users to authenticate both to Novell and Active Directory in order to access required resources. To facilitate this, both the Microsoft Client and the Novell client will be required on all workstations. This will be required until such a time as Novell is decommissioned.

Also, the current method of user creation and deletion is not in any way formalized. The person who currently is in charge of user management must rely on notification by administrator and other staff, and no formal or standardized mechanism is in place for that notification. This could be remediated via a SharePoint application or other method. This should be explored as part of any upcoming collaboration portal project.

Workstation Domain Membership

Workstations will be required to join the new Active Directory domain in order to access Microsoft resources. This can be achieved using the current login script technologies and with applications such as Netdom, which is part of the Windows operating system.

Firewall Port Requirements

Per CPS network staff, there are no firewalls between the central headquarter site on Battlefield Boulevard and the remote locations. All network traffic is handled by Cox communications. With the absence of any firewalling between the central site and the remote sites, the opening of required ports is not necessary. However, the security of any network traffic between sites cannot be guaranteed, due to the fact that it runs over public Internet (Cox). It is recommended, then, that all traffic on the network be encrypted, at least between the Domain Controllers and the RODCs located at the remote sites. Therefore, IPSec should be used for all domain controller traffic.

Should it be determined, contrary to findings, that ports are required to be opened, the following is a list of the ports that should be opened for DC to DC traffic.

Service	Port/protocol
RPC endpoint mapper	135/tcp, 135/udp
Network basic input/output system (NetBIOS) name service	137/tcp, 137/udp
NetBIOS datagram service	138/udp
NetBIOS session service	139/tcp
RPC dynamic assignment	1024-65535/tcp
Server message block (SMB) over IP (Microsoft-DS)	445/tcp, 445/udp
Lightweight Directory Access Protocol (LDAP)	389/tcp
LDAP ping	389/udp
LDAP over SSL	636/tcp
Global catalog LDAP	3268/tcp
Global catalog LDAP over SSL	3269/tcp
Kerberos	88/tcp, 88/udp
Domain Name Service (DNS)	53/tcp[1], 53/udp

Windows Internet Naming Service (WINS) resolution (if required)	1512/tcp, 1512/udp
WINS replication (if required)	42/tcp, 42/udp

Legacy Server Hardware

CPS currently has a minimum of two servers at each remote location. During the course of any decommissioning of legacy Novell hardware, these servers should be evaluated to determine if they meet the minimum recommendations for hardware to be repurposed as potential RODCs and/or distribution points for SCCM software distribution. RODCs should meet the minimum hardware specifications that are recommended for Windows 2008 servers.

The most current hardware available is HP's 4th generation (G4) hardware. This level of hardware is not recommended to act as an AD domain controller, but could be repurposed for use as RODCs or SCCM distribution points. G4 systems should have a minimum of 8GB of RAM, and if possible, multiple processors in order to meet the minimum hardware requirement for RODC/DP functionality.

Please note that Windows 2008 R2 requires 64 bit hardware, and that any hardware not supporting 64 bit operation cannot be considered for use in the Microsoft infrastructure.

Appendix A - Hardware Requirements

Windows 2008 Enterprise Edition Domain Controllers (5)

- Dual Processor, Quad Core 64 bit processors
- 8 GB RAM
- 300GB HDD
- 1 GB NIC

Windows 2008 Standard Edition Read Only Domain Controllers (47)

- Single Processor, Dual Core 64 bit processor
- 8GB RAM
- 300 GB HDD
- 1 GB NIC

Forefront Database Server (1)

- Dual Processor, Quad Core 64 bit processors
- 16 GB RAM
- 4 146 GB HDD
- 3 300GB HDD

All other Forefront Servers (3)

- Single Processor, Dual Core 64 bit processor
- 8GB RAM
- 300 GB HDD
- 1 GB NIC

Appendix B - Software Requirements

Domain Controllers (5)

Windows 2008 Enterprise Edition R2
Forefront Client Security Client
Backup Agent

Read Only Domain Controllers (47)

- Windows 2008 Standard Edition R2
- Forefront Client Security Client

Forefront Database Server (1)

- Windows 2008 Enterprise Edition R2
- SQL 2008 R2 Standard Edition
- Forefront Security for SQL
- Backup Agent

All other Forefront Roles (3)

- Windows 2008 Standard Edition R2
- Forefront Client Security Server

Appendix C – Applications Requiring Login

This section lists the application list provided by CPS that require user login

Desire 2 Learn – distance learning
Edline
- GradeQuick – gradebook
- Site Reporter – administrators use to view grades
- Edline – school/teacher homepages, provides parents access to grade reports

GroupWise 7
Manatee – bookkeeping system used by building level bookkeepers
Datastream 7i by Infor– work order and asset management system
IEP Online
Kronos 6 – time and attendance
PeopleSoft Financials 8.8 (soon to be version 9)
MediaCAST by Inventive Technologies – video distribution and control system
Discovery Ed Streaming (formerly United Streaming)
Websence – internet content filtering
SOLAR – benchmark testing (faculty & administrators only, students use generic login)
School Messenger (administrators and district) – Emergency notification system
Read 180 / System 44 by Scholastic – reading intervention program
SAM 2000 – pretesting software for Certiport exams
Orchard – math / English software
Exam View – testing software issued with textbooks
Type 2 Learn – elementary keyboarding
Knowledge Box by Pearson Digital – used at 2 primary schools only
SuccessMaker by Pearson Digital – used at 3 elementary level schools only
Equitrac Print Management Software - Login used at the copier