System i

Security
Network authentication service

Version 5 Release 4

System i

Security
Network authentication service

Version 5 Release 4

Note

Before using this information and the product it supports, read the information in "Notices," on page 129.

Sixth Edition (February 2006)

This edition applies to version 5, release 4, modification 0 of IBM i5/OS (product number 5722–SS1) and to all subsequent releases and modifications until otherwise indicated in new editions. This version does not run on all reduced instruction set computer (RISC) models nor does it run on CISC models.

Contents

Chapter 1. Network authentication service

Network authentication service allows the System i™ product and several System i services, such as iSeries™ eServer™ Access for Windows®, to use a Kerberos ticket as an optional replacement for a user name and password for authentication.

The Kerberos protocol, developed by Massachusetts Institute of Technology, allows a principal (a user or service) to prove its identity to another service within an unsecure network. Authentication of principals is completed through a centralized server called a Kerberos server or key distribution center (KDC).

Note: Throughout this documentation, the generic term *Kerberos server* is used.

A user is authenticated with a principal and a password that is stored in the Kerberos server. After a principal is authenticated, the Kerberos server issues a ticket-granting ticket (TGT) to the user. When a user needs access to an application or a service on the network, the Kerberos client application on the user's PC sends the TGT back to the Kerberos server to obtain a service ticket for the target service or application. The Kerberos client application then sends the service ticket to the service or application for authentication. When the service or application accepts the ticket, a security context is established and the user's application can then exchange data with a target service. Applications can authenticate a user and securely forward his or her identity to other services on the network. When a user is known, separate functions are needed to verify the user's authorization to use the network resources.

Network authentication service implements the following specifications:

- Kerberos Version 5 protocol Request for Comment (RFC) 1510
- Many of the de facto standard Kerberos protocol application programming interfaces (APIs) prevalent in the industry today
- Generic Security Service (GSS) APIs as defined by RFCs 1509, 1964, and 2743

The i5/OS® implementation of network authentication service operates with authentication, delegation, and data confidentiality services compliant with these RFCs and Microsoft's Windows 2000 Security Service Provider Interface (SSPI) APIs. Microsoft® Windows Active Directory uses Kerberos as its default security mechanism. When users are added to Microsoft Windows Active Directory, their Windows identification is equivalent to a Kerberos principal. Network authentication service provides for interoperability with Microsoft Windows Active Directory and its implementation of the Kerberos protocol.

What's new for V5R4

This topic highlights changes to network authentication service for V5R4.

Network Authentication Enablement Product

In V5R3, the network authentication server shipped with the Cryptographic Access Provider (5722-AC3). In V5R4, the 5722-AC3 product has become part of the base release. In V5R4, the Kerberos network authentication server ships as a separate product, *Network Authentication Enablement* (5722-NAE). Network Authentication Enablement is included with the i5/OS CD.

You need to install Network Authentication Enablement before you can configure a Kerberos server in i5/OS Portable Application Solutions Environment (PASE).

- "Configuring a Kerberos server in i5/OS PASE" on page 89
- "Scenario: Setting up a Kerberos server in i5/OS PASE" on page 12

Simplified Kerberos Configuration in i5/OS PASE

The procedure for configuring a secondary Kerberos server has been simplified.

- "Configuring a secondary Kerberos server" on page 91

Network authentication service commands

This topic contains more reference information about using commands to configure, run, and use network authentication service.

- "Network authentication service commands" on page 122
- Related information

How to see what's new or changed

To help you see where technical changes have been made, this information uses:

- The » image to mark where new or changed information begins.
- The « image to mark where new or changed information ends.

To find other information about what's new or changed this release, see the Memo to users.

Printable PDF

Use this to view and print a PDF of this information.

To view or download the PDF version of this document, select Network authentication service (about 1717 KB).

You can view or download these related topics:

- Single sign-on (600 KB) contains the following topics:
  - Scenarios that show how network authentication service can be used with Enterprise Identity Mapping (EIM) to provide single sign-on in an enterprise.
  - Conceptual information that explains single sign-on and its benefits.
- Enterprise Identity Mapping (EIM) (800 KB) contains the following topics:
  - Scenarios that show common implementations of EIM.
  - Conceptual and planning information that will help you understand and plan for EIM.

Other information

You can find this documentation in the AIX 5L™ Expansion Pack and Bonus Pack CD, or in the *Network Authentication Enablement* CD:

- Manuals:
  - *IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide*.
  - *IBM Network Authentication Service AIX, Linux, and Solaris Application Development Reference*.

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF in your browser (right-click the link above).
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html)  .

Concepts

Network authentication service supports Kerberos protocols and Generic Security Service (GSS) APIs that provide user authentication in a network.

Information regarding Kerberos protocols and GSS APIs exists in multiple sources, so this topic explains the basics as they specifically apply to your System i environment.

Network authentication service terminology

Network authentication service uses these Kerberos protocol terms.

forwardable tickets
Forwardable tickets allow a server to pass on the credentials of the requester to another service. For this to happen, the initial TGT must have been requested with the forwardable option and the server is allowed to delegate credentials.

Kerberos server or key distribution center (KDC)
A network service that provides tickets and temporary session keys. The Kerberos server maintains a database of principals (users and services) and their associated secret keys. It is composed of the authentication server and the ticket-granting server. The authentication server issues ticket-granting tickets, while the ticket-granting server issues service tickets. It is important that you use a secure machine to act as your Kerberos server. If someone gained access to the Kerberos server, your entire realm might be compromised.

key table
A file on the service's host system. Each entry in the file contains the service principal's name and secret key. On the System i platform, a key table file is created during configuration of network authentication service. When a service requests authentication to a System i platform with network authentication service configured, the operating system checks the key table file for that service's credentials. To ensure that users and services are authenticated properly, you must have users and services created on the Kerberos server and on i5/OS. Entries are added to the key table during the processing of the Network Authentication Service wizard. You can also add entries to the key table by using the keytab command from within the Qshell Interpreter in a character-based interface.

Note: This Domain Name System (DNS) name must be the same as the host name defined on the machine. For more information about how DNS and Kerberos work together, see "Host name resolution considerations" on page 80.

password server
Allows clients (principals) to change their password on the Kerberos server remotely. The password server typically runs on the same machine as the Kerberos server.

principal
The name of a user or service in a Kerberos realm. A user is considered a person where a service is used to identify a specific application or set of operating system services. On the i5/OS operating system, the **krbsvr400** service principal is used to identify the service used by iSeries Access for Windows, QFileSrv.400, and Telnet servers, when authenticating from the client to the System i platform.

proxiable tickets
A proxiable ticket is a ticket-granting ticket (TGT) that allows you to get a ticket for a service with IP addresses other than those in the TGT. Unlike forwardable tickets, you cannot transfer a

new TGT from your current TGT; you can only transfer service tickets. Forwardable tickets let you transfer your complete identity (TGT) to another machine, where proxiable tickets only let you transfer particular tickets. Proxiable tickets allow a service to perform a task on behalf of a principal. The service must be able to take on the identity of the principal for a particular purpose. A proxiable ticket tells the Kerberos server that it can issue a new ticket to a different network address, based on the original ticket-granting ticket. With proxiable tickets, a password is not required.

realm A set of users and servers for which a given Kerberos server is the authenticating authority.

realm trust
The Kerberos protocol either searches the configuration file, such as **krb5.conf**, to determine realm trust or by default looks for trust relationships within the realm hierarchy. Using **Trusted realms** in network authentication service allows you to bypass this process and creates a shortcut for authentication. Realm trust can be used in networks where realms are in different domains. For example, if a company has one realm at NY.MYCO.COM and another at LA.MYCO.COM, then you can establish trust between these two realms. If two realms trust each other, their associated Kerberos servers must share a key. Before creating a shortcut, you must set up the Kerberos servers to trust each other.

renewable tickets
In some cases, an application or a service might want to have tickets that are valid for an extended period of time. However, the extended time might allow someone to steal these credentials, which are valid until the ticket expires. Renewable tickets allow for applications to obtain tickets that are valid for extended periods. Renewable tickets contain two expiration times. The first expiration applies to the current instance of the ticket and the second time applies to the latest permissible expiration for the ticket.

service ticket
A ticket that authenticates a principal to a service.

ticket-granting service (TGS)
A service provided by the Kerberos server that issues service tickets.

ticket-granting ticket (TGT)
A ticket that allows access to the ticket-granting service on the Kerberos server. Ticket-granting tickets are passed to the principal by the Kerberos server after the principal has completed a successful request to the authentication server. In a Windows 2000 environment, when a user logs on to the network, the Kerberos server verifies the principal's name and encrypted password and then sends a ticket-granting ticket to the user. From a System i platform, users can request a ticket using the kinit command within the Qshell Interpreter in the character-based interface.

How does network authentication service work?

The System i product can act as a server or a client in the Kerberos network. It is important to understand the authentication processes and the tickets flow in both of these situations.

The Kerberos protocol provides an authentication method for users and services on your network. As a network administrator, you can configure network authentication service so your System i platform will accept Kerberos tickets as a form of authentication. The System i product and several system-specific applications act as a client/server within a Kerberos network, requesting tickets for users and for services for authentication. The Kerberos protocol provides users and services a means to prove their identities (authenticate) to an entire network, but it does not authorize them to resources on that network. Specific authorization to i5/OS functions is maintained through user profiles that are created on i5/OS.

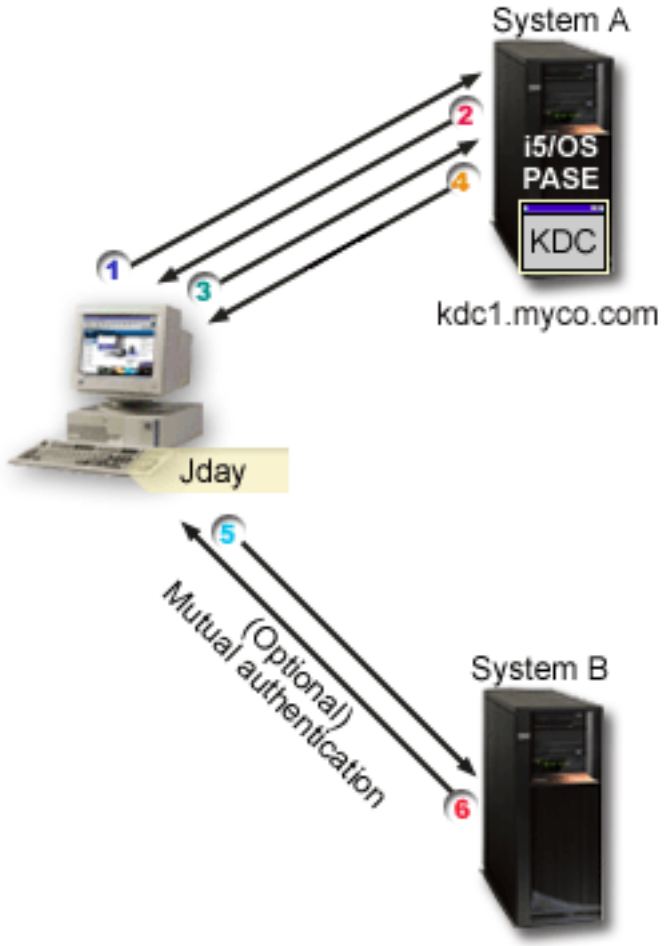
When a user is authenticated using Kerberos, that user is issued an initial ticket, called a ticket-granting ticket (TGT). The user can then use the TGT to request a service ticket to access other services and applications on the network. For authentication to work successfully, an administrator must register the users, i5/OS service principals, and applications that use Kerberos protocol with the Kerberos server. The

System i product can act either as a server, where principals request authentication to services, or it can act as a client requesting tickets for applications and services on the network. The following graphics show how tickets flow in both of these situations.

System i product as a server

This graphic shows how authentication works when a System i product acts as a server in a Kerberos network. In this graphic, the Kerberos server or key distribution center (KDC) located in i5/OS PASE issues tickets to the principal, jday.

The principal jday wants to access an application on System A. In this case, Enterprise Identity Mapping (EIM) is used on the system to map the Kerberos principal to an i5/OS user profile. This is done for any System i function that supports Kerberos authentication, such as IBM® eServer iSeries Access for Windows.



This description provides an overview of how this authentication process works within a network:

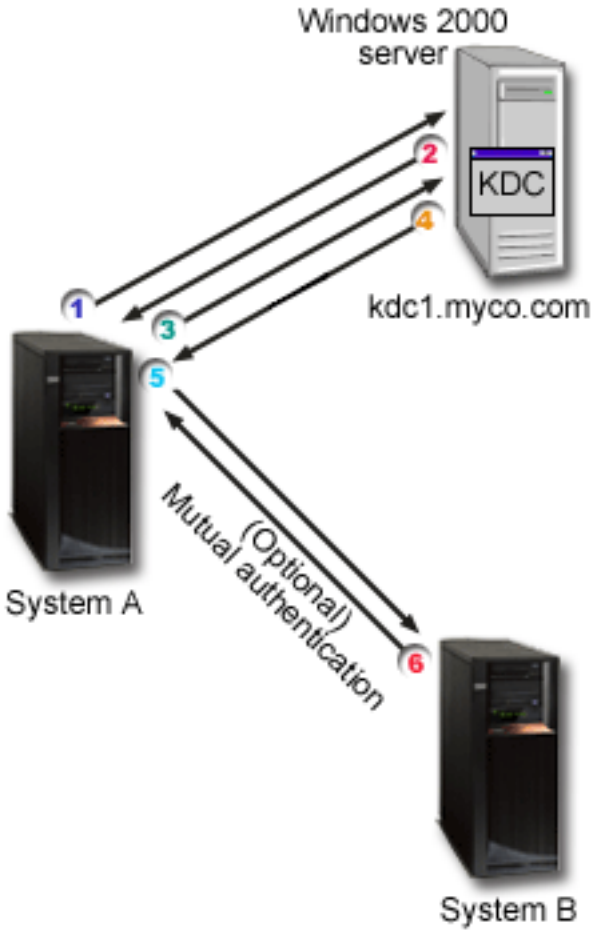
1. The user, jday, authenticates to the Kerberos server by providing a principal and password when he signs into the Kerberos realm. This sends a request to the Kerberos server for a ticket-granting ticket (TGT).
2. The Kerberos server validates his principal name and password and sends a TGT to jday.
3. Jday needs access to an application on the System i platform. The Kerberos client application on jday's PC sends his TGT to the Kerberos server to request a service ticket for the specific application or service, such as iSeries Navigator. The user's workstation manages his credentials cache, which holds tickets and other identifying information for the user. These credentials are

read from the cache as they are needed and new credentials are stored in the cache as they are obtained. This relieves the application of the responsibility for managing the credentials itself.

4. The Kerberos server responds with the service ticket.
5. The application sends the service ticket to the System i service to authenticate the user.
6. The server application validates the ticket by calling the network authentication service APIs and optionally can send a response back to the client for mutual authentication.
7. Using an EIM association, the Kerberos principal is then mapped to the i5/OS user profile.

System i product as a client

This graphic shows how authentication works when a System i product acts as a client in a Kerberos network. In this graphic, the Kerberos server, which is located on the Windows 2000 server, issues tickets to the user who authenticated to Kerberos. System A can be authenticated to other services. In this example, EIM is used on System B to map the Kerberos principal to a user profile. This is done for any System i function that supports Kerberos authentication, such as QFileSvr.400.



This description provides an overview of how this authentication process works within a network:

1. A principal, jday signs in to System A and then requests a ticket-granting ticket by performing a kinit command in the Qshell Interpreter. The system sends this request to the Kerberos server.
2. The Kerberos server validates his principal name and password and sends a ticket-granting ticket to jday.
3. Jday needs access to an application on System B. By calling the Network Authentication Service APIs, the application sends jday's TGT to the Kerberos server to request a service ticket for the

specific application or service. The principal's local machine manages a credentials cache, which holds tickets, session keys, and other identifying information for the user. These credentials are read from the cache as they are needed and new credentials are stored in the cache as they are obtained. This relieves the application of the responsibility for managing the credentials itself.

4. The Kerberos server responds with the service ticket.

   Note: A service principal for System B needs to be added to the Kerberos server and network authentication service must also be configured on System B.
5. The application sends the server ticket to the System i service to authenticate the user.
6. The server application validates the ticket by calling the network authentication service APIs and optionally can send a response back to the client for mutual authentication.
7. Using EIM association, the Kerberos principal is then mapped to the i5/OS user profile.

Network authentication service protocols

Network authentication service uses the Kerberos protocol in conjunction with Generic Security Services (GSS) APIs for authentication to provide authentication and security services.

This topic provides a general description of the network authentication service protocols and how they are used in the System i environment. For more complete information about these standards, links have been provided to the associated Request for Comments standards and other external sources.

Kerberos protocol

The Kerberos protocol provides third-party authentication where users prove their identities to a centralized server, called a Kerberos server or key distribution center (KDC), which issues tickets to the users. The users can then use these tickets to prove their identities on the network. The ticket eliminates the need for multiple sign-ons to different systems. The Network Authentication Service APIs that the System i environment supports originated from Massachusetts Institute of Technology and have become the de facto standard for using the Kerberos protocol.

Security environment assumptions

The Kerberos protocol assumes that all data exchanges occur in an environment where packets can be inserted, changed, or intercepted at will. Use Kerberos as one layer of an overall security plan. Although the Kerberos protocol allows you to authenticate users and applications across your network, you should be aware of some limitations when you define your network security objectives:

- The Kerberos protocol does not protect against denial-of-service attacks. There are places in these protocols where an intruder can prevent an application from participating in the correct authentication steps. Detection and solution of such attacks are typically best left to human administrators and users.
- Key sharing or key theft can allow impersonation attacks. If intruders somehow steal a principal's key, they will be able to masquerade as that user or service. To limit this threat, prohibit users from sharing their keys and document this policy in your security regulations.
- The Kerberos protocol does not protect against typical password vulnerabilities, such as password guessing. If a user chooses a poor password, an attacker might successfully mount an offline dictionary attack by repeatedly attempting to decrypt messages that are encrypted under a key derived from the user's password.

Kerberos sources

Requests for Comments (RFCs) are written definitions of protocol standards and proposed standards used for the Internet. The following RFCs might be helpful for understanding the Kerberos protocol:

RFC 1510
In RFC 1510: The Kerberos Network Authentication Service (V5), the Internet Engineering Task Force (IETF) formally defines Kerberos Network Authentication Service (V5).

To view the RFC listed, visit the RFC index search engine located on the RFC editor Web site. Search for the RFC number you want to view. The search engine results display the corresponding RFC title, author, date, and status.

Kerberos: The Network Authentication Protocol (V5)
Massachusetts Institute of Technology's official documentation of the Kerberos protocol provides programming information and describes features of the protocol.

Generic Security Services (GSS) APIs

Generic Security Service Application Programming Interfaces (GSS APIs) provide security services generically and are supported by a range of security technologies, like the Kerberos protocol. This allows GSS applications to be ported to different environments. Because of this reason, it is recommended that you use these APIs instead of Kerberos APIs. You can write applications that use GSS APIs to communicate with other applications and clients in the same network. Each of the communicating applications plays a role in this exchange. Using GSS APIs, applications can perform the following operations:

- Determine another application's user identification.
- Delegate access rights to another application.
- Apply security services, such as confidentiality and integrity, on a per-message basis.

GSS API sources

Requests for Comments (RFCs) are written definitions of protocol standards and proposed standards used for the Internet. The following RFCs might be helpful for understanding the GSS APIs:

RFC 2743
In RFC 2743: Generic Security Service Application Program Interface Version 2, Update 1, the Internet Engineering Task Force (IETF) formally defines GSS APIs.

RFC 1509
In RFC 1509: Generic Security Service API : C-bindings, the Internet Engineering Task Force (IETF) formally defines GSS APIs.

RFC 1964
In RFC 1964, The Kerberos Version 5 GSS-API Mechanism, the Internet Engineering Task Force (IETF) defines Kerberos Version 5 and GSS API specifications.

To view the RFCs listed, visit the RFC index search engine located on the RFC editor Web site. Search for the RFC number you want to view. The search engine results display the corresponding RFC title, author, date, and status.

Network authentication service environment variables

You can use environment variables with network authentication service to affect how Generic Security Services (GSS) APIs and the Kerberos protocol APIs perform.

You can use environment variables to change the configuration and to manage the network authentication service on your network. The i5/OS operating system supports multiple ways to work with environment variables.

CL commands

- ADDENVVAR
- CHGENVVAR
- RMVENVVAR
- WRKENVVAR

For an example of using environment variables using the CL command, ADDENVVAR, see "API trace tool" on page 120. This set of environment variables allows you to create a log file that traces each of the Kerberos and GSS API calls. The API trace tool allows you to troubleshoot more advanced problems involving your Kerberos-enabled applications, problems that can occur during network authentication service configuration, and problems that can occur during Kerberos ticket requests.

C APIs

- getenv()
- putenv()

For descriptions and examples of these APIs, see the usage notes on the getenv() and the putenv() APIs.

Qshell commands

- export -s env_var_name=value

In addition, you can define an environment variable file (envar file) containing entries of the **form** environment_variable=value. Any variables defined through the Qshell environment or with the CL commands override the same variables in the envar file. The _EUV_ENVAR_FILE environment variable can be used to specify the location of the file containing these entries.

_EUV_ENVAR_FILE

The name of the file that contains environment variable definitions. If this variable is not set, the default is to use the envar file located in the home directory (as specified by the _EUV_HOME or HOME environment variable).

Each line of the file consists of the variable name followed by an equal sign (=) followed by the variable value with no intervening blanks or other punctuation. The variable value consists of everything following the equal sign up to the end of the line (including any embedded and trailing blanks). Any line beginning with a pound sign (#) is treated as a comment line. You can continue a line by ending it with a backward slash (\). No trailing blanks can follow the backward slash. The `_EUV_` must begin in column 1.

Environment variables are not set until the first time that a function in the security run time is invoked. Thus, it is mainly useful for setting environment variables that will be used by functions within the security run time, although it can be used to set environment variables that will be used by the application as well. In this case, the application should not rely on the environment variable values until after the security run time has been initialized. The user profile under which this program runs must have *X authority to each directory in the path preceding this file, and *R authority to this file.

_EUV_HOME and HOME

The security runtime home directory is set to the value of the _EUV_HOME environment variable. If this variable is not specified, the HOME variable is used to determine the security runtime home directory. If neither environment variable is set, the home directory that is configured in the currently running user profile is used. If the home directory does not exist, the current working directory is used. Limit public access to this directory to *EXCLUDE or *R.

_EUV_SEC_KRB5CCNAME_FILE

The name of the file used to locate the default Kerberos credentials cache. If this variable is not set, the default is to use the krb5ccname file located in the security runtime home directory. The running user profile must have *X authority to each directory in the path name preceding this file. If the file does not yet exist, the running user profile must have *WX authority to the parent

directory that contains this file. The user must ensure that public access to the parent directory is limited to prevent a malicious user from changing the credentials cache file that is used.

_EUV_SVC_MSG_LOGGING
The target where messages are logged. The following values are valid:

NO_LOGGING
Suppress all messages. This is the default.

STDOUT_LOGGING
Write all messages (informational and error) to stdout, and write error messages to stderr.

STDERR_LOGGING
Write informational messages to stdout and error messages to stderr.

_EUV_SVC_MSG_LEVEL
The message level when logging messages. Messages that do not meet this criterion are suppressed. The default is to log all messages. The following values are valid:

FATAL
Only unrecoverable messages are logged.

ERROR
Only unrecoverable and error messages are logged.

USER Only unrecoverable, error, and user messages are logged.

WARNING
Only unrecoverable, error, user, and warning messages are logged.

NOTICE
Only unrecoverable, error, user, warning, and notice messages are logged.

VERBOSE
All messages are logged.

_EUV_SVC_STDOUT_FILENAME
The fully qualified name of the file to receive standard output messages. If this environment variable is not defined, messages are written to stdout. The currently running user profile must have *X authority to each directory in the path preceding this file and *WX authority to the parent directory that contains this file.

_EUV_SVC_STDERR_FILENAME
The fully qualified name of the file to receive standard error messages. If this environment variable is not defined, messages are written to stderr. The currently running user profile must have *X authority to each directory in the path preceding this file and *WX authority to the parent directory that contains this file.

_EUV_SVC_DBG_MSG_LOGGING
Whether debug messages are generated. The default is to suppress debug messages. Logging of debug messages should not be enabled unless requested by IBM service, as it can severely affect performance. The following values are valid:

- 0 Suppress debug messages
- 1 Write debug messages

_EUV_SVC_DBG

The subcomponents and levels for the debug messages. Debug messages for a particular subcomponent are not logged unless the subcomponent is included in the _EUV_SVC_DBG list and the debug message level is greater than or equal to the specified level. Use an asterisk (*) to specify all subcomponents.

The subcomponent list consists of a subcomponent name and a debug level separated by a period. You can specify multiple subcomponents by separating the entries with commas. For

example, _EUV_SVC_DBG=*.1,KRB_CCACHE.8 enables debug level 1 for all subcomponents and debug level 8 for the KRB_CCACHE subcomponent. You can specify the following subcomponents:

- KRB_API
- KRB_GENERAL
- KRB_CCACHE
- KRB_RCACHE
- KRB_CRYPTO
- KRB_GSSAPI
- KRB_KEYTAB
- KRB_LIB
- KRB_ASN1
- KRB_OS
- KRB_KDC
- KRB_KDB
- KRB_KUT

_EUV_SVC_DBG_FILENAME
The fully qualified name of the file to receive debug messages. If this environment variable is not defined, debug messages are written to the file specified by the _EUV_SVC_STDOUT_FILENAME. If _EUV_SVC_STDOUT_FILENAME is not specified, then debug messages are written to stdout. The currently running user profile must have *X authority to each directory in the path preceding this file and *WX authority to the parent directory that contains this file.

KRB5_CONFIG
One or more configuration file names separated by colons. The default configuration file is /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf. The currently running user profile must have *X authority to each directory in the path preceding these configuration files and *R authority to the configuration files.

KRB5CCNAME
The default name for the credentials cache file, which is specified as type:name. The supported types are FILE and MEMORY. The default is to perform FILE-based credentials caching in the /QIBM/UserData/OS400/NetworkAuthentication/creds directory. If the default is used, no authority setup is needed. If a FILE-based credentials cache file is specified, then the currently running user profile must have *X authority to each directory in the path. It must have *WX authority to the parent directory when the cache file is first created and *RW authority to the cache file. If the cache file is being deleted, it must have *OBJEXIST authority to the cache file.

KRB5_KTNAME
The default key table name. If not specified, the file specified by the default_keytab_name configuration entry in the configuration file is used. If the configuration entry is not specified, the default file is /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab. The user profile that is currently running must have *X authority to each directory in the path. If the file is being created, it must also have *WX authority to the parent directory. If the file is being updated, it must have *RW authority to the file. Specific authorities that are needed are documented under the Qshell commands and the runtime APIs.

KRB5RCACHETYPE
The default replay cache type. It defaults to dfl.

KRB5RCACHENAME
The default replay cache name. If not specified, the Kerberos run time generates a name.

KRB5RCACHEDIR
The default replay cache directory. It defaults to /QIBM/UserData/OS400/NetworkAuthentication/replay.

Scenarios: Using network authentication service in a Kerberos network

These are common scenarios where you use network authentication service to allow the i5/OS operating system to participate in a Kerberos network.

Scenario: Setting up a Kerberos server in i5/OS PASE

Here are the goals, objectives, prerequisites, and configuration steps for setting up a Kerberos server.

Situation

You are an administrator that manages security for a medium-sized network for your company. You want to authenticate users from a central system. You have decided to create a Kerberos server that will authenticate users to resources across your entire enterprise. You have researched many options for implementing a Kerberos solution on your network. You know that Windows 2000 server uses Kerberos to authenticate users to a Windows domain; however, this adds additional costs to your small IT budget. Instead of using a Windows 2000 domain to authenticate users, you have decided to configure a Kerberos server in your System i environment in the i5/OS Portable Application Solutions Environment (PASE). i5/OS PASE provides an integrated runtime environment for AIX® applications. You want to use the flexibility of i5/OS PASE to configure your own Kerberos server. You want the Kerberos server in i5/OS PASE to authenticate users in your network, who use Windows 2000 and Windows XP workstations.

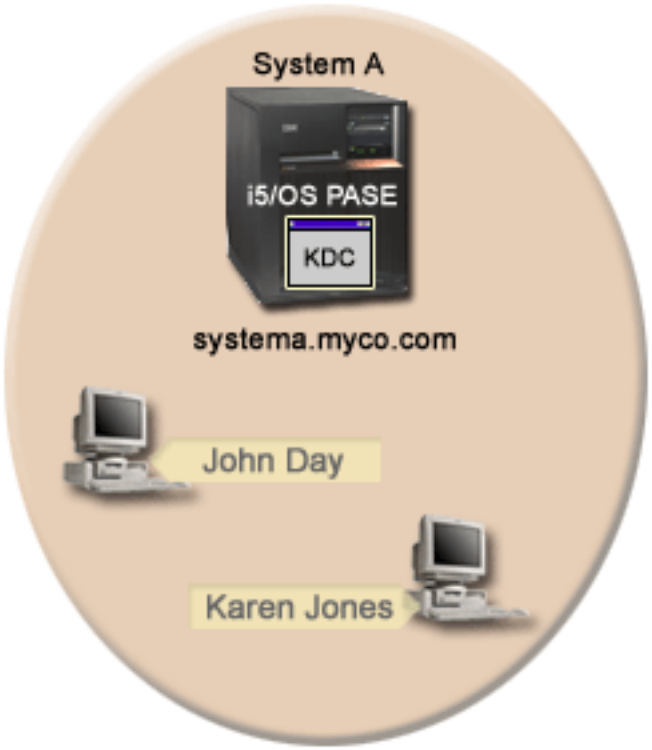
Objectives

In this scenario, MyCo, Inc. wants to establish a Kerberos server in i5/OS PASE by completing the following objectives:

- To configure a Kerberos server in the i5/OS PASE environment
- To add network users to a Kerberos server
- To configure workstations that run Windows 2000 operating system to participate in the Kerberos realm configured in i5/OS PASE
- To configure network authentication service on System A
- To test authentication in your network

Details

The following figure illustrates the network environment for this scenario.



System A

- Acts as the Kerberos server (kdc1.myco.com), also known as a key distribution center (KDC), for the network.
- Runs i5/OS Version 5 Release 3 (V5R3) or later with the following options and licensed programs installed:
  - i5/OS Host Servers (5722-SS1 Option 12)
  - i5/OS PASE (5722-SS1 Option 33)
  - Qshell Interpreter (5722-SS1 Option 30)
  - Network Authentication Enablement (5722-NAE) if you are running V5R4, or later
  - Cryptographic Access Provider (5722-AC3) if you are running V5R3
  - iSeries Access for Windows (5722-XE1)
- Has the fully qualified host name of systema.myco.com.

Client PCs

- **For all PCs in this scenario:**
  - Run Windows 2000 and Windows XP operating systems.
  - Windows 2000 Support Tools (which provides the ksetup command) installed.
- **For administrator's PC:**
  - iSeries Access for Windows (5722-XE1) installed.
  - iSeries Navigator with Security and Network subcomponents installed.

Prerequisites and assumptions

This scenario focuses on the tasks that involve configuring a Kerberos server in i5/OS PASE.

1. All system requirements, including software and operating system installation, have been verified.
   To verify that the required licensed programs have been installed, follow these steps:
   a. In iSeries Navigator, expand *your system* → **Configuration and Service** → **Software** → **Installed Products**.
   b. Ensure that all the necessary licensed programs are installed.
2. All necessary hardware planning and setup have been completed.
3. TCP/IP connections have been configured and tested on your network.
4. A single DNS server is used for host name resolution for the network. Host tables are not used for host name resolution.

   Note: The use of host tables with Kerberos authentication might result in name resolution errors or other problems. For more detailed information about how host name resolution works with Kerberos authentication, see "Host name resolution considerations" on page 80.

Configuration steps

To configure a Kerberos server in i5/OS PASE and to configure network authentication service, complete these steps.

Completing the planning work sheets

Before configuring the Kerberos server and network authentication service in i5/OS PASE, complete these planning work sheets.

All answers on the prerequisite sheet should be `Yes` before you proceed with network authentication service setup.

Table 1. Prerequisite planning work sheet

Questions	Answers
Is your i5/OS V5R3, or later (5722-SS1)?	Yes
Are the following options and licensed programs installed on System A: • i5/OS Host Servers (5722-SS1 Option 12) • i5/OS PASE (5722-SS1 Option 33) • Qshell Interpreter (5722-SS1 Option 30) • Network Authentication Enablement (5722-NAE) if you are using V5R4, or later • Cryptographic Access Provider (5722-AC3) if you are running i5/OS V5R3 • iSeries Access for Windows (5722-XE1)	Yes
Have you installed Windows 2000 or Windows XP on all of your PCs?	Yes
Have you installed Windows 2000 Support Tools (which provides the ksetup command) on all of your PCs?	Yes
Is iSeries Access for Windows (5722-XE1) installed on the administrator's PC?	Yes
Have you installed iSeries Navigator on the administrator's PC? • Is the Security subcomponent of iSeries Navigator installed on the administrator's PC? • Is the Network subcomponent of iSeries Navigator installed on the administrator's PC?	Yes Yes Yes
Have you installed the latest iSeries Access for Windows service pack? See iSeries Access for the latest service pack.	Yes

Table 1. Prerequisite planning work sheet (continued)

Questions	Answers
Do you have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities? You must have these special authorities to use the Network Authentication Service wizard for this scenario.	Yes
Do you have your DNS configured and do you have the correct host names for your System i product and Kerberos server?	Yes
On which operating system do you want to configure the Kerberos server? 1. Windows 2000 Server 2. Windows Server 2003 3. AIX Server 4. i5/OS PASE (V5R3, or later) 5. z/OS®	i5/OS PASE
Have you applied the latest program temporary fixes (PTFs)?	Yes
Is the System i system time within five minutes of the Kerberos server's system time? If not, see "Synchronizing system times" on page 99.	Yes

For this scenario, you must specify a number of different passwords. The following planning worksheet provides a list of the passwords you need to use for this scenario. Refer to this table as you perform the configuration steps for setting up the Kerberos server in i5/OS PASE.

Table 2. Password planning work sheet

Entity	Password
i5/OS PASE administrator: admin/admin **Note:** i5/OS PASE specifies `admin/admin` as the default user name for the administrator.	secret
i5/OS PASE Database Master	pasepwd
Windows 2000 workstations: • pc1.myco.com (John Day's PC) • pc2.myco.com (Karen Jones' PC)	secret1 secret2
Kerberos user principals: • day@MYCO.COM • jones@MYCO.COM	123day 123jones
i5/OS service principal for System A: krbsvr400/systema.myco.com@MYCO.COM	systema123

The following planning work sheet illustrates the type of information you need before you begin configuring the Kerberos server in i5/OS PASE and network authentication service. All answers on the prerequisite work sheet and password planning work sheet should be answered before you proceed with configuring the Kerberos server in i5/OS PASE.

Table 3. Planning work sheet for configuring a Kerberos server in i5/OS PASE and configuring network authentication service

Questions	Answers
What is the name of the Kerberos default realm?	MYCO.COM
Is this default realm located on Microsoft Active Directory?	No

Table 3. Planning work sheet for configuring a Kerberos server in i5/OS PASE and configuring network authentication service (continued)

Questions	Answers
What is the Kerberos server, also known as a key distribution center (KDC), for this Kerberos default realm? What is the port on which the Kerberos server listens?	**KDC:** kdc1.myco.com **Port:** 88 **Note:** This is the default port for the Kerberos server.
Do you want to configure a password server for this default realm?	No **Note:** Currently password servers are not supported by i5/OS PASE or AIX.
For which services do you want to create keytab entries? • i5/OS Kerberos Authentication • LDAP • iSeries IBM HTTP Server • iSeries NetServer™	i5/OS Kerberos Authentication
Do you want to create a batch file to automate adding the service principals to Microsoft Active Directory?	Not applicable
What is the default user name for the i5/OS PASE administrator? What is the password you want to specify for the i5/OS PASE administrator?	User name: admin/admin Password: secret
What is the naming convention for your principals that represent users in your network?	Principals that represent users will be lowercase family name followed by the uppercase realm name
What are the Kerberos user principal names for these users: • John Day • Karen Jones	day@MYCO.COM jones@MYCO.COM
What are the i5/OS user profile names for these users: • John Day • Karen Jones	JOHND KARENJ
What are the Windows 2000 user names for these users: • John Day • Karen Jones	johnday karenjones
What are the host names for these Windows 2000 workstations: • John Day's PC • Karen Jones' PC	pc1.myco.com pc2.myco.com
What is the name of the i5/OS service principal for System A?	krbsvr400/systema.myco.com@MYCO.COM **Note:** The name of this service principal is for example purposes only. In your configuration, specify the host name and domain of your i5/OS in the name of the service principal.

Configuring Kerberos server in i5/OS PASE

To configure a Kerberos server on i5/OS PASE on System A, use the information from your planning work sheets.

Follow these steps to configure a Kerberos server on i5/OS PASE:

1. In a character-based interface, enter `call QP2TERM`. This command opens an interactive shell environment that allows you to work with i5/OS PASE applications.

2. At the command line, enter `export PATH=$PATH:/usr/krb5/sbin`. This command points to the Kerberos scripts that are necessary to run the executable files.
3. At the command line, enter `config.krb5 -S -d myco.com -r MYCO.COM`, where `-d` is the DNS of your network and `-r` is the realm name. (In this example, myco.com is the DNS name and MYCO.COM is the realm name.) This command updates the krb5.config file with the domain name and realm for the Kerberos server, creates the Kerberos database within the integrated file system, and configures the Kerberos server in i5/OS PASE. You will be prompted to add the following passwords:
   - database Master Password: `pasepwd`
   - admin/admin principal password: `secret`
4. Press F3 (Exit) to exit the PASE environment.

Changing encryption values on i5/OS PASE Kerberos server

To operate with Windows workstations, you need to change the default encryption settings on the Kerberos server so that clients can be authenticated to the i5/OS PASE Kerberos server.

To change the default encryption settings, you need to edit the kdc.conf file located in the /etc/krb5 directory by following these steps:

1. In a character-based interface, enter `edtf '/var/krb5/krb5kdc/kdc.conf'` to access the kdc.conf file.
2. Change the following lines in the kdc.conf file:

```
| supported_enctypes = des3-cbc-sha1:normal
| arcfour-hmac:normal aes256-cts:normal
| des-cbc-md5:normal des-cbc-crc:normal
```

   to

```
| supported_enctypes = des-cbc-crc:normal dec-cbc-md5:normal
```

Stopping and restarting Kerberos server in i5/OS PASE

You must stop and restart the Kerberos server in i5/OS PASE to update the encryption values that you just changed.

Complete the following steps to stop and restart the Kerberos server:

1. In a character-based interface, enter `call QP2TERM` at the command line. This command opens an interactive shell environment that allows you to work with i5/OS PASE applications.
2. At the command line, enter `export PATH=$PATH:/usr/krb5/sbin`. This command points to the Kerberos scripts that are necessary to run the executable files.
3. At the command line, enter `stop.krb5`. This command stops the Kerberos server.
4. At the command line, enter `start.krb5`. This command starts the Kerberos server.

Creating host principals for Windows 2000 and Windows XP workstations

You must create the host principals that Kerberos uses to authenticate the PC users.

If you are already in i5/OS PASE, skip steps 1 and 2. Complete these steps to create the host principals for the workstations:

1. In a character-based interface, enter `call QP2TERM` at the command line. This command opens an interactive shell environment that allows you to work with i5/OS PASE applications.
2. At the command line, enter `export PATH=$PATH:/usr/krb5/sbin`. This command points to the Kerberos scripts that are necessary to run the executable files.
3. At the command line, enter `kadmin -p admin/admin`, and press Enter.
4. Sign in with administrator's password. For example, `secret`.
5. At the kadmin prompt, enter `addprinc -pw secret1 host/pc1.myco.com`. This creates a host principal for John Day's PC.

6. At the kadmin prompt, enter `addprinc -pw secret2 host/pc2.myco.com`. This creates a host principal for Karen Jones' PC.
7. Enter `quit` to exit the kadmin interface.

Creating user principals on the Kerberos server

For users to be authenticated to services in your network, you must add them to the Kerberos server as principals.

A principal is the Kerberos term for a user name and password. These principals are stored on the Kerberos server and are used to validate users in the network. Complete the following steps to create user principals:

1. In a character-based interface, type `call QP2TERM` at the command line. This command opens an interactive shell environment that allows you to work with i5/OS PASE applications.
2. At the command line, enter `export PATH=$PATH:/usr/krb5/sbin`. This command points to the Kerberos scripts that are necessary to run the executable files.
3. At the command line, enter `kadmin -p admin/admin`, and press Enter.
4. Sign in with administrator's password. For example, `secret`.
5. At the kadmin prompt, enter `addprinc -pw 123day day`.

After you complete these steps, you will receive a message that reads:

```
Principal "day@MYCO.COM" created.
```

This creates the user principal for John Day.

Repeat these steps for Karen Jones, but specify `jones` for the principal name and `123jones` for the password.

Adding System A service principal to the Kerberos server

For i5/OS interfaces to accept Kerberos tickets, you must add them to the Kerberos server as principals.

Complete the following steps to add the service principal. If you are already in the kadmin environment, skip steps 1 through 4.

1. In a character-based interface, type `call QP2TERM` at the command line. This command opens an interactive shell environment that allows you to work with i5/OS PASE applications.
2. At the command line, enter `export PATH=$PATH:/usr/krb5/sbin`. This command points to the Kerberos scripts that are necessary to run the executable files.
3. At the command line, enter `kadmin -p admin/admin`, and press Enter.
4. Sign in with administrator's password. For example, `secret`.
5. At the kadmin prompt, enter `addprinc -pw systema123 krbsvr400/systema.myco.com`. You will receive a message that reads:

   ```
   Principal "krbsvr400/systema.myco.com@MYCO.COM" created.
   ```
6. Enter `quit` to exit the kadmin interface, and press F3 (Exit) to exit the PASE environment.

Configuring Windows 2000 and Windows XP workstations

This step is optional for configuring a Kerberos server in i5/OS PASE. If you intend to create a single sign-on environment after configuring the Kerberos server, you must complete this step. If not, skip to Step 9 (Configuring network authentication service).

Configure the client workstations as part of a workgroup by setting the Kerberos realm and Kerberos server on the workstation. You also need to set a password that is associated with the workstation.

Note: All passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

To configure the workstations, complete these steps:

1. From a command prompt on the Windows 2000 workstation, enter:

```
C:> ksetup /setdomain MYCO.COM
C:> ksetup /addkdc MYCO.COM kdc1.myco.com
```

2. Set the local machine account password by entering this at the Windows 2000 workstation command prompt:

```
C:> ksetup /setmachpassword secret1
```

3. Map John Day's Kerberos user principal (day@MYCO.COM) to his Windows 2000 user name (johnday). Enter this at the Windows 2000 workstation command prompt:

```
C:> ksetup /mapuser day@MYCO.COM johnday
```

4. To verify that John Day's Kerberos user principal maps to his Windows 2000 user name, enter this at the Windows 2000 workstation command prompt:

```
C:> ksetup
```

   and view the results.
5. Restart the PC for the changes to take effect.
6. Repeat these steps for Karen Jones' workstation, but specify the following information:
   - Local machine account password: `secret2`
   - Kerberos user principal: `jones@MYCO.COM`
   - Windows 2000 user name: `karenjones`

   Related concepts

   Scenario: Creating a single sign-on test environment

Configuring network authentication service

To configure network authentication service, complete these steps.

1. In iSeries Navigator, expand **System A** → **Security**.
2. Right-click **Network Authentication Service** and select **Configure** to start the configuration wizard.

   Note: After you have configured network authentication service, this option will be **Reconfigure**.
3. Review the Welcome page for information about what objects the wizard creates. Click **Next**.
4. On the Specify realm information page, enter `MYCO.COM` in the **Default realm** field. Click **Next**.
5. On the Specify KDC information page, enter `kdc1.myco.com` for the Kerberos server in the **KDC** field and enter 88 in the **Port** field. Click **Next**.
6. On the Specify password information page, select **No**. Click **Next**.
7. On the Select keytab entries page, select **i5/OS Kerberos Authentication**. Click **Next**.
8. On the Create i5/OS keytab entry page, enter and confirm a password, and click **Next**. For example, `systema123`. This password will be used when System A is added to the Kerberos server.
9. On the Summary page, review the network authentication service configuration details. Click **Finish**.

Creating a home directory for users on System A

Each user that connects to the i5/OS operating system and i5/OS applications needs a directory in the /home directory. This directory contains the name of the user's Kerberos credentials cache.

To create a home directory for the users on System A, follow these steps:

1. On the i5/OS command line, enter `CRTDIR '/home/user profile'` where `user profile` is the i5/OS user profile name for the user. For example: `CRTDIR '/home/JOHND'` for the user John Day.
2. Repeat this command for Karen Jones, but specify her i5/OS user profile, `KARENJ`.

Testing network authentication service

To test the network authentication service configuration, request a ticket-granting ticket for your i5/OS principal and other principals within your network.

Note: Be sure you have created a home directory for your i5/OS user profile before performing this test.

To test the network authentication service configuration, follow these steps:

1. On a command line, enter `QSH` to start the Qshell Interpreter.
2. Enter `keytab list` to display a list of principals registered in the keytab file. The following results should display:

```
Principal: krbsvr400/systema.myco.com@MYCO.COM
  Key version: 2
  Key type: 56-bit DES using key derivation
  Entry timestamp: 200X/05/29-11:02:58
```

3. Enter `kinit -k krbsvr400/systema.myco.com@MYCO.COM` to request a ticket-granting ticket from the Kerberos server. This command verifies that your system has been configured properly and the password in the keytab file matches the password stored on the Kerberos server. If this is successful, the QSH command displays without errors.
4. Enter `klist` to verify that the default principal is krbsvr400/systema.myco.com@MYCO.COM. This command displays the contents of a Kerberos credentials cache and verifies that a valid ticket has been created for the i5/OS service principal and placed within the credentials cache on the system.

```
 Ticket cache: FILE:/QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/creds/krbcred

 Default principal: krbsvr400/systema.myco.com@MYCO.COM

Server: krbtgt/MYCO.COM@MYCO.COM
  Valid 200X/06/09-12:08:45 to 20XX/11/05-03:08:45
$
```

You have completed the steps required to configure your system to be a Kerberos server and you can use Kerberos to authenticate the users in the MYCO.COM realm.

Scenario: Configuring network authentication service

Here are the prerequisites and objectives of adding network authentication service to your network.

Situation

You are a network administrator that manages the network for the order receiving department in your company. You recently added a System i product to your network to contain several applications for your department. In your network, you manage users with Microsoft Windows Active Directory on a Microsoft Windows 2000 server. Currently all of your users have workstations that run Microsoft Windows 2000 operating system. You have your own Kerberos-enabled applications that use Generic Security Services (GSS) APIs.

This scenario has the following advantages:

- Simplifies authentication process for users
- Eases the overhead of managing access to systems in the network
- Minimizes threat of password theft

Objectives

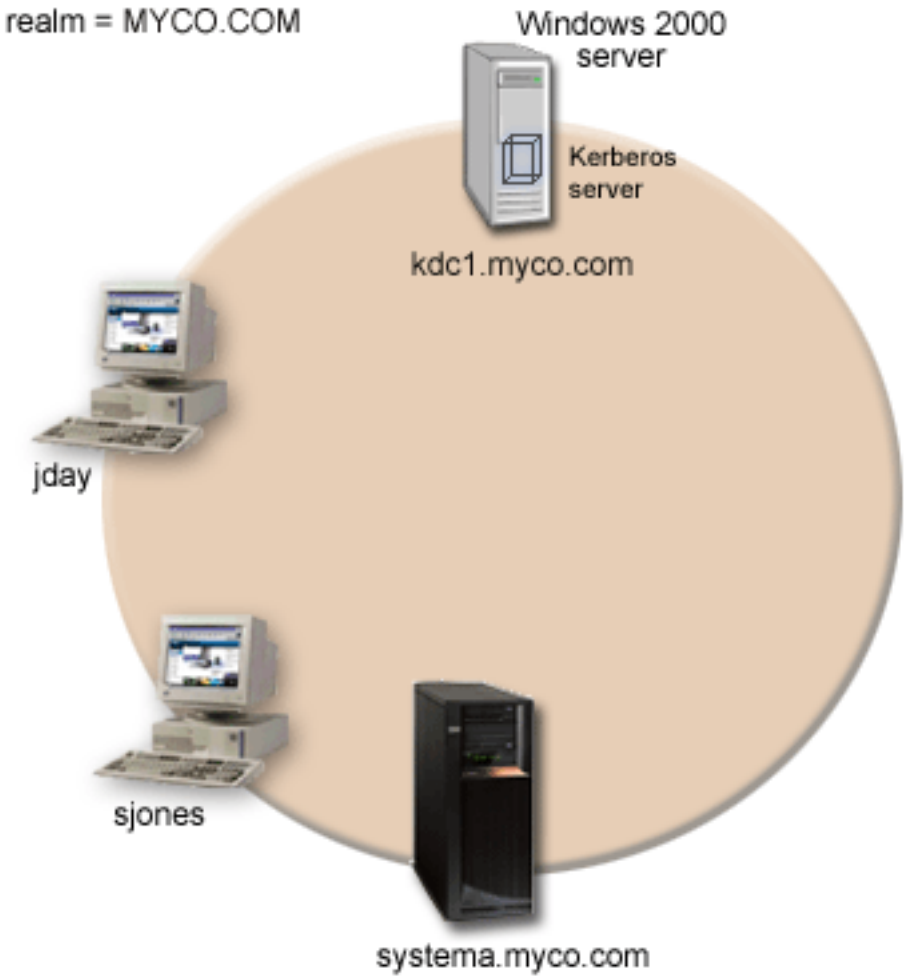
In this scenario, MyCo, Inc. wants to add a System i product to an existing realm where a Windows 2000 server acts as the Kerberos server. The System i platform contains several business critical applications that need to be accessed by the correct users. Users need to be authenticated by the Kerberos server to gain access to these applications.

The objectives of this scenario are as follows:

- To allow the System i platform to participate with an existing Kerberos server
- To allow for both principal names and user names in the network
- To allow Kerberos users to change their own passwords on the Kerberos server

Details

The following figure illustrates the network characteristics of MyCo.



System A

- Runs i5/OS V5R3, or later, with the following options and licensed programs installed:
  - i5/OS Host Servers (5722-SS1 Option 12)
  - Qshell Interpreter (5722-SS1 Option 30)
  - iSeries Access for Windows (5722-XE1)
  - Network Authentication Enablement (5722-NAE) if you are using V5R4, or later
  - Cryptographic Access Provider (5722-AC3) if you are running V5R3
- The principal name of System A is krbsvr400/systema.myco.com@MYCO.COM.

Windows 2000 server

- Acts as the Kerberos server for the MYCO.COM realm.
- The fully qualified host name of the Kerberos server is kdc1.myco.com.

Client PCs

- Run Windows 2000.
- PC used to administer network authentication service has the following products installed:
  - iSeries Access for Windows (5722-XE1)
  - iSeries Navigator and the Security and Network subcomponents

Prerequisites and assumptions

1. All system requirements, including software and operating system installation, have been verified.
   To verify that the required licensed programs have been installed, follow these steps:
   a. In iSeries Navigator, expand *your system* → **Configuration and Service** → **Software** → **Installed Products**.
   b. Ensure that all the necessary licensed programs are installed.
2. All necessary hardware planning and setup have been completed.
3. TCP/IP and basic system security have been configured and tested on each of these servers.
4. A single DNS server is used for host name resolution for the network. Host tables are not used for host name resolution.

   Note: The use of host tables with Kerberos authentication might result in name resolution errors or other problems. For more detailed information about how host name resolution works with Kerberos authentication, see "Host name resolution considerations" on page 80.

Configuration steps

To configure network authentication service on your system, complete these steps.

Completing the planning work sheets

Before configuring network authentication service, complete these planning work sheets.

All answers on the prerequisite work sheet should be `Yes` before you proceed with network authentication service setup.

Table 4. Prerequisite work sheet

Questions	Answers
Is your i5/OS V5R3, or later (5722-SS1)?	Yes
Are the following licensed programs installed on System A: • i5/OS Host Servers (5722-SS1 Option 12) • Qshell Interpreter (5722-SS1 Option 30) • iSeries Access for Windows (5722-XE1) • Network Authentication Enablement (5722-NAE) if you are using i5/OS V5R4, or later • Cryptographic Access Provider (5722-AC3) if you are running i5/OS V5R3	Yes
Have you installed Windows 2000 on your PCs?	Yes
Is iSeries Access for Windows (5722-XE1) installed on the administrator's PC?	Yes
Have you installed iSeries Navigator on the administrator's PC? • Is the Security subcomponent of iSeries Navigator installed on the administrator's PC? • Is the Network subcomponent of iSeries Navigator installed on the administrator's PC?	Yes Yes Yes
Have you installed the latest iSeries Access for Windows service pack? See iSeries Access for the latest service pack.	Yes

Table 4. Prerequisite work sheet (continued)

Questions	Answers
Do you have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities?	Yes
Do you have one of the following installed on the secure system that will act as a Kerberos server? If so, which one? 1. Windows 2000 Server 2. Windows Server 2003 3. AIX Server 4. i5/OS PASE (V5R3 or later) 5. z/OS	Yes, Windows 2000 Server
Are all your PCs in your network configured in a Windows 2000 domain? **Note:** A Windows 2000 domain is similar to a Kerberos realm. Microsoft Active Directory uses Kerberos authentication as its default security mechanism.	Yes
Have you applied the latest program temporary fixes (PTFs)?	Yes
Is the System i system time within five minutes of the Kerberos server's system time? If not, see "Synchronizing system times" on page 99.	Yes

Table 5. Network authentication service planning work sheet

Questions	Answers
What is the name of the Kerberos default realm to which your system will belong? **Note:** A Windows 2000 domain is similar to a Kerberos realm. Microsoft Active Directory uses Kerberos authentication as its default security mechanism.	MYCO.COM
Are you using Microsoft Active Directory?	Yes
What is the Kerberos server for this Kerberos default realm? What is the port on which the Kerberos server listens?	**KDC:** kdc1.myco.com **Port:** 88 **Note:** This is the default port for the Kerberos server.
Do you want to configure a password server for this default realm? If yes, answer the following questions: What is name of the password server for this Kerberos server? What is the port on which the password server listens?	Yes **Password server:**kdc1.myco.com **Port:** 464 **Note:** This is the default port for the password server.
For which services do you want to create keytab entries? • i5/OS Kerberos Authentication • LDAP • iSeries IBM HTTP Server • iSeries NetServer	i5/OS Kerberos Authentication
What is the password that you want to use for your i5/OS service principals? **Note:** All passwords used within this scenario are for example purposes only. They should not be used during an actual configuration.	systema123
Do you want to create a batch file to automate adding the service principals to Microsoft Active Directory?	Yes
What are the i5/OS user profiles names for John Day and Sharon Jones?	JOHND SHARONJ

Configuring network authentication service on System A

To configure network authentication service, follow these steps.

1. In iSeries Navigator, expand **System A** → **Security**.
2. Right-click **Network Authentication Service** and select **Configure** to start the configuration wizard.

   Note: After you have configured network authentication service, this option will be **Reconfigure**.
3. Review the Welcome page for information about what objects the wizard creates. Click **Next**.
4. On the Specify realm information page, enter `MYCO.COM` in the **Default realm** field and select **Microsoft Active Directory is used for Kerberos authentication**. Click **Next**.
5. On the Specify KDC information page, enter `kdc1.myco.com` for the Kerberos server in the **KDC** field and enter 88 in the **Port** field. Click **Next**.
6. On the Specify password information page, select **Yes**. Enter `kdc1.myco.com` in the **Password server** field and `464` in the **Port** field. Click **Next**.
7. On the Select keytab entries page, select **i5/OS Kerberos Authentication**. Click **Next**.
8. On the Create i5/OS keytab entry page, enter and confirm a password. For example, `systema123`. This password will be used when System A is added to the Kerberos server. Click **Next**.
9. Optional: On the Create batch file page, select **Yes** to create this file, and specify the following information:
   - **Batch file:** Add the text `systema` to the end of the default batch file name. For example: `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystema.bat`
   - Select **Include password**. This ensures that all passwords associated with the i5/OS service principal are included in the batch file. It is important to note that passwords are displayed in clear text and can be read by anyone with read access to the batch file. Therefore, it is recommended that you delete the batch file from the Kerberos server and from your PC immediately after use.

     Note: Alternatively, you can add service principals that are generated by the wizard manually to the Kerberos server. If you want to know how to manually add the i5/OS service principal to the Kerberos server, see "Adding i5/OS principals to the Kerberos server" on page 95.
10. On the Summary page, review the network authentication service configuration details. Click **Finish**.

Adding System A principal to the Kerberos server

You can manually add the i5/OS service principal to the Kerberos server. As this scenario illustrates, you can also use the batch file you created in Step 2 to add the principal.

To use the batch file, you must use File Transfer Protocol (FTP) to copy it to the Kerberos server and run it. Follow these steps to use the batch file to add the principal to the Kerberos server:

1. FTP batch file created by the wizard
   a. On the Windows 2000 workstation that the administrator used to configure network authentication service, open a command prompt and type `ftp kdc1.myco.com`. This will start an FTP session on your PC. You will be prompted for the administrator's user name and password.
   b. At the FTP prompt, type `lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access"`. Press Enter. You should receive the message `Local directory now C:\Documents and Settings\All Users\Documents\IBM\Client Access`.
   c. At the FTP prompt, type `binary`. This indicates that the file to be transferred is binary.
   d. At the FTP prompt, type `cd \mydirectory`, where *mydirectory* is a directory located on kdc1.myco.com.
   e. At the FTP prompt, type `put NASConfigsystema.bat`. You should receive this message: `226 Transfer complete`.
2. Run batch file on kdc1.myco.com
   a. On your Windows 2000 server, open the folder where you transferred the batch files.

b. Find the NASConfigsystema.bat file and double-click the file to run it.
c. After the file runs, verify that the i5/OS principal has been added to the Kerberos server by completing the following steps:
   1) On your Windows 2000 server, expand **Start → Programs → Administrative Tools → Active Directory Users and Computers → Users**.
   2) Verify that the system has a user account by selecting the appropriate Windows domain.

      Note: This Windows domain should be the same as the default realm name that you specified for the network authentication service configuration.
   3) In the list of users that is displayed, find **systema_1_krbsvr400**. This is the user account generated for the i5/OS principal name.
   4) **Optional:** Access the properties on your Active Directory users. From the **Account** tab, select the **Account is trusted for delegation**.

      Note: This optional step enables your system to delegate or forward a user's credentials to other systems. As a result, the i5/OS service principal can access services on multiple systems on behalf of the user. This is useful in a multi-tier network.

Creating a home directory for users on System A

Each user that connects to i5/OS and i5/OS applications needs a directory in the /home directory. This directory contains the name of the user's Kerberos credentials cache.

To create a home directory for a user, follow these steps:

1. On the i5/OS command line, enter: `CRTDIR '/home/user profile'` where `user profile` is the i5/OS user profile name for the user. For example, `CRTDIR '/home/JOHND'` for the user John Day.
2. Repeat this command for Sharon Jones, but specify her i5/OS user profile, `SHARONJ`.

Testing network authentication service on System A

To verify that you have configured network authentication service correctly, request a ticket-granting ticket for System A principal.

To test the network authentication service, follow these steps:

1. On a command line, enter `QSH` to start the Qshell Interpreter.
2. Enter `keytab list` to display a list of principals registered in the keytab file. The following results should display:

```
Principal: krbsvr400/systema.myc.com@MYCO.COM
  Key version: 2
  Key type: 56-bit DES using key derivation
  Entry timestamp: 200X/05/29-11:02:58
```

3. Enter `kinit -k krbsvr400/systema.myco.com@MYCO.COM` to request a ticket-granting ticket from the Kerberos server. This command verifies that your system has been configured properly and the password in the keytab file matches the password stored on the Kerberos server. If this is successful, the QSH command displays without errors.
4. Enter `klist` to verify that the default principal is krbsvr400/systema.myco.com@MYCO.COM. This command displays the contents of a Kerberos credentials cache and verifies that a valid ticket has been created for the i5/OS service principal and placed within the credentials cache on the system.

```
 Ticket cache: FILE:/QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/creds/krbcred

 Default principal: krbsvr400/systema.myco.com@MYCO.COM

Server: krbtgt/MYCO.COM@MYCO.COM
  Valid 200X/06/09-12:08:45 to 20XX/11/05-03:08:45
$
```

You have completed the tasks required to configure network authentication service on System A.

Scenario: Setting up cross-realm trust

Here are the prerequisites and objectives for setting up cross-realm trust on your network.

Situation

You are a security administrator for a large wholesale company. Currently you manage security for systems used by employees of the Order Receiving Department and the Shipping Department. You have configured a Kerberos server for the Order Receiving Department. You have configured network authentication service in the System i environment in that department to point to that Kerberos server. The Shipping Department consists of a System i product that has a Kerberos server configured in i5/OS PASE. You have also configured network authentication service on this System i product to point to the Kerberos server in i5/OS PASE.

Because users in both realms need to use services stored on systems located in each department, you want both of the Kerberos servers in each department to authenticate users regardless of which Kerberos realm they are located in.

Objectives

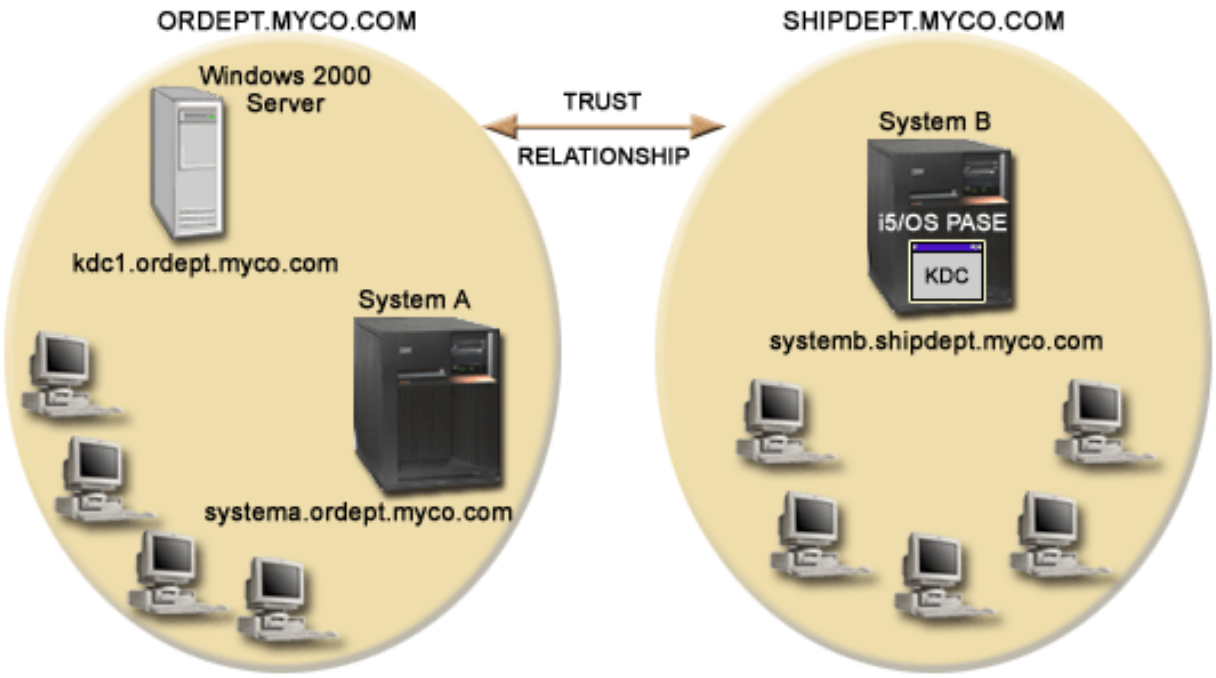
In this scenario, MyCo, Inc. wants to establish a trust relationship between two existing Kerberos realms. One realm consists of a Windows 2000 server acting as the Kerberos server for the Order Receiving Department. This server authenticates users within that department to services located on a System i platform. The other realm consists of a Kerberos server configured in i5/OS PASE on one System i platform, which provides services for the users within the Shipping Department. Your users need to be authenticated to services in both departments.

The objectives of this scenario are as follows:

- To give clients and hosts on each network access to the other's network
- To simplify authentication across networks
- To allow ticket delegation for users and services in both networks

Details

Here is a detailed description of the environment that this scenario describes, including a figure that shows the topology and all major elements of that environment and how they relate to each other.



Order Receiving Department

System A

- Runs i5/OS V5R3, or later, with the following options and licensed programs installed:
  - i5/OS Host Servers (5722-SS1 Option 12)
  - iSeries Access for Windows (5722-XE1)
  - Network Authentication Enablement (5722-NAE) if you are using i5/OS V5R4, or later
  - Cryptographic Access Provider (5722-AC3) if you are running i5/OS V5R3
- Has network authentication service configured to participate in the realm ORDEPT.MYCO.COM. The i5/OS principal, krbsrv400/systema.ordept.myco.com@ORDEPT.MYCO.COM, has been added to the Windows 2000 domain.
- System A has the fully qualified host name of systema.ordept.myco.com.

Windows 2000 server

- Acts as the Kerberos server for the realm, ORDEPT.MYCO.COM.
- Has the DNS host name of kdc1.ordept.myco.com.
- Each user within the Order Department has been defined in Microsoft Active Directory on the Windows 2000 server with a principal name and password.

Client PCs

- Run Windows 2000 operating system.
- PC used to administer network authentication service has the following products installed:
  - iSeries Access for Windows (5722-XE1)
  - iSeries Navigator and the following subcomponents:
    - Security
    - Network

Shipping Department

System B

- Runs i5/OS V5R3 with the following options and licensed programs installed:
  - i5/OS PASE (5722 SS1 Option 33)
  - Cryptographic Access Provider (5722-AC3)
  - iSeries Access for Windows (5722-XE1)
- Has a Kerberos server configured in i5/OS PASE with the realm of SHIPDEPT.MYCO.COM.
- Has network authentication service configured to participate in the realm SHIPDEPT.MYCO.COM. The i5/OS principal, krbsrv400/systemb.shipdept.myco.com@SHIPDEPT.MYCO.COM, has been added to the i5/OS PASE Kerberos server.
- Both System B and the i5/OS PASE Kerberos server share the fully qualified host name systemb.shipdept.myco.com.
- Each user within the Shipping Department has been defined in the i5/OS PASE Kerberos server with a principal name and password.

Client PCs

- Run Windows 2000 operating system.
- PC used to administer network authentication service has the following products installed:
  - iSeries Access for Windows (5722-XE1)
  - iSeries Navigator and the following subcomponents:
    - Security
    - Network

Prerequisites and assumptions

In this scenario, the following assumptions have been made to focus on the tasks that involve establishing a trust relationship between two pre-existing Kerberos realms.

System A prerequisites

1. All system requirements, including software and operating system installation, have been verified.

   To verify that the required licensed programs have been installed, follow these steps:

   a. In iSeries Navigator, expand *your system* → **Configuration and Service** → **Software** → **Installed Products**.

   b. Ensure that all the necessary licensed programs are installed.
2. All necessary hardware planning and setup have been completed.
3. TCP/IP and basic system security have been configured and tested on System A.
4. Network authentication service has been configured and tested.
5. A single DNS server is used for host name resolution for the network. Host tables are not used for host name resolution.

   Note: The use of host tables with Kerberos authentication might result in name resolution errors or other problems. For more detailed information about how host name resolution works with Kerberos authentication, see "Host name resolution considerations" on page 80.

System B prerequisites

1. All system requirements, including software and operating system installation, have been verified.

   To verify that the required licensed programs have been installed, follow these steps:

   a. In iSeries Navigator, expand *your system* → **Configuration and Service** → **Software** → **Installed Products**.

   b. Ensure that all the necessary licensed programs are installed.

2. All necessary hardware planning and setup have been completed.
3. TCP/IP and basic system security have been configured and tested on your system.
4. Network authentication service has been configured and tested.

Windows 2000 server prerequisites

1. All necessary hardware planning and setup have been completed.
2. TCP/IP has been configured and tested on your server.
3. Microsoft Active Directory has been configured and tested.
4. Each user within the Order Department has been defined in Microsoft Active Directory with a principal name and password.

Configuration steps

To set up a trust relationship between two realms, complete these steps.

Completing the planning work sheets

Before setting up cross-realm trust, complete these planning work sheets.

All answers on the prerequisite work sheet should be `Yes` before you proceed with setting up cross-realm trust.

Table 6. Prerequisite planning work sheet

Questions	Answers
Is your i5/OS V5R3, or later (5722-SS1)?	Yes
Are the following options and licensed programs installed on System A: • i5/OS Host Servers (5722-SS1 Option 12) • iSeries Access for Windows (5722-XE1) • Network Authentication Enablement (5722-NAE) if you are using i5/OS V5R4, or later • Cryptographic Access Provider (5722-AC3) if you are running i5/OS V5R3	Yes
Are the following licensed programs installed on System B: • iSeries Access for Windows (5722-XE1) • Network Authentication Enablement (5722-NAE) if you are using i5/OS V5R4, or later • Cryptographic Access Provider (5722-AC3) if you are running i5/OS V5R3 • i5/OS PASE (5722-SS1 Option 33)	Yes
Have you installed Windows 2000 on all of your PCs?	Yes
Is iSeries Access for Windows (5722-XE1) installed on the PC used to administer network authentication service?	Yes
Have you installed iSeries Navigator and the following subcomponents on the PC used to administer network authentication service? • Security • Network	Yes
Have you installed the latest iSeries Access for Windows service pack? See iSeries Access for the latest service pack.	Yes
Do you have *ALLOBJ special authority on the systems?	Yes
Do you have administrative authorities on the Windows 2000 server?	Yes
Do you have your DNS configured and do you have the correct host names for your System i platform and Kerberos server?	Yes

Table 6. Prerequisite planning work sheet (continued)

Questions	Answers
On which operating system do you want to configure the Kerberos server? 1. Windows 2000 Server 2. Windows Server 2003 3. AIX Server 4. i5/OS PASE (V5R3 or later) 5. z/OS	i5/OS PASE
Have you applied the latest program temporary fixes (PTFs)?	Yes
Is the System i system time within five minutes of the Kerberos server's system time? If not, see "Synchronizing system times" on page 99.	Yes

The following planning work sheet illustrates the type of information you need before you begin setting up cross-realm trust.

Table 7. Planning work sheet for cross-realm trust

Planning work sheet for cross-realm trust	Answers
What are the names of the realms for which you want to establish a trusted relationship? • The Kerberos realm using the Windows 2000 server as its Kerberos server • The Kerberos realm using System B as its Kerberos server (configured in i5/OS PASE)	ORDEPT.MYCO.COM SHIPDEPT.MYCO.COM
Have all i5/OS service principals and user principals been added to their respective Kerberos servers?	Yes
What is the default user name for the i5/OS PASE administrator? What is the password you want to specify for the i5/OS PASE administrator? **Note:** This must be the same password you used when you created the Kerberos server in i5/OS PASE.	User name: admin/admin Password: secret
What are the names of the principals that will be used to set up cross realm trust? What is the password for each of these principals?	Principal: krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM Password: shipord1 Principal: krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO .COM Password: shipord2
What are the fully qualified host names for each of the Kerberos servers for these realms? • ORDEPT.MYCO.COM • SHIPDEPT.MYCO.COM	kdc1.ordept.myco.com systemb.shipdept.myco.com
Are the system times for all systems within five minutes of one another? If not, see "Synchronizing system times" on page 99.	Yes

Ensuring that the Kerberos server in i5/OS PASE on System B has started

Before you configure cross-realm trust, you need to ensure that the i5/OS PASE Kerberos server has started.

Use the process statistics command to determine whether the i5/OS PASE Kerberos server has started.

1. In a character-based interface on System B, type `call QP2TERM`. This command opens an interactive shell environment in which you can work with i5/OS PASE applications.
2. At the command line, enter `ps -ef | grep krb5`. This command indicates that you want to view all the processing statistics for every process on the system that contains the string krb5. If the Kerberos server is running, you might see results displayed that are similar to the following example:

```
> ps -ef | grep krb5
     qsys   113   1   0 08:54:04      -  0:00 /usr/krb5/sbin/krb5kdc
     qsys   123   1   0 08:54:13      -  0:00 /usr/krb5/sbin/kadmind
   $
```

   If the Kerberos server is not started, you might see the following results displayed:

```
> ps -ef | grep krb5
   $
```

3. If the Kerberos server is not started, follow these steps:
   a. At the command line, enter `export PATH=$PATH:/usr/krb5/sbin`, and press Enter.
   b. Enter `start.krb5`, and press Enter.

```
> start.krb5
  Starting krb5kdc...
  krb5kdc was started successfully.
  Starting kadmind...
  kadmind was started successfully.
  The command completed successfully.
  $
```

Creating a cross-realm trust principal on the i5/OS PASE Kerberos server

To create a cross-realm trust principal on the i5/OS PASE Kerberos server, follow these steps.

1. In a character-based interface, type `call QP2TERM`. This command opens an interactive shell environment that allows you to work with i5/OS PASE applications.
2. At the command line, enter `export PATH=$PATH:/usr/krb5/sbin`. This command points to the Kerberos scripts that are necessary to run the executable files.
3. At the command line, enter `kadmin -p admin/admin`, and press Enter.
4. Sign in with administrator's password. For example, `secret`.
5. At the kadmin prompt, enter `addprinc krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM`. You will be prompted to enter a password for the principal "krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM". Enter `shipord1` for the password. Press Enter. You will be prompted to re-enter this password, and you will receive a message that reads:

```
Principal "krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM" created.
```

6. At the kadmin prompt, enter `addprinc krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO.COM`. You will be prompted to enter a password for the principal "krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO.COM". Enter `shipord2` for the password. Press Enter. You will be prompted to re-enter this password, and you will receive a message that reads:

```
Principal "krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO.COM" created.
```

7. Enter `quit` to exit the kadmin interface, and press F3 (Exit) to exit the PASE environment.

Changing encryption values on i5/OS PASE Kerberos server

To operate with Windows workstations, you need to change the Kerberos server default encryption settings so that clients can be authenticated to the i5/OS PASE Kerberos server.

To change the default encryption settings, you need to edit the kdc.conf file located in the /var/krb5/krb5kdc directory by following these steps:

1. In a character-based interface, enter `edtf '/var/krb5/krb5kdc/kdc.conf'` to access the kdc.conf file.
2. Change the following lines in the kdc.conf file:

```
| supported_enctypes = des3-cbc-sha1:normal
| arcfour-hmac:normal aes256-cts:normal
| des-cbc-md5:normal des-cbc-crc:normal
```

to

```
| supported_enctypes = des-cbc-crc:normal des-cbc-md5:normal
```

Configuring the Windows 2000 server to trust SHIPDEPT.MYCO.COM

Now that you have configured System B to trust the ORDEPT.MYCO.COM realm, you need to configure the Windows 2000 server to trust the SHIPDEPT.MYCO.COM realm.

Follow these steps to configure the Windows 2000 server:

1. Log on to your Windows 2000 server with your administrator account.
2. From the Start menu, expand **Programs** → **Administrative Tools** → **Active Directory Domain and Trusts**.
3. On the Active Directory Domains and Trusts page, right-click the **ORDEPT.MYCO.COM** realm (sometimes referred to as a Windows domain within the Windows interface) and select **Properties**.
4. On the **Trust** tab, click **Add** on the **Domain trusted by this domain** table.
5. On the Add Trusted Domains page, in the **Trusted domain** field enter `SHIPDEPT.MYCO.COM`. Enter `shipord1` as the password.
6. The **Active Directory** dialog box is displayed indicating that the MYCO.COM domain cannot be contacted. Because the MYCO.COM domain is an interoperable non-Windows domain and you want to set up this side of the trust, click **OK** to close the dialog box.
7. On the **Trust** tab, click **Add** on the **Domain that trust this domain** table.
8. On the Add Trusted Domains page, in the **Trusted domain** field enter `SHIPDEPT.MYCO.COM`. Enter `shipord2` as the password.
9. The **Active Directory** dialog box is displayed indicating that the MYCO.COM domain cannot be contacted. Because the MYCO.COM domain is an interoperable non-Windows domain and you want to set up this side of the trust, click **OK** to close the dialog box.
10. Click **OK**.

Adding the SHIPDEPT.MYCO.COM realm to System A

You must define the SHIPDEPT.MYCO.COM realm on System A so System A can determine where to find the i5/OS PASE Kerberos server within the SHIPDEPT.MYCO.COM realm.

Follow these steps to define the SHIPDEPT.MYCO.COM realm:

1. In iSeries Navigator, expand **System A** → **Security** → **Network Authentication Service**.
2. Right-click **Realms**, and select **Add realm**.
3. On the **Add Realm** dialog box, specify the following information, and click **OK**.
   a. **Realm to add**: `SHIPDEPT.MYCO.COM`
   b. **KDC**: `systemb.shipdept.myco.com`
   c. **Port**: 88

4. Click **Realms** to view the list of realms in the right pane. Verify that the SHIPDEPT.MYCO.COM realm appears in the list.

You have now completed the steps to configure a cross-realm trust relationship between the ORDEPT.MYCO.COM and the SHIPDEPT.MYCO.COM realms.

Scenario: Propagating network authentication service configuration across multiple systems

Here are the prerequisites and objectives for propagating your network authentication service configuration across multiple systems.

Situation

You are a systems administrator for a large automobile parts manufacturer. You currently manage five System i platforms with iSeries Navigator. One system operates as the central system, which stores data and manages these other systems. The security administrator for your company has just configured network authentication service on a new system to participate in a Windows 2000 domain, which authenticates users to the enterprise. The security administrator has tested the network authentication service configuration on this system and has successfully obtained a service ticket for this System i platform. You want to simplify the configuration of network authentication service among these systems that you manage.

Using the Synchronize Functions wizard, you want to take the network authentication service configuration on the model system and apply it to your other systems. The Synchronize Functions wizard makes network authentication service configuration throughout your network quicker and easier because you do not need to configure each system separately.

Because one of the systems runs OS/400® Version 5 Release 2 (V5R2) and this release does not support the Synchronize Functions wizard, you will need to configure your V5R2 system using the network authentication service wizard. You will need to configure this system to match the current network authentication service configuration on your model system.

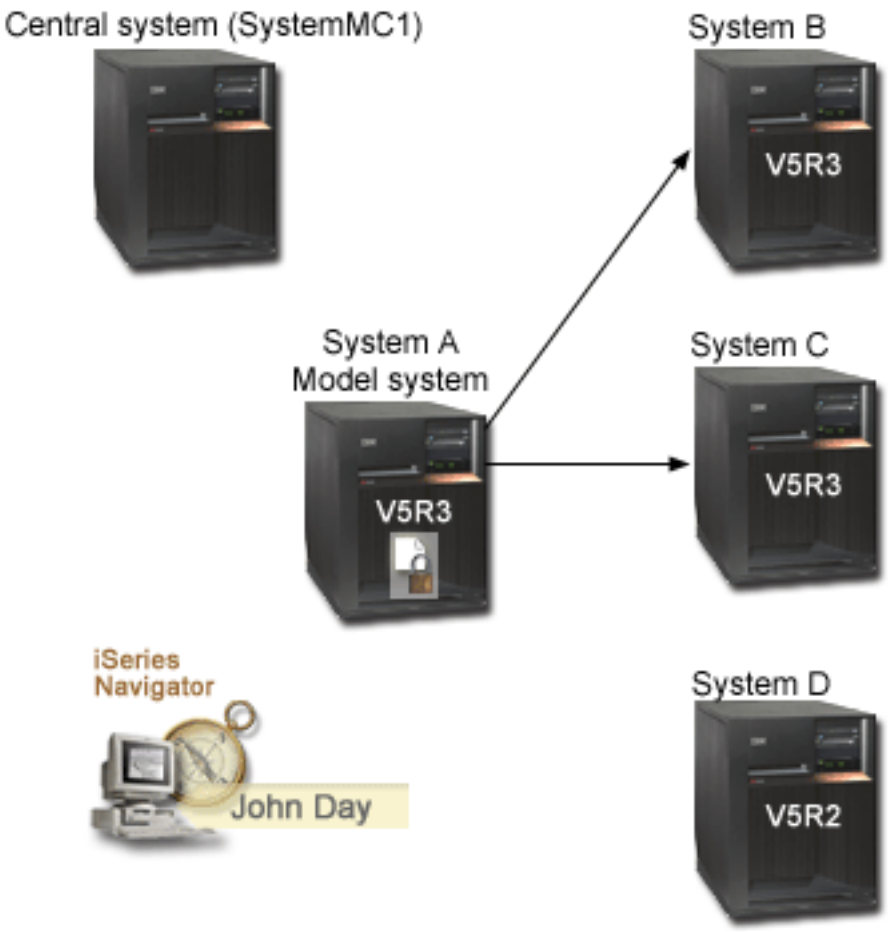
Objectives

In this scenario, MyCo, Inc has three distinct goals:

1. To simplify configuration of network authentication service in the network.
2. To have all System i platforms point to the same Kerberos server.
3. To configure a V5R2 system to also participate in the Kerberos realm.

Details

The following graphic shows the details for this scenario.



SystemMC1: Central system

- Runs i5/OS V5R3, or later, with the following options and licensed programs installed:
  - i5/OS Host Servers (5722-SS1 Option 12)
  - iSeries Access for Windows (5722-XE1)
  - Network Authentication Enablement (5722-NAE) if you are using i5/OS V5R4, or later
  - Cryptographic Access Provider (5722-AC3) if you are running i5/OS V5R3
- Stores, schedules and runs synchronization setting tasks for each of the endpoint systems.

System A: Model system

- Runs i5/OS V5R3, or later, with the following options and licensed programs installed:
  - i5/OS Host Servers (5722-SS1 Option 12)
  - iSeries Access for Windows (5722-XE1)
  - Network Authentication Enablement (5722-NAE) if you are using i5/OS V5R4, or later
  - Cryptographic Access Provider (5722-AC3) if you are running i5/OS V5R3
- Is the model system for propagating network authentication service configuration to endpoint systems.

System B: Endpoint system

- Runs i5/OS V5R3, or later, with the following options and licensed programs installed:
  - i5/OS Host Servers (5722-SS1 Option 12)
  - iSeries Access for Windows (5722-XE1)
  - Network Authentication Enablement (5722-NAE) if you are using i5/OS V5R4, or later
  - Cryptographic Access Provider (5722-AC3) if you are running i5/OS V5R3
- Is one of the endpoint systems for the propagation of network authentication service configuration.

System C: Endpoint system
- Runs i5/OS V5R3 with the following options and licensed programs installed:
  - i5/OS Host Servers (5722-SS1 Option 12)
  - iSeries Access for Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- Is one of the endpoint systems for the propagation of network authentication service configuration.

System D: Endpoint system
- Runs OS/400 V5R2 with the following options and licensed programs installed:
  - i5/OS Host Servers (5722-SS1 Option 12)
  - iSeries Access for Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- Has the following V5R2 PTFs (program temporary fixes) applied:
  - SI08977
  - SI08979
- Requires separate configuration of network authentication service using the Network Authentication Service wizard in iSeries Navigator.

Client PC
- Runs iSeries Access for Windows (5722-XE1).
- Runs iSeries Navigator with the following subcomponents:

  Note: Only required for PC used to administer network authentication service.
  - Network
  - Security

Windows 2000 server (not shown in graphic)
- Operates as the Kerberos server for the network (kdc1.myco.com).
- All users have been added to Microsoft Windows Active Directory.

Note: The KDC server name, **kdc1.myco.com**, is a fictitious name used in this scenario.

Prerequisites and assumptions

SystemMC1: Central system prerequisites
1. All system requirements, including software and operating system installation, have been verified.
   To verify that these licensed programs have been installed, follow these steps:
   a. In iSeries Navigator, expand *your system* → **Configuration and Service** → **Software** → **Installed Products**.
   b. Ensure that all the necessary licensed programs are installed.
2. All necessary hardware planning and setup have been completed.

3. TCP/IP and basic system security have been configured and tested on System A.
4. No one has changed the default settings in iSeries Navigator to disable the Task Status window from opening when a task starts. To verify that the default setting has not been changed, follow these steps:
   a. In iSeries Navigator, right-click ***your central system*** and select **User Preferences**.
   b. On the General page, verify that **Automatically open a task status window when one of my tasks starts** is selected.
5. Secure Sockets Layer (SSL) has been configured to protect the transmission of data between these systems.

   Note: When you propagate network authentication service configuration among systems, sensitive information like passwords are sent across the network. You should use SSL to protect this information, especially if it is being sent outside your local area network (LAN). See Scenario: Securing all connections to your Management Central server with SSL for details.

System A: Model system prerequisites

1. This scenario assumes that Network authentication service is properly configured on the model system (System A).
2. All system requirements, including software and operating system installation, have been verified.

   To verify that these licensed programs have been installed, follow these steps:
   a. In iSeries Navigator, expand ***your system*** → **Configuration and Service** → **Software** → **Installed Products**.
   b. Ensure that all the necessary licensed programs are installed.
3. All necessary hardware planning and setup have been completed.
4. TCP/IP and basic system security have been configured and tested on your system.
5. Secure Sockets Layer (SSL) has been configured to protect the transmission of data between these systems.

   Note: When you propagate network authentication service configuration among systems, sensitive information like passwords are sent across the network. You should use SSL to protect this information, especially if it is being sent outside your local area network (LAN). See Scenario: Securing all connections to your Management Central server with SSL for details.

System B, System C, and System D: Endpoint system prerequisites

1. All system requirements, including software and operating system installation, have been verified.

   To verify that these licensed programs have been installed, follow these steps:
   a. In iSeries Navigator, expand ***your system*** → **Configuration and Service** → **Software** → **Installed Products**.
   b. Ensure that all the necessary licensed programs are installed.
2. All necessary hardware planning and setup have been completed.
3. TCP/IP and basic system security have been configured and tested on your system.
4. Secure Sockets Layer (SSL) has been configured to protect the transmission of data between these systems.

   Note: When you propagate network authentication service configuration among systems, sensitive information like passwords are sent across the network. You should use SSL to protect this information, especially if it is being sent outside your local area network (LAN). See Scenario: Securing all connections to your Management Central server with SSL for details.

Windows 2000 server (not shown in graphic)

1. All necessary hardware planning and setup have been completed.
2. TCP/IP has been configured and tested on the server.

3. Windows domain has been configured and tested.
4. All users within your network have been added to a Windows domain through Active Directory.

Configuration steps

To use the Synchronize Functions wizard to propagate network authentication service configuration to endpoint systems, you must complete the following steps.

Completing the planning work sheets

Before you begin using iSeries Navigator to propagate the configuration on a model system to target systems, complete these planning work sheets.

All answers should be `Yes` before you proceed with propagating network authentication service.

Table 8. Propagating network authentication service - prerequisite work sheet

Prerequisite work sheet	Answers
Is your i5/OS V5R3 (5722-SS1), or later, for the following systems: • Central system • System A • System B • System C	Yes
Have you applied the latest program temporary fixes (PTFs)?	Yes
Is OS/400 V5R2 (5722-SS1), or later, running on System D?	Yes
For System D, have you applied the latest program temporary fixes (PTFs), including the following fixes? • SI08977 • SI08979	
Are the following options and licensed programs installed on all your System i models? • i5/OS Host Servers (5722-SS1 Option 12) • iSeries Access for Windows (5722-XE1) • Network Authentication Enablement (5722-NAE) if you are using i5/OS V5R4, or later • Cryptographic Access Provider (5722-AC3) if you are running i5/OS V5R3	Yes
Is iSeries Access for Windows (5722-XE1) installed on the administrator's PC?	Yes
Is iSeries Navigator installed on the administrator's PC? • Is the Network subcomponent of iSeries Navigator installed on the administrator's PC? • Is the Security subcomponent of iSeries Navigator installed on the administrator's PC?	Yes
Have you installed the latest IBM eServer iSeries Access for Windows service pack? See iSeries Access for the latest service pack.	Yes
Do you have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities?	Yes

Table 8. Propagating network authentication service - prerequisite work sheet (continued)

Prerequisite work sheet	Answers
Do you have one of the following systems acting as the Kerberos server? If yes, specify which system. 1. Microsoft Windows 2000 Server **Note:** Microsoft Windows 2000 Server uses Kerberos authentication as its default security mechanism. 2. Windows Server 2003 3. i5/OS PASE (V5R3, or later) 4. AIX server 5. z/OS	Yes, Windows 2000 Server
For Windows 2000 Server and Windows Server 2003, do you have Windows Support Tools (which provides the ktpass tool) installed?	Yes
Is the System i system time within 5 minutes of the system time on the Kerberos server? If not, see Synchronizing system times.	Yes

Table 9. Synchronize functions planning work sheet

Questions	Answers
What is the name of the system group?	MyCo system group
What systems will be included in this system group?	System B, System C, System D
What functions do you plan to propagate to this system group?	Network authentication service
For which services do you want to create keytab entries? • i5/OS Kerberos Authentication • LDAP • iSeries IBM HTTP Server • iSeries NetServer	i5/OS Kerberos Authentication
What are the service principal names for the systems to which you want to propagate configuration?	krbsvr400/systema.myco.com@MYCO.COM krbsvr400/systemb.myco.com@MYCO.COM krbsvr400/systemc.myco.com@MYCO.COM krbsvr400/systemd.myco.com@MYCO.COM
What are the passwords that are associated with each of these principals?	The password for the principals for Systems A, B, and C will be `systema123`. The password for the principal for System D will be `systemd123`.
What is the fully qualified host name for each System i platform?	systema.myco.com systemb.myco.com systemc.myco.com systemd.myco.com
What is the name of the Windows 2000 domain? **Note:** A Windows 2000 domain is similar to a Kerberos realm. Microsoft Active Directory uses Kerberos authentication as its default security mechanism.	MYCO.COM

Table 10. Network authentication service planning work sheet for System D

Questions	Answers
What is the name of the Kerberos default realm to which your System i platform belongs? **Note:** A Windows 2000 domain is similar to a Kerberos realm. Microsoft Active Directory uses Kerberos authentication as its default security mechanism.	MYCO.COM

Table 10. Network authentication service planning work sheet for System D (continued)

Questions	Answers
Are you using Microsoft Active Directory?	Yes
What is the Kerberos server for this Kerberos default realm? What is the port on which the Kerberos server listens?	**KDC:** kdc1.myco.com **Port:** 88 **Note:** This is the default port for the Kerberos server.
Do you want to configure a password server for this default realm? If yes, answer the following questions: What is the name of the password server for this Kerberos server? What is the port on which the password server listens?	Yes **Password server:** kdc1.myco.com **Port:** 464 **Note:** This is the default port for the password server.
For which services do you want to create keytab entries? • i5/OS Kerberos Authentication • LDAP • iSeries IBM HTTP Server • iSeries NetServer	i5/OS Kerberos Authentication
What is the password for your i5/OS service principals?	systemd123

Creating a system group

Before you can propagate the network authentication service configuration to a target system, you must create a system group for all the endpoint systems.

A system group is a collection of systems that you can manage and to which you can apply similar settings and attributes, such as the network authentication service configuration. Follow these steps to create a system group:

1. In iSeries Navigator, expand **Management Central (SystemMC1)**.
2. Right-click **System Groups** and select **New System Group** to create a new system group.
3. On the General page, enter `MyCo system group` in the name field and specify a description for this system group.
4. From the **Available System** list, select **System B**, **System C**, and **System D**, and click **Add**. This will add these systems to the **Selected systems** list. Click **OK**.
5. Expand **System Groups** to verify that your system group was added.

Propagating system settings from the model system (System A) to System B and System C

To propagate system settings to multiple endpoint systems, use the Synchronize Functions wizard in iSeries Navigator. The wizard can propagate system settings such as a network authentication service configuration.

To propagate the network authentication service configuration to the target systems, complete these steps:

1. In iSeries Navigator, expand **Management Central (SystemMC1)** → **System Groups**.
2. Right-click **MyCo system group** and select **System Values** → **Synchronize Functions**. This launches the **Synchronize Functions Wizard**.
3. On the Welcome page, review the information about the Synchronize Functions wizard, and click **Next**. The Welcome page lists the functions that you can choose to synchronize later in the wizard.

   Note: When you propagate network authentication service configuration among systems, sensitive information like passwords are sent across the network. You should use SSL to protect this

information, especially if it is being sent outside your local area network (LAN). See Scenario: Securing all connections to your Management Central server with SSL for details.

4. On the Model System page, select System A as the model system, and click **Next**. This model system will be used as a base for synchronizing the network authentication service configuration to other systems.
5. On the Target Systems and Groups page, select **MyCo system group**. Click **Next**.
6. On the What to Update page, select **Network Authentication Service (Kerberos)**. Click **Verify configuration**. After the configuration has been verified, click **Next**.

   Note: If the verification of the network authentication service does not complete successfully, then there might be a problem with the network authentication service configuration on the model system. To recover from this error, you must check the configuration on the model system, fix the configuration and then return to Step 2 in these instructions.
7. On the Network Authentication Service page, select **i5/OS Kerberos Authentication** and enter `systema123` in the **Password** and **Confirm password** fields. Click **Next**.

   Note: This password is used for the keytab entry on each target system. If your security policy requires a different password on each system, then you can skip this step. Instead, after you complete this wizard, you can manually add the keytab entries to individual systems and enter a different password for each system.
8. On the Summary page, verify that the appropriate settings are listed on this page. Click **Finish**.
9. By default, a dialog box is displayed that indicates the Synchronize Functions task has started. However, if you have changed the default setting, this dialog box is not displayed. Click **OK**.
10. The **Synchronize Functions Status** dialog box is displayed. Verify that the task has completed successfully. Assume that the task completed successfully on all the endpoint systems except System D. Because System D is running OS/400 V5R2, it does not support the Synchronize Functions wizard.

    To recover from this error, you must manually configure network authentication service on System D so that it matches the configuration on the model system (System A).

Configuring network authentication service on System D

You need to configure network authentication service on System D so that it matches the configuration settings on System A.

To configure network authentication service, follow these steps:

1. In iSeries Navigator, expand **System D** → **Security** .
2. Right-click **Network Authentication Service** and select **Configure** to start the configuration wizard.

   Note: After you have configured network authentication service, this option will be **Reconfigure**.
3. Review the Welcome page for information about what objects the wizard creates. Click **Next**.
4. On the Specify realm information page, enter `MYCO.COM` in the **Default realm** field and select **Microsoft Active Directory is used for Kerberos authentication**. Click **Next**.
5. On the Specify KDC information page, enter kdc1.myco.com for the name of the Kerberos server for this realm in the **KDC** field and enter 88 in the**Port** field. Click **Next**.
6. On the Specify password information page, select **Yes** to configure System D to point to the password server configured for the default realm. The password server has already been configured. It allows principals to change passwords on the Kerberos server. Enter `kdc1.myco.com` in the **Password server** field. The password server has the default port of 464. Click **Next**.
7. On the Select keytab entries page, select **i5/OS Kerberos Authentication**. Click **Next**.
8. On the Create i5/OS keytab entry page, enter and confirm a password. For example, `systemd123`. Click **Next**.
9. Optional: On the Create batch file page, select **No**.

10. On the Summary page, review the network authentication service configuration details. Click **Finish**.

Adding the principals for endpoint systems to the Windows 2000 domain

Here are the steps for adding principals for endpoint systems.

1. **System B steps**
   a. On your Windows 2000 server, expand **Administrative Tools** → **Active Directory Users and Computers**.
   b. Select **MYCO.COM** as the domain and expand **Action** → **New** → **User**.

      Note: This Windows domain should be the same as the default realm name that you specified for the network authentication service configuration.
   c. In the **Name** field, enter `systemb` to identify the System i platform to this Windows domain. This adds a new user account for System B.
   d. Access the properties on the Active Directory user systemb. From the **Account** tab, select **Account is trusted for delegation**. This allows the i5/OS service principal to access other services on behalf of a signed-in user.
   e. On the Windows 2000 server, you need to map the user account you just created to the i5/OS service principal by using the **ktpass** command. The ktpass tool is provided in the **Service Tools** folder on the Windows 2000 Server installation CD. At a Windows command prompt, enter the following command:

      ```
      ktpass -mapuser systemb -pass systema123 -princ krbsvr400/systemb.myco.com@MYCO.COM
      -mapop set
      ```
2. **System C steps**
   a. On your Windows 2000 server, expand **Administrative Tools** → **Active Directory Users and Computers**.
   b. Select **MYCO.COM** as the domain and expand **Action** → **New** → **User**.

      Note: This Windows domain should be the same as the default realm name that you specified for the network authentication service configuration.
   c. In the **Name** field, enter `systemc` to identify the System i platform to this Windows domain. This adds a new user account for System C.
   d. Access the properties on the Active Directory user systemc. From the **Account** tab, select **Account is trusted for delegation**. This allows the i5/OS service principal to access other services on behalf of a signed-in user.
   e. On the Windows 2000 server, you need to map the user account you just created to the i5/OS service principal by using the ktpass command. The ktpass tool is provided in the **Service Tools** folder on the Windows 2000 Server installation CD. At a Windows command prompt, enter the following command:

      ```
      ktpass -mapuser systemc -pass systema123 -princ krbsvr400/systemc.myco.com@MYCO.COM
      -mapop set
      ```
3. **System D steps**
   a. On your Windows 2000 server, expand **Administrative Tools** → **Active Directory Users and Computers**.
   b. Select **MYCO.COM** as the domain and expand **Action** → **New** → **User**.

      Note: This Windows domain should be the same as the default realm name that you specified for the network authentication service configuration.
   c. In the **Name** field, enter `systemd` to identify the System i platform to this Windows domain. This adds a new user account for System D.

d. Access the properties on the Active Directory user systemd. From the **Account** tab, select **Account is trusted for delegation**. This allows the i5/OS service principal to access other services on behalf of a signed-in user.
e. On the Windows 2000 server, you need to map the user account you just created to the i5/OS service principal by using the ktpass command. The ktpass tool is provided in the **Service Tools** folder on the Windows 2000 Server installation CD. At a Windows command prompt, enter the following command:

```
ktpass -mapuser systemd -pass systemd123 -princ krbsvr400/systemd.myco.com@MYCO.COM
-mapop set
```

You have completed the propagation of the network authentication service configuration to multiple systems. To configure the Management Central server to take advantage of network authentication service, you need to perform some additional tasks. See "Scenario: Using Kerberos authentication between Management Central servers" for details.

Scenario: Using Kerberos authentication between Management Central servers

Here are the prerequisites and objectives for using Kerberos authentication between Management Central servers.

Situation

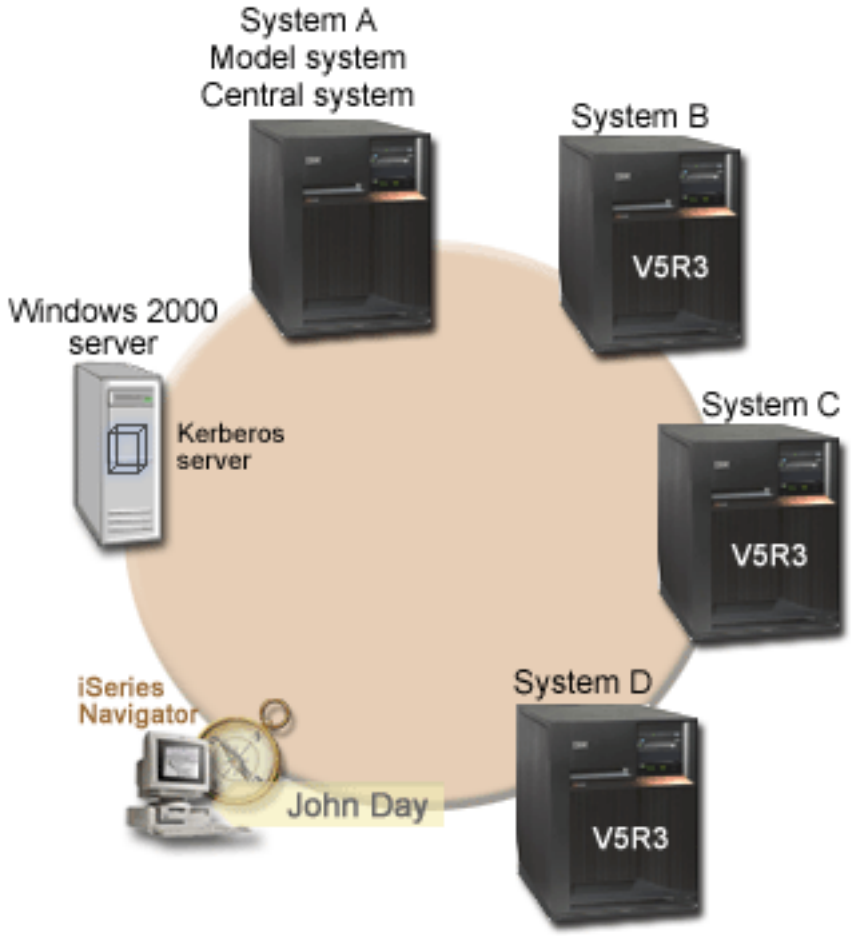
You are a network administrator for a medium-sized parts manufacturer. You currently manage four System i products using iSeries Navigator on a client PC. You want your Management Central server jobs to use Kerberos authentication instead of other authentication methods that you have used in the past, namely password synchronization.

Objectives

In this scenario, the goal for MyCo, Inc. is to use Kerberos authentication among Management Central servers.

Details

The following graphic shows the details for this scenario.



System A: Model system and central system

- Runs i5/OS V5R3, or later, with the following options and licensed programs installed:
  - i5/OS Host Servers (5722-SS1 Option 12)
  - iSeries Access for Windows (5722-XE1)
  - Network Authentication Enablement (5722-NAE) if you are using i5/OS V5R4, or later
  - Cryptographic Access Provider (5722-AC3) if you are running i5/OS V5R3
- i5/OS service principal, krbsvr400/systema.myco.com@MYCO.COM, and associated password have been added to the keytab file.
- Stores, schedules, and runs synchronization setting tasks for each of the endpoint systems.

System B: Endpoint system

- Runs i5/OS V5R3, or later, with the following options and licensed programs installed:
  - i5/OS Host Servers (5722-SS1 Option 12)
  - iSeries Access for Windows (5722-XE1)
  - Network Authentication Enablement (5722-NAE) if you are using i5/OS V5R4, or later
  - Cryptographic Access Provider (5722-AC3) if you are running i5/OS V5R3

- i5/OS service principal, krbsvr400/systemb.myco.com@MYCO.COM, and associated password have been added to the keytab file.

System C: Endpoint system

- Runs i5/OS V5R4 with the following options and licensed programs installed:
  - i5/OS Host Servers (5722-SS1 Option 12)
  - iSeries Access for Windows (5722-XE1)
  - Network Authentication Enablement (5722-NAE)
- i5/OS service principal, krbsvr400/systemc.myco.com@MYCO.COM, and associated password have been added to the keytab file.

System D: Endpoint system

- Runs i5/OS V5R3, or later, with the following options and licensed programs installed:
  - i5/OS Host Servers (5722-SS1 Option 12)
  - iSeries Access for Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- i5/OS service principal, krbsvr400/systemd.myco.com@MYCO.COM, and associated password have been added to the keytab file.

Windows 2000 server

- Operates as the Kerberos server for these systems.
- The following i5/OS service principals have been added to the Windows 2000 server:
  - krbsvr400/systema.myco.com@MYCO.COM
  - krbsvr400/systemb.myco.com@MYCO.COM
  - krbsvr400/systemc.myco.com@MYCO.COM
  - krbsvr400/systemd.myco.com@MYCO.COM

Client PC

- Runs iSeries Access for Windows (5722-XE1).
- Runs iSeries Navigator with the following subcomponents:

  Note: Only required for PC used to administer network authentication service.
  - Network
  - Security

Prerequisites and assumptions

1. All system requirements, including software and operating system installation, have been verified.

   To verify that the licensed programs have been installed, follow these steps:
   a. In iSeries Navigator, expand ***your system*** → **Configuration and Service** → **Software** → **Installed Products**.
   b. Ensure that all the necessary licensed programs are installed.
2. All necessary hardware planning and setup have been completed.
3. TCP/IP and basic system security have been configured and tested on each of these systems.
4. No one has changed the default settings in iSeries Navigator to stop the Task Status window from opening when a task starts. To verify that the default setting has not been changed, follow these steps:
   a. In iSeries Navigator, right-click ***your central system*** and select **User Preferences**.
   b. On the General page, verify that **Automatically open a task status window when one of my tasks starts** is selected.

5. This scenario is based on the assumption that network authentication service has been configured on each system using the Synchronize Functions wizard in iSeries Navigator. This wizard propagates network authentication service configuration from a model system to multiple target systems. See “Scenario: Propagating network authentication service configuration across multiple systems” on page 34 for details on how to use the Synchronize Functions wizard.

Configuration steps

To configure Kerberos authentication between Management Central servers, perform these steps.

Completing the planning work sheets

These planning work sheets illustrate the type of information you need before you enable your systems to use Kerberos authentication.

Table 11. Using Kerberos authentication between Management Central servers - prerequisite work sheet

Prerequisite work sheet	Answers
Is your i5/OS V5R3 (5722-SS1), or later, for all of your System i platforms?	Yes
Have you applied the latest program temporary fixes (PTFs)?	Yes
Are the following options and licensed programs installed on all your System i models? • i5/OS Host Servers (5722-SS1 Option 12) • iSeries Access for Windows (5722-XE1) • Network Authentication Enablement (5722-NAE) if you are using i5/OS V5R4, or later • Cryptographic Access Provider (5722-AC3) if you are running i5/OS V5R3	Yes
Is iSeries Access for Windows (5722-XE1) installed on the administrator’s PC?	Yes
Is iSeries Navigator installed on the administrator’s PC? • Is the Network subcomponent of iSeries Navigator installed on the administrator’s PC? • Is the Security subcomponent of iSeries Navigator installed on the administrator’s PC?	Yes
Have you installed the latest IBM eServer iSeries Access for Windows service pack? See iSeries Access for the latest service pack.	Yes
Do you have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities?	Yes
Do you have one of the following systems acting as the Kerberos server? If yes, specify which system. 1. Microsoft Windows 2000 Server **Note:** Microsoft Windows 2000 Server uses Kerberos authentication as its default security mechanism. 2. Windows Server 2003 3. i5/OS PASE (V5R3, or later) 4. AIX server 5. z/OS	Yes, Windows 2000 Server
For Windows 2000 Server and Windows Server 2003, do you have Windows Support Tools (which provides the ktpass tool) installed?	Yes

Table 11. Using Kerberos authentication between Management Central servers - prerequisite work sheet (continued)

Prerequisite work sheet	Answers
Is the System i system time within 5 minutes of the system time on the Kerberos server? If not, see "Synchronizing system times" on page 99.	Yes

Table 12. Using Kerberos authentication between Management Central servers - planning work sheet

Questions	Answers
What is the name of the system group?	MyCo2 system group
What systems will be included in this system group?	System A, System B, System C, System D
What are the service principal names for the System i platforms?	krbsvr400/systema.myco.com@MYCO.COM krbsvr400/systemb.myco.com@MYCO.COM krbsvr400/systemc.myco.com@MYCO.COM krbsvr400/systemd.myco.com@MYCO.COM

Setting the central system to use Kerberos authentication

System A is the model system and central system for the other target systems.

To set Kerberos authentication on the central system, complete these steps:

1. In iSeries Navigator, right-click **Management Central (System A)** and select **Properties**.
2. On the **Security** tab, select **Use Kerberos authentication** and set the authentication level to **Add to trusted group**.
3. Select **Do not use** in the **Identity Mapping** field and click **OK**. This setting allows you to enable or disable the use of Enterprise Identity Mapping (EIM) by Management Central servers to enable a single sign-on environment for your endpoint systems. If you want to enable single sign-on for your endpoint systems, see Scenario: Configuring the Management Central server for a single sign-on environment for a scenario that shows this configuration.

   Note: The note at the bottom of the Security page indicates that the settings will take effect the next time the Management Central servers are started. Do not restart the servers now. This scenario indicates the appropriate time to restart the servers in a subsequent step.
4. A dialog box is displayed that indicates that the changes to these settings affect only this central system and that Kerberos must be properly configured before these settings can be used by the Management Central server jobs. Click **OK**. You have enabled Kerberos authentication to be used by the central system.

Creating MyCo2 system group

A system group is a collection of systems that you can manage and to which you can apply similar settings and attributes, such as the network authentication service configuration.

Before you can apply the appropriate settings to the other systems in your network, you must create a system group for all the endpoint systems.

1. In iSeries Navigator, expand **Management Central (System A)**.
2. Right-click **System Groups** and select **New System Group** to create a new system group.
3. On the General page, enter `MyCo2 system group` in the name field. Specify a description for this system group.
4. From the **Available System** list, select System A, System B, System C, and System D and click **Add**. This adds these systems to the **Selected systems** list. Click **OK**.
5. Expand **System Groups** to verify that your system group was added.

Collecting system values inventory

You need to use the Collect Inventory function in iSeries Navigator to add the Kerberos authentication settings to an inventory for the target systems in the MyCo2 system group.

To collect inventory for the MyCo2 system group, complete the following steps:

1. In iSeries Navigator, expand **Management Central (System A)** → **System Group**.
2. Right-click **MyCo2 system group** and select **Inventory** → **Collect**.
3. On the Collect Inventory - MyCo2 system group page, select **System values**. Click **OK**. By default, a dialog box is displayed that indicates the Synchronize Functions Collect Inventory task has started. However, if you have changed the default setting, this dialog box is not displayed. Click **OK**.
4. On the Collect Inventory Status page, read all the status values that are displayed and fix any problems that you might encounter. For details on specific status values related to inventory collection that appear on this page, select **Help** → **Task Status Help**. From the **Task Status** help page, select **Inventory**. This page displays all the status values that you might encounter with detailed descriptions and recovery information.
5. If the inventory collection completed successfully, close the status window.

Comparing and updating Kerberos settings in iSeries Navigator

After collecting system values inventory, you need to take the Kerberos settings that were selected on the central system and apply them to each of the target systems in the MyCo2 system group.

To update the target systems in the MyCo2 system group, complete the following steps:

1. In iSeries Navigator, expand **Management Central (System A)** → **System Group**.
2. Right-click **MyCo2 system group** and select **System Values** → **Compare and Update**.
3. Complete the fields on the **Compare and Update - MyCo2 system group** dialog box:
   a. Select **System A** for the **Model system** field.
   b. Select **Management Central** for the **Category** field.
   c. From the list of **Items to compare**, select **Use Kerberos authentication to verify requests** and **Kerberos authentication trust level**.
4. Verify that the target systems in the MyCo2 system group are displayed in the list of target systems and click **OK** to start the update. This will update each of the target systems within the MyCo2 system group with the Kerberos authentication settings that were selected on the model system.
5. By default, a dialog box is displayed that indicates the Compare and Update task has started. However, if you have changed the default setting, this dialog box is not displayed. Click **OK**.
6. On the **Update Values Status** dialog box, verify that the update completes on each system, and close the dialog box.

Restarting Management Central server on the central system and target systems

After completing the update for each of the target systems within the MyCo2 system group, you need to restart all the Management Central servers on the central and target systems.

To restart these Management Central servers, complete the following steps:

1. In iSeries Navigator, expand **My connections** → **System A** → **Network** → **Servers** → **TCP/IP**.
2. Right-click **Management Central** and select **Stop**. Wait until the Management Central server has stopped. Press F5 to refresh the screen and view the status in the right pane. The status should display **Stopped** when the server has stopped.
3. Right-click **Management Central** and select **Start**. This will restart the Management Central servers on the Central System.
4. Repeat steps 1-3 on the target systems: System B, System C, and System D.

Adding Kerberos service principal to the trusted group file for each endpoint

After all the Management Central servers have been restarted, you need to add the central system's Kerberos service principal to the trusted group file for each of the endpoint systems.

From the central system, run a remote command, such as Display Library List (DSPLIBL), to all the endpoint systems. Each endpoint system automatically adds the central system's Kerberos service principal to its individual trusted group file because **Add to trusted group** is selected as the authentication level on each endpoint system. You can run any remote command from the central system to an endpoint system to cause the Management Central server job on the endpoint system to record the necessary Kerberos service principals in the trusted group file. The DSPLIBL command is used for example purposes only.

Note: If you use a model or source system to run tasks, such as send fixes, send users, synchronize time, you should run these tasks so that the correct Kerberos service principals are added to the correct trusted group files.

For this scenario, you decide to run a remote command to all the endpoint systems to add the Kerberos service principal to the trusted group file on each endpoint system. To run a remote command, follow these steps:

1. In iSeries Navigator, expand **Management Central (System A)** → **System Groups**.
2. Right-click **MyCo2 system group** and select **Run Command**.
3. On the Run Command-MyCo2 system group page, enter `dsplibl` in the **Commands to run** field and click **OK** to start the command task immediately. You can also click **Previous Commands** to select from a list of commands you have previously run, or you can click **Prompt** to get assistance in entering or selecting an i5/OS command.
4. By default, a dialog box is displayed that indicates the Run Command task has started. However, if you have changed the default setting, this dialog box is not displayed. Click **OK**.
5. On the **Run Command Status** dialog box, verify that the command completes on each system and close the dialog box.

Verifying the Kerberos principals are added to the trusted group file

After running the remote command, you can verify that the central system's Kerberos service principal is in the trusted group file on each of the target systems.

1. In iSeries Navigator, expand **System B** → **File Systems** → **Integrated File System** → **Root** → **QIBM** → **UserData** → **OS400** → **MGTC** → **config**.
2. Right-click **McTrustedGroup.conf** and select **Edit** to view the contents of the file.
   a. Right-click **Integrated File System** and select **Properties**.
   b. On the **Integrated File System Properties** dialog box, select **All files** for **Enable edit options for:**, and click **OK**.
3. Verify that the central system's Kerberos service principal is listed as one of the Management Central Trusted Group Members.
4. Repeat these steps for System C and System D to verify that the central system's Kerberos service principal is added to each of the target systems.

Allowing trusted connections for the central system

After the remote command runs successfully to the endpoint systems, you need to allow trusted connections among Management Central servers.

Complete the following steps to allow trusted connections. This ensures that only the central system for MyCo2 system group (System A) can run tasks to the target systems.

1. In iSeries Navigator, right-click **Management Central (System A)** and select **Properties**.
2. On the **Security** tab, select **Use Kerberos authentication** and set the authentication level to **Allow only trusted connections**.

3. Select **Do not use** in the **Identity Mapping** field.
4. A dialog box is displayed that indicates that the changes to these settings affect only this central system and that Kerberos must be properly configured before these settings can be used by the Management Central server jobs. Click **OK**.

Repeating steps 4 through 6 for target systems

After allowing trusted connections for the central system, you must repeat steps 4 through 6 in this scenario to apply these changes to the target systems in the MyCo2 system group. This ensures that the target systems are configured to allow trusted connections.

Refer to these steps:

1. Step 4: Collecting system values inventory
2. Step 5: Comparing and updating Kerberos settings in iSeries Navigator
3. Step 6: Restarting Management Central server on the central system and target systems

Testing authentication on the endpoint systems

After the servers are restarted, the systems use Kerberos for authentication and the trusted group for authorization. For a system to accept and carry out a request, that system verifies not only that the requesting system has a valid Kerberos principal, but also that it trusts that Kerberos principal by checking if that principal is in its trusted group list.

Note: You need to repeat these steps on each of the target systems, using the following i5/OS service principals:

- krbsvr400/systema.myco.com@MYCO.COM
- krbsvr400/systemb.myco.com@MYCO.COM
- krbsvr400/systemc.myco.com@MYCO.COM
- krbsvr400/systemd.myco.com@MYCO.COM

To verify that Kerberos authentication is working on the endpoint systems, complete the following tasks:

Note: Be sure you have created a home directory for your i5/OS user profile before performing these tasks.

1. Close any sessions of iSeries Navigator.
2. On a command line, enter `QSH` to start the Qshell Interpreter.
3. Enter `keytab list` to display a list of principals registered in the keytab file. You should see results that are similar to this display:

```
Principal: krbsvr400/systema.myco.com@MYCO.COM
  Key version: 2
  Key type: 56-bit DES using key derivation
  Entry timestamp: 200X/05/29-11:02:58
```

4. Enter `kinit -k krbsvr400/systema.myco.com@MYCO.COM` to request a ticket-granting ticket from the Kerberos server. This command verifies that your system has been configured properly and the password in the keytab file matches the password stored on the Kerberos server. If this is successful, the QSH command displays without errors.
5. Enter `klist` to verify that the default principal is krbsvr400/systema.myco.com@MYCO.COM. This command displays the contents of a Kerberos credentials cache and verifies that a valid ticket has been created for the i5/OS service principal and placed within the credentials cache on the system.

```
 Ticket cache: FILE:/QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/creds/krbcred

 Default principal: krbsvr400/systema.myco.com@MYCO.COM

Server: krbtgt/MYCO.COM@MYCO.COM
  Valid 200X/06/09-12:08:45 to 20XX/11/05-03:08:45
$
```

You have now completed the tasks required to configure your Management Central server jobs to use Kerberos authentication between endpoint systems.

Scenario: Enabling single sign-on for i5/OS

Here are the prerequisites and objectives for enabling single sign-on for the i5/OS operating system.

Situation

You are a network administrator that manages a network and network security for your company, including the Order Receiving department. You oversee the IT operations for a large number of employees who take customer orders over the telephone. You also supervise two other network administrators who help you maintain the network.

The employees in the Order Receiving department use Windows 2000 and i5/OS and require multiple passwords for the different applications they use every day. Consequently, you spend a lot of time managing and troubleshooting problems related to passwords and user identities, such as resetting forgotten passwords.

As the company's network administrator, you are always looking for ways to improve the business, starting with the Order Receiving department. You know that most of your employees need the same type of authority to access the application that they use to query inventory status. It seems redundant and time consuming for you to maintain individual user profiles and numerous passwords that are required in this situation. In addition, you know that all of your employees can benefit by using fewer user IDs and passwords. You want to do these things:

- Simplify the task of password management for the Order Receiving department. Specifically, you want to efficiently manage user access to the application your employees routinely use for customer orders.
- Decrease the use of multiple user IDs and passwords for the department employees, as well as for the network administrators. However, you do not want to make the Windows 2000 IDs and i5/OS user profiles the same nor do you want to use password caching or synching.

Based on your research, you know that i5/OS supports single sign-on, a solution that allows your users to log on once to access multiple applications and services that normally require them to log on with multiple user IDs and passwords. Because your users do not need to provide as many user IDs and passwords to do their jobs, you have fewer password problems to solve for them. Single sign-on seems to be an ideal solution because it allows you to simplify password management in the following ways:

- For typical users that require the same authority to an application, you can create policy associations. For example, you want the order clerks in the Order Receiving department to be able to log on once with their Windows user name and password and then be able to access a new inventory query application in the manufacturing department without having to be authenticated again. However, you also want to ensure that the level of authorization that they have when using this application is appropriate. To attain this goal, you decide to create a policy association that maps the Windows 2000 user identities for this group of users to a single i5/OS user profile that has the appropriate level of authority for running the inventory query application. Because this is a query-only application in which users cannot change data, you are not as concerned about detailed auditing for this application. Consequently, you feel confident that using a policy association in this situation conforms to your security policy.

You create a policy association to map the group of order clerks with similar authority requirements to a single i5/OS user profile with the appropriate level of authority for the inventory query application. Your users benefit by having one less password to remember and one less logon to perform. As the administrator, you benefit by having to maintain only one user profile for user access to the application instead of multiple user profiles for everyone in the group.

- For each of your network administrators who have user profiles with special authorities, such as *ALLOBJ and *SECADM, you can create identifier associations. For example, you want all of the user identities for a single network administrator to be precisely and individually mapped to one another because of the administrator's high level of authority.

  Based on your company's security policy, you decide to create identifier associations to map specifically from each network administrator's Windows identity to that administrator's i5/OS user profile. You can more easily monitor and trace the activity of the administrator because of the one-to-one mapping that identifier associations provide. For example, you can monitor the jobs and objects that run on the system for a specific user identity. Your network administrator benefits by having one less password to remember and one less log-on to perform. As the network administrator, you benefit by tightly controlling the relationships between all of your administrator's user identities.

This scenario has the following advantages:

- Simplifies authentication process for users.
- Simplifies managing access to applications.
- Eases the overhead of managing access to systems in the network.
- Minimizes the threat of password theft.
- Avoids the need for multiple sign-ons.
- Simplifies user identity management across the network.

Objectives

In this scenario, you are the administrator at MyCo, Inc., who wants to enable single sign-on for the users in the Order Receiving department.

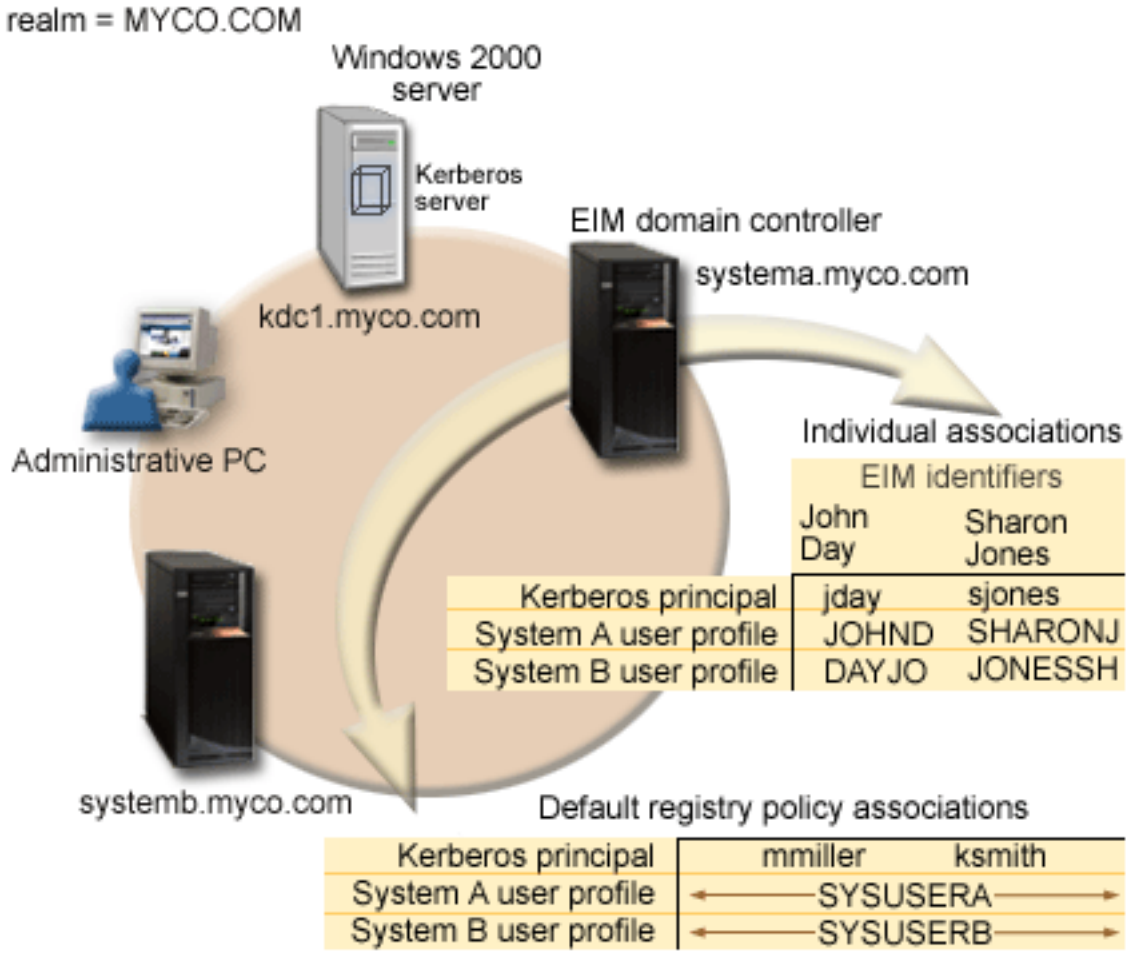
The objectives of this scenario are as follows:

- System A and System B must participate in the MYCO.COM realm to authenticate the users and services that are participating in this single sign-on environment. To enable the systems to use Kerberos, Systems A and B must be configured for network authentication service.
- The IBM Directory Server for iSeries (LDAP) on System A must function as the domain controller for the new EIM domain.

  Note: Refer to Domains to learn how two different types of domains, an EIM domain and a Windows 2000 domain, fit into the single sign-on environment.
- All user identities in the Kerberos registry must map successfully to a single i5/OS user profile with appropriate authority for user access to the inventory query application.
- Based on your security policy, two administrators, John Day and Sharon Jones, who also have user identities in the Kerberos registry, must have identifier associations to map these identities to their i5/OS user profiles which have *SECADM special authority. These one-to-one mappings enable you to closely monitor the jobs and objects that run on the system for these user identities.
- A Kerberos service principal must be used to authenticate the users to the IBM iSeries Access for Windows applications, including iSeries Navigator.

Details

The following figure illustrates the network environment for this scenario.



The figure illustrates the following points relevant to this scenario.

EIM domain data defined for the enterprise

- Three registry definition names:
  - A registry definition name of MYCO.COM for the Windows 2000 server registry. You will define this when you use the EIM configuration wizard on System A.
  - A registry definition name of SYSTEMA.MYCO.COM for the i5/OS registry on System A. You will define this when you use the EIM configuration wizard on System A.
  - A registry definition name of SYSTEMB.MYCO.COM for the i5/OS registry on System B. You will define this when you use the EIM configuration wizard on System B.
- Two default registry policy associations:

  Note: EIM lookup operation processing assigns the highest priority to identifier associations. Therefore, when a user identity is defined as a source in both a policy association and an identifier association, only the identifier association maps that user identity. In this scenario, two network administrators, John Day and Sharon Jones, both have user identities in the MYCO.COM registry, which is the source of the default registry policy associations. However, as shown below, these administrators also have identifier associations defined for their user identities in

the MYCO.COM registry. The identifier associations ensure that their MYCO.COM user identities are not mapped by the policy associations. Instead, the identifier associations ensure that their user identities in the MYCO.COM registry are individually mapped to other specific individual user identities.

  - One default registry policy association maps all user identities in the Windows 2000 server registry called MYCO.COM to a single i5/OS user profile called SYSUSERA in the SYSTEMA.MYCO.COM registry on System A. For this scenario, mmiller and ksmith represent two of these user identities.
  - One default registry policy association maps all user identities in the Windows 2000 server registry called MYCO.COM to a single i5/OS user profile called SYSUSERB in the SYSTEMB.MYCO.COM registry on System B. For this scenario, mmiller and ksmith represent two of these user identities.
- Two EIM identifiers named John Day and Sharon Jones to represent the two network administrators in the company who have those names.
- For the John Day EIM identifier, these identifier associations are defined:
  - A source association for the jday user identity, which is a Kerberos principal in the Windows 2000 server registry.
  - A target association for the JOHND user identity, which is a user profile in the i5/OS registry on System A.
  - A target association for the DAYJO user identity, which is a user profile in the i5/OS registry on System B.
- For the Sharon Jones EIM identifier, these identifier associations are defined:
  - A source association for the sjones user identity, which is a Kerberos principal in the Windows 2000 server registry.
  - A target association for the SHARONJ user identity, which is a user profile in the i5/OS registry on System A.
  - A target association for the JONESSH user identity, which is a user profile in the i5/OS registry on System B.

Windows 2000 server

- Acts as the Kerberos server (`kdc1.myco.com`), also known as a key distribution center (KDC), for the network.
- The default realm for the Kerberos server is `MYCO.COM`.
- All Microsoft Windows Active Directory users that do not have identifier associations are mapped to a single i5/OS user profile on each of the System i platforms.

System A

- Runs i5/OS V5R3, or later, with the following options and licensed programs installed:
  - i5/OS Host Servers (5722-SS1 Option 12)
  - Qshell Interpreter (5722-SS1 Option 30)
  - iSeries Access for Windows (5722-XE1)
  - Network Authentication Enablement (5722-NAE) if you are using i5/OS V5R4
  - Cryptographic Access Provider (5722-AC3) if you are using i5/OS V5R3

  Note: You can implement this scenario using a system that runs OS/400 V5R2. However, some of the configuration steps are slightly different. In addition, this scenario demonstrates some of the single sign-on functions that are only available in i5/OS V5R3, and later, such as policy associations.
- The directory server on System A will be configured to be the EIM domain controller for the new EIM domain, MyCoEimDomain.
- Participates in the EIM domain, MyCoEimDomain.
- Has the service principal name of `krbsvr400/systema.myco.com@MYCO.COM`.

- Has the fully qualified host name of `systema.myco.com`. This name is registered in a single Domain Name System (DNS) to which all PCs and servers in the network point.
- Home directories on System A store the Kerberos credentials cache for i5/OS user profiles.

System B

- Runs i5/OS V5R3, or later, with the following options and licensed programs installed:
  - i5/OS Host Servers (5722-SS1 Option 12)
  - Qshell Interpreter (5722-SS1 Option 30)
  - iSeries Access for Windows (5722-XE1)
  - Network Authentication Enablement (5722-NAE) if you are using i5/OS V5R4, or later
  - Cryptographic Access Provider (5722-AC3) if you are running i5/OS V5R3
- Has the fully qualified host name of `systemb.myco.com`. This name is registered in a single Domain Name System (DNS) to which all PCs and servers in the network point.
- The principal name for System B is `krbsvr400/systemb.myco.com@MYCO.COM`.
- Participates in the EIM domain, MyCoEimDomain.
- Home directories on System B store the Kerberos credentials cache for i5/OS user profiles.

Administrative PC

- Runs Microsoft Windows 2000 operating system.
- Runs iSeries Access for Windows (5722-XE1).
- Runs iSeries Navigator with the following subcomponents installed:
  - Network
  - Security
  - Users and Groups
- Serves as the primary logon system for the administrator.
- Configured to be part of the MYCO.COM realm (Windows domain).

Prerequisites and assumptions

Successful implementation of this scenario requires that the following assumptions and prerequisites are met:

1. All system requirements, including software and operating system installation, have been verified.

   To verify that these licensed programs have been installed, follow these steps:

   a. In iSeries Navigator, expand *your system* → **Configuration and Service** → **Software** → **Installed Products**.

   b. Ensure that all the necessary licensed programs are installed.

   Note: The Network Authentication Service APIs support job environments for most EBCDIC CCSIDs. However, CCSID 290 and 5026 are not supported because of the variance of lowercase letters a to z.
2. All necessary hardware planning and setup are complete.
3. TCP/IP and basic system security are configured and tested on each system.
4. The directory server and EIM should not be previously configured on System A.

   Note: Instructions in this scenario are based on the assumption that the directory server has not been previously configured on System A. However, if you already configured the directory server, you can still use these instructions with only slight differences. These differences are noted in the appropriate places within the configuration steps.

5. A single DNS server is used for host name resolution for the network. Host tables are not used for host name resolution.

   Note: The use of host tables with Kerberos authentication might result in name resolution errors or other problems. For more detailed information about how host name resolution works with Kerberos authentication, see "Host name resolution considerations" on page 80.

Configuration steps

Note: You need to thoroughly understand the concepts related to single sign-on, which include network authentication service and Enterprise Identity Mapping (EIM) concepts, before you implement this scenario. See the following information to learn about the terms and concepts related to single sign-on:

- Enterprise Identity Mapping concepts
- Network authentication service concepts

To configure single sign-on on your system, complete these steps.

Related concepts

Single sign-on overview

Domains

Completing the planning work sheets

These planning work sheets demonstrate the information that you need to gather and the decisions you need to make as you prepare to configure the single sign-on function described by this scenario.

The following planning work sheets are tailored to fit this scenario based on the general single sign-on planning worksheets. To ensure a successful implementation, you must be able to answer Yes to all prerequisite items in the work sheet and you should gather all the information necessary to complete the work sheets before you perform any configuration tasks.

Note: The Network Authentication Service APIs support job environments for most EBCDIC CCSIDs. However, CCSID 290 and 5026 are not supported because of the variance of lowercase letters a to z.

Table 13. Single sign-on prerequisite work sheet

Prerequisite work sheet	Answers
Is your i5/OS V5R3 (5722-SS1), or later?	Yes
Are the following options and licensed programs installed on System A and System B? • i5/OS Host Servers (5722-SS1 Option 12) • Qshell Interpreter (5722-SS1 Option 30) • iSeries Access for Windows (5722-XE1) • Network Authentication Enablement (5722-NAE) if you are using i5/OS V5R4, or later • Cryptographic Access Provider (5722-AC3) if you are running i5/OS V5R3	Yes
Have you installed an application that is enabled for single sign-on on each of the PCs that will participate in the single sign-on environment? **Note:** For this scenario, all of the participating PCs have iSeries Access for Windows (5722-XE1) installed.	Yes

Table 13. Single sign-on prerequisite work sheet (continued)

Prerequisite work sheet	Answers
Is iSeries Navigator installed on the administrator's PC? • Is the Network subcomponent of iSeries Navigator that is installed on the PC used to administer single sign-on? • Is the Security subcomponent of iSeries Navigator that is installed on the PC used to administer single sign-on? • Is the Users and Groups subcomponent of iSeries Navigator that is installed on the PC used to administer single sign-on?	Yes
Have you installed the latest IBM eServer iSeries Access for Windows service pack? See the iSeries Access Web page for the latest service pack.	Yes
Does the single sign-on administrator have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities?	Yes
Do you have one of the following systems acting as the Kerberos server (also known as the KDC)? If yes, specify which system. 1. Microsoft Windows 2000 Server **Note:** Microsoft Windows 2000 Server uses Kerberos authentication as its default security mechanism. 2. Windows Server 2003 3. i5/OS PASE (V5R3 or later) 4. AIX server 5. z/OS	Yes, Windows 2000 Server
Are all your PCs in your network configured in a Windows 2000 domain?	Yes
Have you applied the latest program temporary fixes (PTFs)?	Yes
Is the System i system time within 5 minutes of the system time on the Kerberos server? If not, see "Synchronizing system times" on page 99.	Yes

You need this information to configure EIM and network authentication service on System A.

Table 14. Single sign-on configuration planning work sheet for System A

Configuration planning work sheet for System A	Answers
Use the following information to complete the EIM Configuration wizard. The information in this work sheet correlates with the information you need to supply for each page in the wizard:	
How do you want to configure EIM for your system? • Join an existing domain • Create and join a new domain	Create and join a new domain
Where do you want to configure the EIM domain?	On the local directory server **Note:** This will configure the directory server on the same system on which you are currently configuring EIM.
Do you want to configure network authentication service? **Note:** You must configure network authentication service to configure single sign-on.	Yes
The Network Authentication Service wizard starts from the EIM Configuration wizard. Use the following information to complete the Network Authentication Service wizard.	

Table 14. Single sign-on configuration planning work sheet for System A (continued)

Configuration planning work sheet for System A	Answers
What is the name of the Kerberos default realm to which your System i product will belong? **Note:** A Windows 2000 domain is similar to a Kerberos realm. Microsoft Windows Active Directory uses Kerberos authentication as its default security mechanism.	`MYCO.COM`
Are you using Microsoft Active Directory?	Yes
What is the Kerberos server, also known as a key distribution center (KDC), for this Kerberos default realm? What is the port on which the Kerberos server listens?	**KDC:** `kdc1.myco.com` **Port:** `88` **Note:** This is the default port for the Kerberos server.
Do you want to configure a password server for this default realm? If yes, answer the following questions: What is name of the password server for this Kerberos server? What is the port on which the password server listens?	Yes **Password server:** `kdc1.myco.com` **Port:** `464` **Note:** This is the default port for the password server.
For which services do you want to create keytab entries? • i5/OS Kerberos Authentication • LDAP • iSeries IBM HTTP Server • iSeries NetServer	i5/OS Kerberos Authentication
What is the password for your service principal or principals?	`systema123`
Do you want to create a batch file to automate adding the service principals for System A to the Kerberos registry?	Yes
Do you want to include passwords with the i5/OS service principals in the batch file?	Yes
As you exit the Network Authentication Service wizard, you will return to the EIM Configuration wizard. Use the following information to complete the EIM Configuration wizard:	
Specify user information that the wizard should use when configuring the directory server. This is the connection user. You must specify the port number, administrator distinguished name, and a password for the administrator. **Note:** Specify the LDAP administrator's distinguished name (DN) and password to ensure the wizard has enough authority to administer the EIM domain and the objects in it.	**Port:** `389` **Distinguished name:** `cn=administrator` **Password:** `mycopwd`
What is the name of the EIM domain that you want to create?	`MyCoEimDomain`
Do you want to specify a parent DN for the EIM domain?	No
Which user registries do you want to add to the EIM domain?	Local i5/OS--SYSTEMA.MYCO.COM Kerberos--KDC1.MYCO.COM **Note:** You should not select **Kerberos user identities are case sensitive** when the wizard presents this option.
Which EIM user do you want System A to use when performing EIM operations? This is the system user. **Note:** If you have not configured the directory server before configuring single sign-on, the only distinguished name (DN) you can provide for the system user is the LDAP administrator's DN and password.	**User type:** `Distinguished name` **Distinguished name:** `cn=administrator` **Password:** `mycopwd`

You need this information to allow System B to participate in the EIM domain and to configure network authentication service on System B.

Table 15. Single sign-on configuration planning work sheet for System B

Configuration planning work sheet for System B	Answers
Use the following information to complete the EIM Configuration wizard for System B:	
How do you want to configure EIM on your system?	Join an existing domain
Do you want to configure network authentication service? **Note:** You must configure network authentication service to configure single sign-on.	Yes
The Network Authentication Service wizard starts from the EIM Configuration wizard. Use the following information to complete the Network Authentication Service wizard: **Note:** You can start the Network Authentication Service wizard independently of the EIM Configuration wizard.	
What is the name of the Kerberos default realm to which your System i product will belong? **Note:** A Windows 2000 domain is equivalent to a Kerberos realm. Microsoft Active Directory uses Kerberos authentication as its default security mechanism.	`MYCO.COM`
Are you using Microsoft Active Directory?	Yes
What is the Kerberos server for this Kerberos default realm? What is the port on which the Kerberos server listens?	**KDC:** `kdc1.myco.com` **Port:** `88` **Note:** This is the default port for the Kerberos server.
Do you want to configure a password server for this default realm? If yes, answer the following questions: What is name of the password server for this Kerberos server? What is the port on which the password server listens?	Yes **Password server:** `kdc1.myco.com` **Port:** `464` **Note:** This is the default port for the password server.
For which services do you want to create keytab entries? • i5/OS Kerberos Authentication • LDAP • iSeries IBM HTTP Server • iSeries NetServer	i5/OS Kerberos Authentication
What is the password for your i5/OS service principals?	systemb123
Do you want to create a batch file to automate adding the service principals for System B to the Kerberos registry?	Yes
Do you want to include passwords with the i5/OS service principals in the batch file?	Yes
As you exit the Network Authentication Service wizard, you will return to the EIM Configuration wizard. Use the following information to complete the EIM Configuration wizard for System B:	
What is the name of the EIM domain controller for the EIM domain that you want to join?	systema.myco.com
Do you plan on securing the connection with SSL or TLS?	No
What is the port on which the EIM domain controller listens?	389
Which user do you want to use to connect to the domain controller? This is the connection user. **Note:** Specify the LDAP administrator's distinguished name (DN) and password to ensure the wizard has enough authority to administer the EIM domain and the objects in it.	**User type:** `Distinguished name and password` **Distinguished name:** `cn=administrator` **Password:** `mycopwd`
What is the name of the EIM domain that you want to join?	`MyCoEimDomain`

Table 15. Single sign-on configuration planning work sheet for System B (continued)

Configuration planning work sheet for System B	Answers
Do you want to specify a parent DN for the EIM domain?	No
What is the name of the user registry that you want to add to the EIM domain?	Local i5/OS--SYSTEMB.MYCO.COM
Which EIM user do you want System B to use when performing EIM operations? This is the system user. **Note:** Earlier in this scenario, you used the EIM Configuration wizard to configure the directory server on System A. In doing so, you created a distinguished name (DN) and password for the LDAP administrator. This is currently the only DN defined for the directory server. Therefore, this is the DN and password that you must supply here.	**User type:** `Distinguished name and password` **Distinguished name:** `cn=administrator` **Password:** `mycopwd`

Table 16. Single sign-on configuration planning work sheet - user profiles

i5/OS user profile name	Password is specified	Special authority (Privilege class)	System
SYSUSERA	No	User	System A
SYSUSERB	No	User	System B

Table 17. Single sign-on configuration planning work sheet - EIM domain data

Identifier name	User registry	User identity	Association type	Identifier description
John Day	MYCO.COM	jday	Source	Kerberos (Windows 2000) login user identity
John Day	SYSTEMA.MYCO.COM	JOHND	Target	i5/OS user profile on System A
John Day	SYSTEMB.MYCO.COM	DAYJO	Target	i5/OS user profile on System B
Sharon Jones	MYCO.COM	sjones	Source	Kerberos (Windows 2000) login user identity
Sharon Jones	SYSTEMA.MYCO.COM	SHARONJ	Target	i5/OS user profile on System A
Sharon Jones	SYSTEMB.MYCO.COM	JONESSH	Target	i5/OS user profile on System B

Table 18. Single sign-on configuration planning work sheet - EIM domain data - policy associations

Policy association type	Source user registry	Target user registry	User identity	Description
Default registry	MYCO.COM	SYSTEMA.MYCO.COM	SYSUSERA	Maps authenticated Kerberos user to appropriate i5/OS user profile
Default registry	MYCO.COM	SYSTEMB.MYCO.COM	SYSUSERB	Maps authenticated Kerberos user to appropriate i5/OS user profile

Creating a basic single sign-on configuration for System A

The EIM Configuration wizard helps you create a basic EIM configuration. It also opens the Network Authentication Service wizard that you use to create a basic network authentication service configuration.

Note: Instructions in this scenario are based on the assumption that the directory server has not been previously configured on System A. However, if you already configured the directory server, you can still use these instructions with only slight differences. These differences are noted in the appropriate places within the configuration steps.

Use the information from your work sheets to configure EIM and network authentication service on System A. When you complete this step, you accomplish the following tasks:

- Create a new EIM domain.
- Configure the directory server on System A to be the EIM domain controller.
- Configure network authentication service.
- Create EIM registry definitions for the i5/OS registry and the Kerberos registry on System A.
- Configure System A to participate in the EIM domain.

1. In iSeries Navigator, expand **System A → Network → Enterprise Identity Mapping**.
2. Right-click **Configuration** and select **Configure** to start the EIM configuration wizard.
3. On the Welcome page, select **Create and join a new domain**. Click **Next**.
4. On the Specify EIM Domain Location page, select **On the local Directory server**. Click **Next**.
5. Complete these tasks to configure network authentication service:
   a. On the Configure Network Authentication Service page, select **Yes**.

      Note: This starts the Network Authentication Service wizard. With this wizard, you can configure several i5/OS interfaces and services to participate in the Kerberos realm.

   b. On the Specify Realm Information page, enter `MYCO.COM` in the **Default realm** field and select **Microsoft Active Directory is used for Kerberos authentication**. Click **Next**.
   c. On the Specify KDC Information page, enter `kdc1.myco.com` for the name of the Kerberos server in the **KDC** field and enter `88` in the **Port** field. Click **Next**.
   d. On the Specify Password Server Information page, select **Yes**. Enter `kdc1.myco.com` in the **Password server** field and `464` in the **Port** field. Click **Next**.
   e. On the Select Keytab Entries page, select **i5/OS Kerberos Authentication**. Click **Next**.
   f. On the Create i5/OS Keytab Entry page, enter and confirm a password, and click **Next**. For example, `systema123`. This password is used when the System A service principal is added to the Kerberos server.

      Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

   g. On the Create Batch File page, select **Yes**, specify the following information, and click **Next**:
      - **Batch file:** Add the text `systema` to the end of the default batch file name. For example, `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystema.bat`.
      - Select **Include password**. This ensures that all passwords associated with the i5/OS service principal are included in the batch file. It is important to note that passwords are displayed in clear text and can be read by anyone with read access to the batch file. Therefore, it is recommended that you delete the batch file from the Kerberos server and from your PC immediately after use.

        Note: If you do not include the password, you will be prompted for the password when the batch file is run.

h. On the Summary page, review the network authentication service configuration details. Click **Finish**.

6. On the Configure Directory Server page, enter the following information, and click **Next**:

   Note: If you configured the directory server before you started this scenario, you will see the Specify User for Connection page instead of the Configure Directory Server page. In that case, you must specify the distinguished name and password for the LDAP administrator.

   - **Port**: `389`
   - **Distinguished name**: `cn=administrator`
   - **Password:** `mycopwd`

     Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

7. On the Specify Domain page, enter the name of the domain in the **Domain** field. For example, `MyCoEimDomain`.
8. On the Specify Parent DN for Domain page, select **No**. Click **Next**.

   Note: If the directory server is active, a message is displayed that indicates that you need to end and restart the directory server for the changes to take effect. Click **Yes** to restart the directory server.

9. On the Registry Information page, select **Local i5/OS** and **Kerberos**. Click **Next**. Write down the registry names. You will need these registry names when you create associations to EIM identifiers.

   Note:

   - Registry names must be unique to the domain.
   - You can enter a specific registry definition name for the user registry if you want to use a specific registry definition naming plan. However, for this scenario you can accept the default values.

10. On the Specify EIM System User page, select the user the operating system uses when performing EIM operations on behalf of operating system functions, and click **Next**:

    Note: Because you did not configure the directory server before performing the steps in this scenario, the only distinguished name (DN) that you can choose is the LDAP administrator's DN.

    - **User type**: `Distinguished name and password`
    - **Distinguished name**: `cn=administrator`
    - **Password**: `mycopwd`

      Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

11. On the **Summary** page, confirm the EIM configuration information. Click **Finish**.

Configuring System B to participate in the EIM domain and configuring System B for network authentication service

After you have created a new domain and configured network authentication service on System A, you need to configure System B to participate in the EIM domain and configure network authentication service on System B.

Use the information from your work sheets to complete this step.

1. In iSeries Navigator, expand **System B → Network → Enterprise Identity Mapping**.

2. Right-click **Configuration** and select **Configure** to start the configuration wizard.
3. On the Welcome page, select **Join an existing domain**. Click **Next**.
4. Complete these tasks to configure network authentication service.
   a. On the Configure Network Authentication Service page, select **Yes**.

      Note: This starts the Network Authentication Service wizard. This wizard allows you to configure several i5/OS interfaces and services to participate in a Kerberos network.
   b. On the Specify Realm Information page, enter `MYCO.COM` in the **Default realm** field and select **Microsoft Active Directory is used for Kerberos authentication**. Click **Next**.
   c. On the Specify KDC Information page, enter `kdc1.myco.com` for the name of the Kerberos server in the **KDC** field and enter `88` in the **Port** field. Click **Next**.
   d. On the Specify Password Server Information page, select **Yes**. Enter `kdc1.myco.com` in the **Password server** field and `464` in the **Port** field. Click **Next**.
   e. On the Select Keytab Entries page, select **i5/OS Kerberos Authentication**. Click **Next**.
   f. On the Create i5/OS Keytab Entry page, enter and confirm a password, and click **Next**. For example, type `systema123`. This password will be used when the System A service principal is added to the Kerberos server.

      Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.
   g. Optional: On the Create Batch File page, select **Yes**, specify the following information, and click **Next**:
      - **Batch file:** Add the text `systemb` to the end of the default batch file name. For example, type `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystemb.bat`.
      - Select **Include password**. This ensures that all passwords associated with the i5/OS service principal are included in the batch file. It is important to note that passwords are displayed in clear text and can be read by anyone with read access to the batch file. Therefore, it is recommended that you delete the batch file from the Kerberos server and from your PC immediately after use.

        Note: If you do not include the password, you will be prompted for the password when the batch file is run.
   h. On the Summary page, review the network authentication service configuration details. Click **Finish**.
5. On the Specify Domain Controller page, specify the following information, and click **Next**:
   - **Domain controller name**: `systema.myco.com`
   - **Port**: `389`
6. On the Specify User for Connection page, specify the following information, and click **Next**:

   Note: Specify the LDAP administrator's DN and password that you created earlier in this scenario on System A.
   a. **User type**: `Distinguished name and password`
   b. **Distinguished name**: `cn=administrator`
   c. **Password**: `mycopwd`

      Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.
7. On the Specify Domain page, select the name of the domain that you want to join. Click **Next**. For example, `MyCoEimDomain`.

8. On the Registry Information page, select **Local i5/OS** and deselect **Kerberos registry**. (The Kerberos registry was created when you created the MyCoEimDomain domain.) Click **Next**. Write down the registry names. You will need these registry names when you create associations to EIM identifiers.

   Note:
   - Registry names must be unique to the domain.
   - You can enter a specific registry definition name for the user registry if you want to use a specific registry definition naming plan. However, for this scenario you can accept the default values.

9. On the Specify EIM System User page, select the user the operating system uses when performing EIM operations on behalf of operating system functions, and click **Next**:

   Note: Specify the LDAP administrator's DN and password that you created earlier in this scenario on System A.

   a. **User type**: `Distinguished name and password`
   b. **Distinguished name**: `cn=administrator`
   c. **Password**: `mycopwd`

   Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

10. On the Summary page, confirm the EIM configuration. Click **Finish**.

Adding both i5/OS service principals to the Kerberos server

You can manually add the necessary i5/OS service principals to the Kerberos server. As this scenario illustrates, you can also use a batch file to add them.

You created this batch file in step 2. To use this file, you can use File Transfer Protocol (FTP) to copy the file to the Kerberos server and run it.

To use the batch file to add principal names to the Kerberos server, follow these steps:

1. Create FTP batch files
   a. On the Windows 2000 workstation that the administrator used to configure network authentication service, open a command prompt and type `ftp kdc1.myco.com`. This starts an FTP session on your PC. You will be prompted for the administrator's user name and password.
   b. At the FTP prompt, type `lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access"`. Press Enter. You should receive the message `Local directory now C:\Documents and Settings\All Users\Documents\IBM\Client Access`.
   c. At the FTP prompt, type `cd \`*`mydirectory`*, where *mydirectory* is a directory located on kdc1.myco.com.
   d. At the FTP prompt, type `put NASConfigsystema.bat`. You should receive this message: `226 Transfer complete`.
   e. Type `quit` to exit the FTP session.
2. Run both batch files on kdc1.myco.com
   a. On your Windows 2000 server, open the directory where you transferred the batch files.
   b. Find the `NASConfigsystema.bat` file and double-click the file to run it.
   c. Repeat steps 1.a through 2.b for `NASConfigsystemb.bat`.
   d. After each file runs, verify that the i5/OS principal has been added to the Kerberos server by completing the following steps:
      1) On your Windows 2000 server, expand **Administrative Tools** → **Active Directory Users and Computers** → **Users**.

2) Verify the System i platform has a user account by selecting the appropriate Windows 2000 domain.

   Note: This Windows 2000 domain should be the same as the default realm name that you specified in the network authentication service configuration.

3) In the list of users that is displayed, find **systema_1_krbsvr400** and **systemb_1_krbsvr400**. These are the user accounts generated for the i5/OS principal name.

4) Access the properties on your Active Directory users. From the **Account** tab, select **Account is trusted for delegation**.

   Note: This optional step enables your system to delegate, or forward, a user's credentials to other systems. As a result, the i5/OS service principal can access services on multiple systems on behalf of the user. This is useful in a multi-tier network.

Creating user profiles on Systems A and B

You want all of your users in the MYCO.COM Kerberos registry to map to a single i5/OS user profile on each of your System i platforms. Therefore, you need to create an i5/OS user profile on System A and System B.

Use the information from your work sheets to create a user profile for these users:

1. In iSeries Navigator, expand **System A → User and Groups**.
2. Right-click **All Users**, and select **New User**.
3. On the **New User** dialog box, enter `SYSUSERA` in the **User name** field.
4. In the **Password** field, select **No password (sign-on not allowed)**.
5. Click **Capabilities**.
6. On the Privileges page, select **User** in the **Privilege class** field. Click **OK** and click **Add**.
7. Repeat steps 1 through 6 on System B, but enter `SYSUSERB` in the **User name** field.

Creating home directories on Systems A and B

Each user that connects to i5/OS and i5/OS applications needs a directory in the /home directory. This directory stores the user's Kerberos credentials cache.

To create a home directory for a user, follow these steps:

1. On the System A command line, enter `CRTDIR '/home/user profile'`, where `user profile` is the i5/OS user profile name for the user. For example: `CRTDIR '/home/SYSUSERA'`.
2. Repeat this command on System B but specify `SYSUSERB` to create a home directory for the user profile on System B.

Testing network authentication service on Systems A and B

After you complete the network authentication service configuration tasks for both of your systems, you need to verify that your configurations work correctly for both System A and System B.

You can do this testing by completing these steps to request a ticket-granting ticket for the System A and System B principals:

Note: Ensure that you have created a home directory for your i5/OS user profile before performing this procedure.

1. On a command line, enter `QSH` to start the Qshell Interpreter.
2. Enter `keytab list` to display a list of principals registered in the keytab file. In this scenario, krbsvr400/systema.myco.com@MYCO.COM should display as the principal name for System A.
3. Enter `kinit -k krbsvr400/systema.myco.com@MYCO.COM` to request a ticket-granting ticket from the Kerberos server. By running this command, you can verify that your system has been configured

properly and that the password in the keytab file matches the password stored on the Kerberos server. If this is successful, the kinit command displays without errors.

4. Enter `klist` to verify that the default principal is krbsvr400/systema.myco.com@MYCO.COM. This command displays the contents of a Kerberos credentials cache and verifies that a valid ticket has been created for the i5/OS service principal and placed within the credentials cache on the system.

```
Ticket cache: FILE:/QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/creds/krbcred

Default principal: krbsvr400/systema.myco.com@MYCO.COM

Server: krbtgt/MYCO.COM@MYCO.COM
  Valid 200X/06/09-12:08:45 to 20XX/11/05-03:08:45
$
```

Creating EIM identifiers for two administrators, John Day and Sharon Jones

As part of setting up your single sign-on test environment, you need to create EIM identifiers for two of your administrators so they can both log on to i5/OS using their Windows user identities.

In this scenario, you create two EIM identifiers, one named John Day and the other named Sharon Jones. To create the EIM identifiers, follow these steps:

1. In iSeries Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain**.

   Note: You might be prompted to connect to the domain controller. In that case, the **Connect to EIM Domain Controller** dialog box is displayed. You must connect to the domain before you can perform actions in it. To connect to the domain controller, provide the following information and click **OK**:

   a. **User type**: `Distinguished name`
   b. **Distinguished name**: `cn=administrator`
   c. **Password**: `mycopwd`

      Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

2. Right-click **Identifiers** and select **New Identifier**.
3. On the **New EIM Identifier** dialog box, enter `John Day` in the **Identifier** field. Click **OK**.
4. Repeat steps 2 through 4, but enter `Sharon Jones` in the **Identifier** field.

Creating identifier associations for John Day

You must create the appropriate associations between the EIM identifier, John Day, and the user identities that the person represented by the identifier uses. These identifier associations, when properly configured, enable the user to participate in a single sign-on environment.

In this scenario, you need to create one source association and two target associations for the John Day identifier:

- A source association for the jday Kerberos principal, which is the user identity that John Day uses to log in to Windows and the network. The source association allows the Kerberos principal to be mapped to another user identity as defined in a corresponding target association.
- A target association for the JOHND i5/OS user profile, which is the user identity that John Day uses to log in to iSeries Navigator and other i5/OS applications on System A. The target association specifies that a mapping lookup operation can map to this user identity from another one as defined in a source association for the same identifier.

- A target association for the DAYJO i5/OS user profile, which is the user identity that John Day uses to log in to iSeries Navigator and other i5/OS applications on System B. The target association specifies that a mapping lookup operation can map to this user identity from another one as defined in a source association for the same identifier.

Use the information from your planning work sheets to create the associations.

To create the source association for John Day's Kerberos principal, follow these steps:

1. On System A, expand **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain** → **Identifiers**.
2. Right-click **John Day** and select **Properties**.
3. On the Associations page, click **Add**.
4. In the **Add Association** dialog box, specify or click **Browse** to select the following information, and click **OK**:
   a. **Registry**: `MYCO.COM`
   b. **User**: `jday`
   c. **Association type**: `Source`
5. Click **OK** to close the **Add Associations** dialog box.

   To create a target association for John Day's i5/OS user profile on System A, follow these steps:
6. On the Associations page, click **Add**.
7. In the **Add Association** dialog box, specify or click **Browse** to select the following information, and click **OK**:
   a. **Registry**: `SYSTEMA.MYCO.COM`
   b. **User**: `JOHND`
   c. **Association type**: `Target`
8. Click **OK** to close the **Add Associations** dialog box.

   To create a target association for John Day's i5/OS user profile on System B, follow these steps:
9. On the Associations page, click **Add**.
10. In the **Add Association** dialog box, specify or click **Browse** to select the following information, and click **OK**:
    a. **Registry**: `SYSTEMB.MYCO.COM`
    b. **User**: `DAYJO`
    c. **Association type**: `Target`
11. Click **OK** to close the **Add Associations** dialog box.
12. Click **OK** to close the **Properties** dialog box.

Creating identifier associations for Sharon Jones

You must create the appropriate associations between the EIM identifier, Sharon Jones, and the user identities that the person represented by the identifier uses. These associations, when properly configured, enable the user to participate in a single sign-on environment.

In this scenario, you need to create one source association and two target associations for the Sharon Jones identifier:

- A source association for the sjones Kerberos principal, which is the user identity that Sharon Jones uses to log in to Windows and the network. The source association allows the Kerberos principal to be mapped to another user identity as defined in a corresponding target association.
- A target association for the SHARONJ i5/OS user profile, which is the user identity that Sharon Jones uses to log in to iSeries Navigator and other i5/OS applications on System A. The target association specifies that a mapping lookup operation can map to this user identity from another one as defined in a source association for the same identifier.

- A target association for the JONESSH i5/OS user profile, which is the user identity that Sharon Jones uses to log in to iSeries Navigator and other i5/OS applications on System B. The target association specifies that a mapping lookup operation can map to this user identity from another one as defined in a source association for the same identifier.

Use the information from your planning work sheets to create the associations:

To create the source association for Sharon Jones's Kerberos principal, follow these steps:

1. On System A, expand **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain** → **Identifiers**.
2. Right-click **Sharon Jones** and select **Properties**.
3. On the Associations page, click **Add**.
4. On the **Add Association** dialog box, specify or **Browse** to select the following information, and click **OK**:
   a. **Registry**: `MYCO.COM`
   b. **User**: `sjones`
   c. **Association type**: `Source`
5. Click **OK** to close the **Add Associations** dialog box.

   To create a target association to Sharon Jones' i5/OS user profile on System A, follow these steps:
6. On the Associations page, click **Add**.
7. On the **Add Association** dialog box, specify or **Browse** to select the following information, and click **OK**:
   a. **Registry**: `SYSTEMA.MYCO.COM`
   b. **User**: `SHARONJ`
   c. **Association type**: `Target`
8. Click **OK** to close the **Add Associations** dialog box.

   To create a target association to Sharon Jones' i5/OS user profile on System B, follow these steps:
9. On the Associations page, click **Add**.
10. On the **Add Association** dialog box, specify or **Browse** to select the following information, and click **OK**:
    a. **Registry**: `SYSTEMB.MYCO.COM`
    b. **User**: `JONESSH`
    c. **Association type**: `Target`
11. Click **OK** to close the **Add Associations** dialog box.
12. Click **OK** to close the **Properties** dialog box.

Creating default registry policy associations

You can use policy associations to create mappings directly between a group of users and a single target user identity.

You want to have all your Microsoft Active Directory users on the Windows 2000 server map to the user profile SYSUSERA on System A and to the user profile SYSUSERB on System B. In this case, you can create a default registry policy association that maps all the user identities (for which no identifier associations exist) in the MYCO.COM Kerberos registry to a single i5/OS user profile on System A.

You need two policy associations to accomplish this goal. Each policy association uses the MYCO.COM user registry definition as the source of the association. However, each policy association maps user identities in this registry to different target user identities, depending on which System i platform the Kerberos user accesses:

- One policy association maps the Kerberos principals in the MYCO.COM user registry to a target user of SYSUSERA in the target registry of SYSTEMA.MYCO.COM.
- The other policy association maps the Kerberos principals in the MYCO.COM user registry to a target user of SYSUSERB in the target registry of SYSTEMB.MYCO.COM.

Use the information from your planning works sheets to create two default registry policy associations.

Before you can use policy associations, you must first enable the domain to use policy associations for mapping lookup operations.

To enable the domain to use policy associations for mapping lookup operations, complete the following steps:

1. In iSeries Navigator, expand **System A → Network → Enterprise Identity Mapping → Domain Management**.
2. Right-click **MyCoEimDomain**, and select **Mapping policy**.
3. On the General page, select the **Enable mapping lookups using policy associations for domain MyCoEimDomain**.

To create the default registry policy association for the users to map to the SYSUSERA user profile on System A, complete the following steps:

1. On the Registry page, click **Add**.
2. In the **Add Default Registry Policy Association** dialog box, specify or **Browse** to select the following information, and click **OK**:
   a. **Source registry**: `MYCO.COM`
   b. **Target registry**: `SYSTEMA.MYCO.COM`
   c. **Target user**: `SYSUSERB`
3. Click **OK** to close the **Mapping Policy** dialog box.

To create the default registry policy association for the users to map to the SYSUSERB user profile on System B, complete the following steps:

1. On the Registry page, click **Add**.
2. In the **Add Default Registry Policy Association** dialog box, specify or **Browse** to select the following information, and click **OK**:
   a. **Source registry**: `MYCO.COM`
   b. **Target registry**: `SYSTEMB.MYCO.COM`
   c. **Target user**: `SYSUSERB`
3. Click **OK** to close the **Mapping Policy** dialog box.

Enabling registries to participate in lookup operations and to use policy associations

To use policy associations for a registry, you must enable their use for that registry as well as enable that registry to participate in lookup operations.

EIM allows you to control how each registry participates in EIM. Because a policy association can have a large scale effect within an enterprise, you can control whether a registry can be affected by policy associations. Also, you can control whether a registry can participate in mapping lookup operations at all.

To enable registries to use policy associations and participate in lookup operations, complete the following procedures:

To enable the MYCO.COM registry to participate in mapping lookup operations, follow these steps:

1. In iSeries Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain** → **User registries**.
2. Right-click the **MYCO.COM** registry and select **Mapping Policy**.
3. On the General page, select **Enable mapping lookups for registry MYCO.COM**, and click **OK**.

   To enable the SYSTEMA.MYCO.COM registry to participate in mapping lookup operations and to use policy associations, follow these steps:
4. In iSeries Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain** → **User registries**.
5. Right-click the **SYSTEMA.MYCO.COM** registry and select **Mapping Policy**.
6. On the General page, select **Enable mapping lookups for registry SYSTEMA.MYCO.COM**, select **Use policy associations**, and click **OK**.
7. Repeat steps 1 through 6 to enable the SYSTEMB.MYCO.COM registry to participate in mapping lookup operations and to use policy associations, but on the General page, select **Enable mapping lookups for registry SYSTEMB.MYCO.COM**, select **Use policy associations**, and click **OK**.

Testing EIM identity mappings

Now that you have created all the associations that you need, you must verify that EIM mapping lookup operations return the correct results based on the configured associations.

For this scenario, you must test the mappings used for the identifier associations for each of the administrators and you must test the mappings used for the default registry policy associations. To test the EIM mappings, follow these steps:

Test mappings for John Day

To test that identifier mappings work as expected for John Day, follow these steps:

1. In iSeries Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain**.

   Note: You might be prompted to connect to the domain controller. In that case, the **Connect to EIM Domain Controller** dialog box is displayed. You must connect to the domain before you can perform actions in it. To connect to the domain controller, provide the following information and click **OK**:

   a. **User type**: `Distinguished name`
   b. **Distinguished name**: `cn=administrator`
   c. **Password**: `mycopwd`

      Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.
2. Right-click **MyCoEimDomain** and select **Test a mapping**.
3. On the **Test a mapping** dialog box, specify or click **Browse** to select the following information, and click **Test**:

   a. **Source registry**: `MYCO.COM`
   b. **Source user**: `jday`
   c. **Target registry**: `SYSTEMA.MYCO.COM`

   Results will display in the **Mapping found** portion of the page, as follows:

For these fields	See these results
Target user	JOHND
Origin	EIM Identifier: John Day

4. Click **Close**.
5. Repeat these steps but select `SYSTEMB.MYCO.COM` for the **Target registry** field. Results will display in the **Mapping found** portion of the page, as follows:

For these fields	See these results
Target user	DAYJO
Origin	EIM Identifier: John Day

Test mappings for Sharon Jones

To test the mappings used for the individual associations for Sharon Jones, follow these steps:

6. In iSeries Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain**.

   Note: You might be prompted to connect to the domain controller. In that case, the **Connect to EIM Domain Controller** dialog box is displayed. You must connect to the domain before you can perform actions in it. To connect to the domain controller, provide the following information and click **OK**:

   a. **User type**: `Distinguished name`
   b. **Distinguished name**: `cn=administrator`
   c. **Password**: `mycopwd`

   Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.
7. Right-click **MyCoEimDomain** and select **Test a mapping**.
8. On the **Test a mapping** dialog box, specify or click **Browse** to select the following information, and click **Test**:
   a. **Source registry**: `MYCO.COM`
   b. **Source user**: `sjones`
   c. **Target registry**: `SYSTEMA.MYCO.COM`

   Results will display in the **Mapping found** portion of the page, as follows:

For these fields	See these results
Target user	SHARONJ
Origin	EIM Identifier: Sharon Jones

9. Click **Close**.
10. Repeat steps through 1 to 9 but select `SYSTEMB.MYCO.COM` for the **Target registry** field. Results are displayed in the **Mapping found** portion of the page, as follows:

For these fields	See these results
Target user	JONESSH
Origin	EIM Identifier: Sharon Jones

Test mappings used for default registry policy associations

To test that mappings work as expected for the users in the Order Receiving Department, as based on the policy associations that you defined, follow these steps:

11. In iSeries Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain**.

Note: You might be prompted to connect to the domain controller. In that case, the **Connect to EIM Domain Controller** dialog box is displayed. You must connect to the domain before you can perform actions in it. To connect to the domain controller, provide the following information and click **OK**:

a. **User type**: `Distinguished name`
b. **Distinguished name**: `cn=administrator`
c. **Password**: `mycopwd`

Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.

12. Right-click **MyCoEimDomain** and select **Test a mapping**.
13. On the **Test a mapping** dialog box, specify or click **Browse** to select the following information, and click **Test**:
    a. **Source registry**: `MYCO.COM`
    b. **Source user**: `mmiller`
    c. **Target registry**: `SYSTEMA.MYCO.COM`

    Results are displayed in the **Mapping found** portion of the page, as follows:

For these fields	See these results
Target user	SYSUSERA
Origin	Registry policy association

14. Click **Close**.

To test the mappings used for the default registry policy association that maps your users to the SYSUSERB profile on System B, follow these steps:

1. In iSeries Navigator, expand **System A** → **Network** → **Enterprise Identity Mapping** → **Domain Management** → **MyCoEimDomain**.

   Note: You might be prompted to connect to the domain controller. In that case, the **Connect to EIM Domain Controller** dialog box is displayed. You must connect to the domain before you can perform actions in it. To connect to the domain controller, provide the following information and click **OK**:

   a. **User type**: `Distinguished name`
   b. **Distinguished name**: `cn=administrator`
   c. **Password**: `mycopwd`

   Note: Any and all passwords specified in this scenario are for example purposes only. To prevent a compromise to your system or network security, you should never use these passwords as part of your own configuration.
2. Right-click **MyCoEimDomain** and select **Test a mapping**.
3. On the **Test a mapping** dialog box, specify or click **Browse** to select the following information, and click **Test**:
   a. **Source registry**: `MYCO.COM`
   b. **Source user**: `ksmith`
   c. **Target registry**: `SYSTEMB.MYCO.COM`

Results are displayed in the **Mapping found** portion of the page, as follows:

For these fields	See these results
Target user	SYSUSERB
Origin	Registry policy association

4. Click **Close**. If you receive messages or errors that indicate problems with your mappings or with communications, see Troubleshooting EIM to help you find solutions to these problems.

Configuring iSeries Access for Windows applications to use Kerberos authentication

Based on your single sign-on objectives, all users in the Order Receiving department must use Kerberos to authenticate before they can use iSeries Navigator to access Systems A and B. Therefore, you need to configure iSeries Access for Windows to use Kerberos authentication.

To configure iSeries Access for Windows applications to use Kerberos authentication, follow these steps:

Note: All of your users need to perform all of these steps on their own PCs.

1. Log on to the Windows 2000 domain by signing in to the PC.
2. In iSeries Navigator on the PC, right-click **System A** and select **Properties**.
3. On the Connection page, select **Use Kerberos principal name, no prompting**. This allows iSeries Access for Windows connections to use the Kerberos principal name and password for authentication.
4. A message is displayed that indicates you need to close and restart all applications that are currently running for the changes to the connection settings to take effect. Click **OK**. Then, end and restart iSeries Navigator.
5. Repeat these steps for System B.

Verifying network authentication service and EIM configuration

Now that you have verified the individual pieces of your single sign-on configuration and ensured that all setup is complete, you must verify that you have configured Enterprise Identity Mapping (EIM) and network authentication service correctly and that single sign-on works as expected.

To verify that your single sign-on environment works correctly, have John Day follow these steps:

1. In iSeries Navigator, expand **System A** to open a connection to System A.
2. Press F5 to refresh the screen.
3. In the right pane, find `System A` in the **Name** column, and verify that John Day's i5/OS user profile, `JOHND`, is displayed as the corresponding entry in the **Signed On User** column. iSeries Navigator successfully used EIM to map the jday Kerberos principal to the JOHND System A user profile because of the associations defined for EIM identifier, John Day. The iSeries Navigator session for System A is now connected as JOHND.
4. Repeat these steps for Sharon Jones and for at least one of the user identities that is mapped to the SYSUSERA or SYSUSERB user profile.

Post configuration considerations

The number of additional EIM users that you define depends on your security policy's emphasis on the separation of security duties and responsibilities.

Now that you finished this scenario, the only EIM user you have defined that EIM can use is the DN for the LDAP administrator. The LDAP administrator DN that you specified for the system user on Systems A and B has a high level of authority to all data on the directory server. Therefore, you might consider creating one or more DNs as additional users that have more appropriate and limited access control for EIM data. Typically, you might create at least the two following types of DNs:

- **A user that has EIM administrator access control**

This EIM administrator DN provides the appropriate level of authority for an administrator who is responsible for managing the EIM domain. This EIM administrator DN can be used to connect to the domain controller when managing all aspects of the EIM domain by means of iSeries Navigator.

- **At least one user that has all of the following access controls**:
  - Identifier administrator
  - Registry administrator
  - EIM mapping operations

  This user provides the appropriate level of access control required for the system user that performs EIM operations on behalf of the operating system.

Note: To use this new DN for the system user instead of the LDAP administrator DN, you must change the EIM configuration properties for each system. For this scenario, you need to change the EIM configuration properties for both Systems A and B. See the information about managing EIM configuration properties to learn how to change the system user DN.

Related concepts

EIM access control

IBM Directory Server for iSeries (LDAP)

Related tasks

Managing EIM configuration properties

Planning network authentication service

Before implementing network authentication service or a Kerberos solution on your network, it is essential to complete the necessary planning tasks.

To plan network authentication service and a Kerberos implementation, you need to gather the appropriate information about the systems and users on your network. Several planning work sheets have been provided to help you to configure network authentication service in your network.

Note: Many different Kerberos authentication solutions exist and can be used in your enterprise. This information focuses on planning an i5/OS implementation and considerations when you use network authentication service with a Kerberos server configured in Microsoft Windows Active Directory or i5/OS PASE.

For information about setting up a Kerberos server in Microsoft Windows Active Directory, see Windows 2000 Server .

The following IBM systems support Kerberos authentication. For information about platform-specific Kerberos implementation, see the following sources:

- **System p™**
  - *IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide.*
  - *IBM Network Authentication Service AIX, Linux, and Solaris Application Development Reference.*

  Note: You can find this documentation in the AIX 5L Expansion Pack and Bonus Pack CD .
- **System z™**
  - z/OS Security Server Network Authentication Service Administration

Use these tasks to help you plan network authentication service.

Planning a Kerberos server

Plan for a Kerberos server based on your operating system.

A Kerberos server or key distribution center (KDC) maintains a database of principals and their associated passwords. It is composed of the authentication server and the ticket-granting server. When a principal logs into a Kerberos network, the authentication server validates the principal and sends them a ticket-granting ticket. When planning to use Kerberos authentication, you need to decide what system you want to configure as a Kerberos server.

Note: The network authentication service information focuses on Kerberos servers that run in either i5/OS PASE or Windows 2000 server. Most scenarios and examples assume that a Windows 2000 server has been configured as a Kerberos server, unless explicitly mentioned otherwise. If you are using any of these other operating systems or third-party applications for Kerberos authentication, see the corresponding documentation.

The following list provides details on Kerberos server support on three key operating systems:

Microsoft Windows 2000 and Windows Server 2003

Both Microsoft Windows 2000 and Windows Server 20003 operating systems support Kerberos authentication as their default security mechanism. When administrators add users and services though Microsoft Windows Active Directory, they are in effect creating Kerberos principals for those users and services. If you have a Windows 2000 or 2003 server in your network, you have a Kerberos server built into those operating systems. For information about how Kerberos authentication is used on Microsoft Windows servers, see Windows 2000 Server.

AIX and i5/OS PASE

Both AIX and i5/OS PASE support a Kerberos server through the kadmin command. Administrators need to enter the PASE environment (by entering `call QP2TERM`) to configure and manage the PASE Kerberos server. i5/OS PASE provides a run-time environment for AIX applications, such as a Kerberos server. The following documentation can help you configure and manage a Kerberos server in AIX.

- *IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide*.
- *IBM Network Authentication Service AIX, Linux, and Solaris Application Development Reference*.

Note: You can find this documentation in the AIX 5L Expansion Pack and Bonus Pack CD.

z/OS Security Server Network Authentication Service for z/OS is the IBM z/OS program based on Kerberos Version 5. Network Authentication Service for z/OS provides Kerberos security services without requiring that you purchase or use a middleware program. These services support for a native Kerberos server. See z/OS Security Server Network Authentication Service Administration for details on configuring and managing a z/OS Kerberos server.

No matter what operating system provides the Kerberos server, you need to determine the server ports for the Kerberos server, secure access to the Kerberos server, and ensure that time between clients and the Kerberos server are synchronized.

Determining server ports

Network authentication service uses port 88 as the default for the Kerberos server. However, other ports can be specified in the configuration files of the Kerberos server. You should verify the port number in the Kerberos configuration files located on the Kerberos server.

Securing access to the Kerberos server

The Kerberos server should be located on a secure, dedicated system, to help ensure that the database of principals and passwords is not compromised. Users should have limited access to the Kerberos server. If the system on which the Kerberos server resides is also used for some other purpose, such as a Web server or an FTP server, someone might take advantage of security flaws within these applications and gain access to the database stored on the Kerberos server. For

a Kerberos server in Microsoft Windows Active Directory, you can optionally configure a password server that principals can use to manage and update their own passwords stored on the Kerberos server. If you have configured a Kerberos server in i5/OS PASE and you are unable to dedicate the System i platform to Kerberos authentication, you should ensure that only your administrator has access to the Kerberos configuration.

Synchronizing system times

Kerberos authentication requires that system time is synchronized. Kerberos rejects any authentication requests from a system or client whose time is not within the specified maximum clock skew of the Kerberos server. Because each ticket is embedded with the time it was sent to a principal, hackers cannot resend the same ticket at a later time to attempt to be authenticated to the network. The System i platform also rejects tickets from a Kerberos server if its clock is not within the maximum clock skew set during network authentication service configuration. The default value is 300 seconds (five minutes) for the maximum clock skew. During network authentication service configuration, the maximum clock skew is set to this default; however, if necessary, you can change this value. It is recommended that this value not be greater than 300 seconds. See "Synchronizing system times" on page 99 for details on how to work with system times.

Table 19. Example planning work sheet for Kerberos server. This planning work sheet provides an example of how an administrator planned the Kerberos server for a network.

Questions	Answers
On which operating system do you plan to configure your Kerberos server? • Windows 2000 Server • Windows Server 2003 • AIX Server • i5/OS PASE (V5R3, or later) • z/OS	i5/OS Portable Application Solutions Environment (PASE)
What is the fully qualified domain name for the Kerberos server?	systema.myco.com
Are times between the PCs and systems that connect to the Kerberos server synchronized? What is the maximum clock skew?	Yes, 300 seconds
Should I install the Network Authentication Enablement (5722-NAE) product?	Yes, if you plan to configure a Kerberos server in i5/OS PASE on a V5R4 system. In V5R4, the network authentication server ships as a separate product, *Network Authentication Enablement* (5722-NAE). If you are using i5/OS V5R3, you need to install Cryptographic Access Provider (5722-AC3) instead to configure a Kerberos server in i5/OS PASE.

Planning realms

Understanding your enterprise can help you plan for realms in your environment.

In the Kerberos protocol, realms consist of a collection of machines and services that use a single authentication server called a Kerberos server or key distribution center (KDC). Realms are managed individually. Applications and services within the realm typically share some common use or purpose. The following general questions can help you plan realms in your enterprise:

How large is my current environment?

The size of your environment determines the number of realms you need. In a larger enterprise, you might consider several realms that are based on organizational boundaries or how certain systems are used within the enterprise. For example, you establish realms that represent different

organizations in your company, such as realms for your human resource department, customer service department, or shipping department. You can also create realms for a collection of systems or services that perform similar functions. Typically, smaller enterprises might need only one or two realms.

How quickly do I anticipate my environment to grow?
If you plan for your enterprise to grow quickly, you might want to set up several realms representing smaller organizational units in your enterprise. If you anticipate that your enterprise will grow more slowly, you can set up only one or two realms based on your organization now.

How many administrators will I need to manage these realms?
No matter how large or small your enterprise is, you need to make sure you have knowledgeable personnel to set up and administer the realms that you need.

Naming realms

According to the conventions of the Kerberos protocol, realm names are typically comprised of an uppercase version of the domain name, such as MYCO.COM. In networks with multiple realms, you can create a realm name that includes an uppercase descriptive name and domain name. For example, you might have two realms, one called HR.MYCO.COM and the other named SHIPPING.MYCO.COM, each representing a particular department in your organization.

It is not necessary to use uppercase; however, some implementations of Kerberos enforce this convention. For example, realm names are strictly uppercase in a Microsoft Windows Active Directory. If you are configuring network authentication service on the System i platform to participate in a Kerberos realm configured in Microsoft Windows Active Directory, you must enter the realm name in uppercase.

For a Kerberos server that is configured in i5/OS PASE, you can create either upper or lowercase realm names. However, if you plan to create trust relationships between a Kerberos server configured with Microsoft Window Active Directory and a Kerberos server configured in i5/OS PASE, the realm names should be uppercase.

Table 20. Example planning work sheet for Kerberos realms

Questions	Answers
How many realms do you need?	Two
How do you plan to organize realms?	Currently our company has a Windows 2000 server that authenticates users in our Order Receiving Department. Our Shipping Department use a Kerberos server in i5/OS PASE. Each of these departments will have its own realm.
What will be the naming convention used for realms?	We will use an uppercase shortened name that indicates the department followed by an uppercase version of the Windows 2000 domain name. For example, ORDEPT.MYCO.COM will represent the Order Receiving Department and SHIPDEPT.MYCO.COM will represent the Shipping Department.

Planning principal names

Principals are names of users or services in a Kerberos network. Principal names consist of the user name or service name and the name of the realm to which that user or service belongs.

If Mary Jones uses the realm MYCO.COM, her principal name might be jonesm@MYCO.COM. Mary Jones uses this principal name and its associated password to be authenticated by a centralized Kerberos server. All principals are added to the Kerberos server, which maintains a database of all users and services within a realm.

When developing a system for naming principals, you should assign principal names using a consistent naming convention that will accommodate current and future users. Use the following suggestions to establish a naming convention for your principals:

- Use family name and initial of first name
- Use first initial and full family name
- Use first name plus last initial
- Use application or service names with identifying numbers, such as database1.

i5/OS principal names

When you configure network authentication service on System i platforms, the principal names can be optionally created. Each of these principals represents services located on the i5/OS operating system. During the configuration of network authentication service, a key table entry is created on the system for each of the service principals that you choose to create. This key table entry stores the service principal name and the encrypted password that you specified during configuration. It is important to note that all i5/OS service principals need to be added to the Kerberos server after network authentication service is configured. The methods of adding the i5/OS principal to the Kerberos server varies based on the Kerberos server that you have configured in your enterprise. For instructions on how to add the i5/OS principal name to either a Windows 2000 domain or a Kerberos server in i5/OS PASE, see "Adding i5/OS principals to the Kerberos server" on page 95. The following information describes each of the i5/OS service principals that are created during network authentication service configuration:

i5/OS Kerberos Authentication

When you choose to create a keytab entry for i5/OS Kerberos Authentication, the service principal is generated in the keytab file in one of these formats: **krbsvr400/System i fully qualified domain name@REALM NAME** or **krbsvr400/System i host name@REALM NAME**. For example, a valid service principal for i5/OS Kerberos Authentication might be krbsvr400/systema.myco.com@MYCO.COM or krbsvr400/systema@MYCO.COM. i5/OS generates the principal based on the host name that it finds on either the DNS server or on the System i platform depending on how the System i platform is configured to resolve host names.

The service principal is used for several i5/OS interfaces, such as QFileSrv.400, Telnet, Distributed Relational Database Architecture™ (DRDA®), iSeries NetServer, and IBM eServer iSeries Access for Windows including iSeries Navigator. Each of these applications might require additional configuration to enable Kerberos authentication.

LDAP In addition to the i5/OS service principal name, you can optionally configure additional service principals for IBM Directory Server for iSeries (LDAP) during network authentication service configuration. The LDAP principal name is **ldap/System i fully qualified domain name@REALM NAME**. For example, a valid LDAP principal name might be ldap/systema.myco.com@MYCO.COM. This principal name identifies the directory server located on that System i platform.

Note: In past releases, the Network Authentication Service wizard created an uppercase keytab entry for LDAP service. If you have configured the LDAP principal previously, when you reconfigure network authentication service or access the wizard through the Enterprise Identity Mapping (EIM) interface, you will be prompted to change this principal name to its lowercase version.

If you plan on using Kerberos authentication with the directory server, you not only need to configure network authentication service, but also change properties for the directory server to accept Kerberos authentication. When Kerberos authentication is used, directory server associates the server distinguished name (DN) with the Kerberos principal name. You can choose to have the server DN associated by using one of the following methods:

- The server can create a DN based on the Kerberos principal name. When you choose this option, a Kerberos identity of the form **principal@realm** generates a DN of the form **ibm-kn=principal@realm**. **ibm-kn=** is equivalent to **ibm-kerberosName=**.

- The server can search the directory for a distinguished name (DN) that contains an entry for the Kerberos principal and realm. When you choose this option, the server searches the directory for an entry that specifies this Kerberos identity.

See IBM Directory Server for iSeries (LDAP) for details on the configuration Kerberos authentication for the directory server.

HTTP Server powered by Apache

In addition to the i5/OS service principal name, you can optionally configure additional service principals for HTTP Server powered by Apache (HTTP) during network authentication service configuration. The HTTP principal name is HTTP/*System i fully qualified domain name@REALM NAME*. This principal name identifies the HTTP Server instances on the System i platform that will be using Kerberos to authenticate Web users. To use Kerberos authentication with an HTTP Server instance, you also need to complete additional configuration steps that pertain to HTTP Server.

See the HTTP Server for i5/OS: documentation home page to find information about using Kerberos authentication with HTTP Server.

iSeries NetServer

For iSeries NetServer, you can also choose to create several NetServer principals that are automatically added to the keytab file on the System i platform. Each of these NetServer principals represents all the potential clients that you might use to connect with iSeries NetServer. The following table shows the iSeries NetServer principal name and the clients they represent:

Table 21. iSeries NetServer principal names

Client connection	iSeries NetServer principal name
Windows XP	cifs/System i fully qualified domain name cifs/System i host name cifs/QSystem i host name cifs/qSystem i host name cifs/IP address
Windows 2000	HOST/System i fully qualified domain name HOST/System i host name HOST/QSystem i host name HOST/qSystem i host name HOST/IP address

See iSeries NetServer for more information about using Kerberos authentication with this application.

Example planning work sheet

Table 22. Example principal planning work sheet

Questions	Answers
What is the naming convention that you plan to use for Kerberos principals that represent users in your network?	First initial followed by first five letters of the family name in lowercase, for example, mjones
What is the naming convention for applications on your network?	Descriptive name followed by number, for example, database123
For which i5/OS services do you plan to use Kerberos authentication?	i5/OS Kerberos authentication will be used for the following services: 1. iSeries Access for Windows, iSeries Navigator, NetServer, and Telnet 2. HTTP Server powered by Apache 3. LDAP

Table 22. Example principal planning work sheet (continued)

Questions	Answers
What are the i5/OS principal names for each of these i5/OS services?	1. krbsvr400/systema.myco.com@MYCO.COM 2. HTTP/systema.myco.com@MYCO.COM 3. ldap/systema.myco.com@MYCO.COM

Host name resolution considerations

To ensure that Kerberos authentication and host name resolution work properly with your Kerberos-enabled applications, verify that your PCs and your System i platforms resolve the same host name for the system on which the service application resides.

In a Kerberos environment, both the client and the server use some method of host name resolution to determine the host name for the system on which a particular application or service resides. If the System i platforms and the PCs use a Domain Name System (DNS) server, it is important that they use the same DNS server to perform host name resolution or, if they use more than one DNS server, that the host names are the same on both DNS servers. If your System i platform or PC resolves host names locally (from a local host table or file), they might resolve a host name that is different from the corresponding host name recorded on the DNS server. This might cause network authentication service to fail.

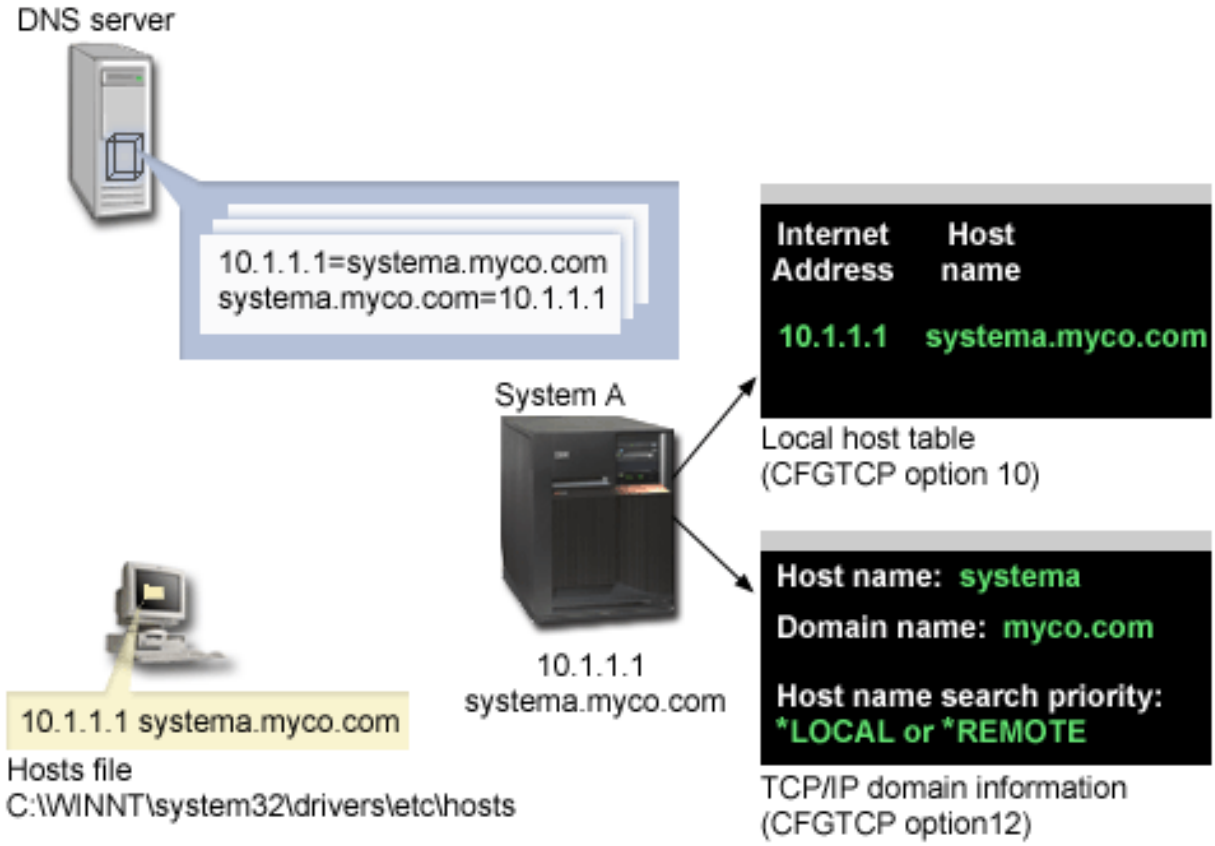
To ensure that Kerberos authentication and host name resolution work properly with your Kerberos-enabled applications, you must verify that your PCs and your System i platforms resolve the same host name for the system on which the service application resides. In the following example, this system is called System A.

The following instructions demonstrate how to determine whether the PCs and System i platforms resolve the same name for System A. Refer to the example work sheets as you follow the instructions.

You can enter your own information in the blank work sheets when you perform these steps for your Kerberos realm.

This graphic illustrates the system files and records that contain host name information in the following example.

Note: The IP address 10.1.1.1 represents a public IP address. This address is for example purposes only.



Details

DNS server

- Contains data resource records that indicate that IP address `10.1.1.1` correlates to host name `systema.myco.com`, the IP address and host name for System A.
- Might be used by the PC, System A, or both for host resolution.

  Note: This example demonstrates one DNS server. However, your network might use more than one DNS server. For example, your PC might use one DNS server to resolve host names and your System i platform might use a different DNS server. You need to determine how many DNS servers your realm is using for host resolution and adapt this information to your situation.

PC

- Runs Windows 2000 operating system.
- Represents both the PC used to administer network authentication service and the PC used by a user with no special authorities for his routine tasks.
- Contains the `hosts` file which indicates that IP address `10.1.1.1` correlates to host name `systema.myco.com`.

  Note: You can find the hosts file in these folders:
  - Windows 2000 operating system: C:\WINNT\system32\drivers\etc\hosts
  - Windows XP operating system: C:\WINDOWS\system32\drivers\etc\hosts

System A

- Runs i5/OS V5R3.
- Contains a service application that you need to access using network authentication service (Kerberos authentication).
- Within the Configure TCP (CFGTCP) menu, options 10 and 12 indicate the following information for System A:
  - Option 10 (Work with TCP/IP host table entries):
    - **Internet Address**: `10.1.1.1`
    - **Host Name**: `systema.myco.com`
  - Option 12 (Change TCP/IP domain information):
    - **Host name**: `systema`
    - **Domain name**: `myco.com`
    - **Host name search priority**: `*LOCAL` or `*REMOTE`

      Note: The Host name search priority parameter indicates either *LOCAL or *REMOTE depending on how your network administrator configured TCP/IP to perform host resolution on the system.

Table 23. Example: PC host name resolution work sheet

On the PC, determine the host name for System A.		
Step	**Source**	**Host name**
1.a.1	PC hosts file	systema.myco.com
1.b.1	DNS server	systema.myco.com

Table 24. Example: i5/OS host name resolution work sheet

On System A, determine the host name for System A.		
Step	**Source**	**Host name**
2.a.2	System A CFGTCP menu, option 12	**Host name**: `systema` **Domain name**: `myco.com`
Note: *Host name search priority* value: `*LOCAL` or `*REMOTE`		
2.b.2	System A CFGTCP menu, option 10	systema.myco.com
2.c.1	DNS server	systema.myco.com

Table 25. Example: Matching host names work sheet

These three host names must match exactly.	
Step	**Host name**
Step 1	systema.myco.com
Step 2.a.2	systema myco.com
2d	systema.myco.com

You can use the following three work sheets to verify that your PCs and your System i platforms resolve the same host name for the system on which the service application resides.

Table 26. PC host name resolution work sheet

On the PC, determine the host name for the System i platform.		
Step	**Source**	**Host name**
1.a.1	PC hosts file	
1.b.1	DNS server	

Table 27. i5/OS host name resolution work sheet

On your System i platform, determine the host name for the System i platform.		
Step	**Source**	**Host name**
2.a.2	System i CFGTCP menu, option 12	**Host name**: **Domain name**:
Note *Host name search priority* value: `*LOCAL` or `*REMOTE`		
2.b.2	System i CFGTCP menu, option 10	
2.c.1	DNS server	

Table 28. Matching host names work sheet

These three host names must match exactly.	
Step	**Host name**
Step 1	
Step 2.a.2	
2d	

Resolving your host names

Verify that your PCs and your System i platforms resolve the same host name.

Use the previous example work sheets as reference for resolving host names. To verify that the PCs and System i platforms are resolving the same host name for System A, follow these steps:

1. From the PC, determine the fully qualified TCP/IP host name for System A.

   Note: Depending on how you manage your network, you might want to do this on other PCs that are joining the single sign-on environment.

   a. In Windows Explorer on the PC, open the `hosts` file from one of these locations:
      - Windows 2000 operating system: C:\WINNT\system32\drivers\etc\hosts
      - Windows XP operating system: C:\WINDOWS\system32\drivers\etc\hosts

      Note: If the `hosts` file does not exist on the PC, then your PC might be using a DNS server to resolve host names. In that case, skip to Step 1b.

      On the work sheet, write down the first host name entry for System A, noting the uppercase or lowercase characters. For example, `systema.myco.com`.

Note: If the hosts file does not contain an entry for System A, then your PC might be using a DNS server to resolve host names. In that case, see Step 1b.

b. Use NSLOOKUP to query the DNS server.

Note: Skip this step if you found a host name entry in the PC's `hosts` file, and proceed to step 2. (The `hosts` file takes precedence over DNS servers when the operating system resolves host names for the PC.)

1) At a command prompt, type `NSLOOKUP` and press Enter. At the NSLOOKUP prompt, type `10.1.1.1` to query the DNS server for System A. Write down the host name returned by the DNS server, noting the uppercase or lowercase characters, for example, `systema.myco.com`.
2) At the NSLOOKUP prompt, type `systema.myco.com`. This must be the host name returned by the DNS server in the previous step. Verify that the DNS server returns the IP address that you expect, for example, `10.1.1.1`.

Note: If NSLOOKUP does not return the expected results, your DNS configuration is incomplete. For example, if NSLOOKUP returns an IP address that is different from the address you entered in step 1.b.1, you need to contact the DNS administrator to resolve this problem before you can continue with the next steps.

2. From System A, determine its fully qualified TCP/IP host name.
   a. TCP/IP domain information
      1) At the command prompt, type `CFGTCP` and select Option 12 (Change TCP/IP domain).
      2) Write down the values for the *Host name* parameter and the *Domain name* parameter, noting the uppercase or lowercase characters. For example:
         - **Host name**: `systema`
         - **Domain name**: `myco.com`
      3) Write down the value for the *Host name search priority* parameter.
         - `*LOCAL` - The operating system searches the local host table (equivalent of `hosts` file on the PC) first. If there is not a matching entry in the host table and you have configured a DNS server, the operating system then searches your DNS server.
         - `*REMOTE` - The operating system searches the DNS server first. If there is not a matching entry in the DNS server, the operating system then searches the local host table.
   b. TCP/IP host table
      1) At the command prompt, type `CFGTCP` and select Option 10 (Work with TCP/IP Host Table Entries).
      2) Write down the value in the *Host Name* column that corresponds to System A (IP address 10.1.1.1), noting the uppercase or lowercase characters, for example, `systema.myco.com`.

      Note: If you do not find an entry for System A in the host table, proceed to the next step.
   c. DNS server
      1) At a command prompt, type `NSLOOKUP` and press Enter. At the NSLOOKUP prompt, type `10.1.1.1` to query the DNS server for System A. Write down the host name returned by the DNS server, noting the uppercase or lowercase characters, for example, `systema.myco.com`.
      2) At the NSLOOKUP prompt, type `systema.myco.com`. This must be the host name returned by the DNS server in the previous step. Verify that the DNS server returns the IP address that you expect, for example, `10.1.1.1`.

      Note: If NSLOOKUP does not return the expected results, your DNS configuration is incomplete. For example, if NSLOOKUP returns an IP address that is different from the address you entered in Step 2.c.1, you need to contact the DNS administrator to resolve this problem before you can continue with the next steps.
   d. Determine which host name value for System A to keep, based on its TCP/IP configuration.

- If the value for the *Host name search priority* parameter is *LOCAL, keep the entry noted from the local host table (Step 2.b.2).
- If the value for the *Host name search priority* parameter is *REMOTE, keep the entry noted from the DNS server (Step 2.c.1).
- If only one of these sources contains an entry for System A, keep that entry.

3. Compare the results from these steps:
   a. Step 1: The name that the PC uses for System A.

      Note: If you find an entry for System A in the PC's hosts file, use that entry. Otherwise, use the entry from the DNS server.

   b. Step 2.a.2: The name that System A calls itself within its TCP/IP configuration.
   c. Step 2d: The name that System A calls itself based on host name resolution.

   All three of these entries must match exactly, including uppercase and lowercase characters. If the results do not exactly match, you will receive an error message indicating that a keytab entry cannot be found.

Network authentication service planning work sheets

To successfully configure network authentication service, you must understand the requirements and complete the necessary planning steps.

This topic provides a prerequisite worksheet and planning work sheet to ensure all necessary steps are completed. Use the following work sheets to aid in planning a Kerberos implementation and configuring network authentication service.

Prerequisite work sheet

Use this planning work sheet to ensure that all required prerequisites have been completed. You should be able to answer Yes to all prerequisite items before you perform any configuration tasks.

Table 29. Prerequisite work sheet

Questions	Answers
Is your i5/OS V5R3 (5722-SS1), or later?	
If you are using i5/OS V5R3, is Cryptographic Access Provider (5722-AC3) installed on your systems? If you are using i5/OS V5R4, is Network Authentication Enablement (5722-NAE) installed on your systems?	
Is iSeries Access for Windows (5722-XE1) installed on the administrator's PC and on your systems?	
Is the Security subcomponent of iSeries Navigator installed on the administrator's PC?	
Is the Network subcomponent of iSeries Navigator installed on the administrator's PC?	
Have you installed the latest IBM eServer iSeries Access for Windows service pack? See the iSeries Access Web page for the latest service pack.	
Do you have *SECADM, *ALLOBJ, and *IOSYSCFG special authorities?	

Table 29. Prerequisite work sheet (continued)

Questions	Answers
Do you have one of the following installed on a secure system that will act as a Kerberos server? Which one? 1. Windows 2000 Server 2. Windows Server 2003 3. AIX Server 4. i5/OS PASE (V5R3, or later) 5. z/OS	
For Windows 2000 Server and Windows Server 2003, do you have Windows Support Tools (which provides the ktpass tool) installed on the system being used as the key distribution center?	
If your Kerberos server is on a Windows 2000 or 2003 server, are all your PCs in your network configured in a Windows domain?	
Have you applied the latest program temporary fixes (PTFs)?	
Is the System i system time within five minutes of the Kerberos server's system time? If not see "Synchronizing system times" on page 99.	

Table 30. Kerberos server planning work sheet

Questions	Answers
On which operating system do you plan to configure your Kerberos server? • Windows 2000 Server • Windows Server 2003 • AIX Server • i5/OS PASE (V5R3, or later) • z/OS	
What is the fully qualified domain name for the Kerberos server?	
Are times between the PCs and systems that connect to the Kerberos server synchronized? What is the maximum clock skew?	

Table 31. Kerberos realm planning work sheet

Questions	Answers
How many realms do you need?	
How do you plan to organize realms?	
What will be the naming convention used for realms?	

Table 32. Principal planning work sheet

Questions	Answers
What is the naming convention that you plan to use for Kerberos principals that represent users in your network?	
What is the naming convention for applications on your network?	
For which i5/OS services do you plan to use Kerberos authentication?	

Table 32. Principal planning work sheet (continued)

Questions	Answers
What are the i5/OS principal names for each of these i5/OS services?	

Table 33. Host name resolution considerations work sheet

Question	Answer
Are the PCs and System i platform using the same DNS server to resolve host names?	
Are you using a local host table on the System i platform to resolve host names?	
Do your PC and your System i platform resolve the same host name for the System i platform? See "Host name resolution considerations" on page 80 for assistance.	

The following planning work sheet illustrates the type of information you need before you begin configuring the Kerberos server in i5/OS PASE and network authentication service. All answers on the prerequisite work sheet should be answered before you proceed with configuring the Kerberos server in i5/OS PASE.

Table 34. i5/OS PASE planning work sheet

Questions	Answers
Do you have PASE installed?	
What is the name of the default realm?	
What is the Kerberos server for this Kerberos default realm? What is the port on which the Kerberos server listens?	
What is the naming convention for your principals that represent users in your network?	
What are the principal names for your users in your network?	

Use the following planning work sheet to gather the information that you need before you begin configuring network authentication service. All answers on the prerequisite work sheet should be answered before you proceed with network authentication service configuration.

Table 35. Network authentication service planning work sheet

Questions	Answers
What is the name of the Kerberos default realm to which your system will belong? **Note:** A Windows 2000 domain is similar to a Kerberos realm. Microsoft Active Directory uses Kerberos authentication as its default security mechanism.	
Are you using Microsoft Active Directory?	
What is the Kerberos server for this Kerberos default realm? What is the port on which the Kerberos server listens?	
Do you want to configure a password server for this default realm? If yes, answer the following questions: What is name of the password server for this Kerberos server? What is the port on which the password server listens?	

Table 35. Network authentication service planning work sheet (continued)

Questions	Answers
For which services do you want to create keytab entries? • i5/OS Kerberos Authentication • LDAP • iSeries IBM HTTP Server • iSeries NetServer	
If you plan to create a service principal for i5/OS Kerberos Authentication, what is its password?	
If you plan to create a service principal for LDAP, what is its password?	
If you plan to create a service principal for HTTP Server, what is its password?	
If you plan to create a service principal for NetServer, what is its password? **Note:** During the network authentication service wizard, several principals will be created for iSeries NetServer. Write these down here as they are displayed in the wizard. They will be needed when you add these principals to the Kerberos server.	
Do you want to create a batch file to automate adding the service principals to Microsoft Active Directory?	
Do you want to include passwords with the i5/OS service principals in the batch file?	

Configuring network authentication service

Network authentication service allows the System i product to participate in an existing Kerberos network. Network authentication service assumes that you have a Kerberos server configured on a secure system in your network.

Configuring a Kerberos server

Currently, you can configure a Kerberos server in i5/OS Portable Application Solutions Environment (i5/OS PASE). In addition to this i5/OS support, the System i platform also interoperates with the Microsoft Windows 2000, Windows 2003, AIX Server, and z/OS. Use the following information to learn how to configure a Kerberos server on each of these platforms:

- Windows 2000 server
- z/OS Security Server Network Authentication Service Administration
- *IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide*

Note: You can find this documentation in the AIX 5L Expansion Pack and Bonus Pack CD.

Configuring a Kerberos server in i5/OS PASE

1. "Configuring a Kerberos server in i5/OS PASE" on page 89
2. "Changing encryption values on Kerberos server" on page 90
3. "Stopping and restarting the Kerberos server" on page 90
4. "Creating host, user, and service principals" on page 90
5. "Configuring Windows 2000 and Windows XP workstations" on page 91
6. "Configuring a secondary Kerberos server" on page 91

Configuring network authentication service on the System i platform

1. "Configuring network authentication service" on page 93

2. “Adding i5/OS principals to the Kerberos server” on page 95
3. “Creating a home directory” on page 97
4. “Testing network authentication service configuration” on page 97

Configuring a Kerberos server in i5/OS PASE

To provide an integrated runtime environment for AIX applications, configure and manage a Kerberos server from your System i platform.

i5/OS supports a Kerberos server in i5/OS Portable Application Solutions Environment (PASE). i5/OS PASE provides an integrated runtime environment for AIX applications. You can configure and manage a Kerberos server from your System i platform. To configure a Kerberos server in i5/OS PASE, complete the following steps:

1. In a character-based interface, type `call QP2TERM` at the command prompt. This command opens an interactive shell environment where you can work with i5/OS PASE applications.
2. At the command line, enter `export PATH=$PATH:/usr/krb5/sbin`. This command points to the Kerberos scripts that are necessary to run the executable files.
3. At the command line, enter `config.krb5 -S -d systema.myco.com -r MYCO.COM`, where `-d` is the DNS of your network and `-r` is the realm name. (In this example, myco.com is the DNS name and MYCO.COM is the realm name.) This command updates the krb5.config file with the domain name and realm for the Kerberos server, creates the Kerberos database within the integrated file system, and configures the Kerberos server in i5/OS PASE. You will be prompted to add a database Master Password and a password for the admin/admin principal, which is used to administer the Kerberos server.

   | **Note:** For V5R3 and V5R4, only the existing database is supported for storing Kerberos principals.
   | The LDAP directory plug-in is currently not supported.

4. Optional: If you want the Kerberos server and the administration server to automatically start during an initial program load (IPL), you need to perform two additional steps. You must create a job description and add an autostart job entry. To configure i5/OS to automatically start the Kerberos server and administration server during an IPL, follow these steps:
   a. Create a job description.

      At an i5/OS command line, type the following command where *xxxxxx* is the i5/OS user profile with *ALLOBJ user authority:

      ```
      CRTJOBD JOBD(QGPL/KRB5PASE) JOBQ(QSYS/QSYSNOMAX) TEXT('Start KDC and admin server in
      PASE') USER(xxxxxx) RQSDTA('QSYS/CALL PGM(QSYS/QP2SHELL) PARM(''/usr/krb5/sbin/
      start.krb5'')') SYNTAX(*NOCHK) INLLIBL(*SYSVAL) ENDSEV( 30)
      ```

   b. Add an autostart job entry. At the command line, type the following command:

      ```
      ADDAJE SBSD(QSYS/QSYSWRK) JOB(KRB5PASE) JOBD(QGPL/KRB5PASE).
      ```

   Note: As an alternative to starting the servers during an IPL, you can manually start the servers after the IPL by following these steps:
   a. In a character-based interface, type `call QP2TERM` to open the i5/OS PASE interactive shell environment.
   b. At the command line, enter `/usr/krb5/sbin/start.krb5` to start the servers.

What do I do next?

If you are using Windows 2000 or Windows XP workstations with a Kerberos server that is not configured through Windows 2000 Active Directory, (such as a Kerberos server in i5/OS PASE), you must perform several configuration steps on both the Kerberos server and the workstation to ensure that Kerberos authentication works properly.

Changing encryption values on Kerberos server

To operate with Windows workstations, the Kerberos server default encryption settings need to be changed so that clients can be authenticated to the i5/OS PASE Kerberos server.

To change the default encryption settings, you need to edit the kdc.conf file located in the/etc/krb5 directory by following these steps:

1. In a character-based interface, enter `edtf '/var/krb5/krb5kdc/kdc.conf'` to access the kdc.conf file.
2. Change the following lines in the kdc.conf file:

```
supported_enctypes = des3-cbc-sha1:normal
arcfour-hmac:normal aes256-cts:normal
des-cbc-md5:normal des-cbc-crc:normal
```

   to

```
supported_enctypes = des-cbc-crc:normal des-cbc-md5:normal
```

Stopping and restarting the Kerberos server

You must stop and restart the Kerberos server in i5/OS PASE to update the encryption values that you just changed.

Complete the following steps:

1. In a character-based interface, enter `call QP2TERM` at the command line. This command opens an interactive shell environment that allows you to work with i5/OS PASE applications.
2. At the command line, enter `export PATH=$PATH:/usr/krb5/sbin`. This command points to the Kerberos scripts that are necessary to run the executable files.
3. At the command line, enter `stop.krb5`. This command stops the Kerberos server.
4. At the command line, enter `start.krb5`. This command starts the Kerberos server.

Creating host, user, and service principals

Here is the procedure for creating host principals for your Windows 2000 and Windows XP workstations and for creating user and service principals on your Kerberos server.

To provide interoperability between a Windows 2000 or Windows XP workstation and a Kerberos server in i5/OS PASE, you need to add a host principal for the workstation to the Kerberos realm. For users to be authenticated to services in your network, you must add them to the Kerberos server as principals. These user principals are stored on the Kerberos server and are used to validate users on the network. For i5/OS to accept Kerberos tickets, you must add them to the Kerberos server as principals. Complete the following tasks:

Note: User names, host names, and passwords are used for example purposes only.

1. In a character-based interface, enter `call QP2TERM` at the command line. This command opens an interactive shell environment where you can work with i5/OS PASE applications.
2. At the command line, enter `export PATH=$PATH:/usr/krb5/sbin`. This command points to the Kerberos scripts that are necessary to run the executable files.
3. At the command line, enter `kadmin -p admin/admin`, and press Enter.
4. Sign in with administrator's password.
5. At the kadmin prompt, enter `addprinc -pw secret1 host/pc1.myco.com`. This command creates a host principal for the PC in your network. Repeat this step for all the PCs in your network.
6. Enter `addprinc -pw secret jonesm`. This command creates a principal for your user, Mary Jones. Repeat this step for all of your users.
7. At the kadmin prompt, enter `addprinc -pw systema123 krbsvr400/systema.myco.com`. This command creates a service principal for the Kerberos server.
8. Enter `quit` to exit the kadmin interface, and press F3 (Exit) to exit the PASE environment.

Configuring Windows 2000 and Windows XP workstations

To configure your client workstations, set the Kerberos realm and the Kerberos server.

After you have created a host principal for your Windows 2000 workstation on the Kerberos server in i5/OS PASE, you need to configure the client workstations. You need to make this client part of a workgroup by setting the Kerberos realm and Kerberos server on the workstation. You also need to set a password that will be associated with the workstation. To configure the workstations, complete these steps:

Note: User names, host names, and passwords are used for example purposes only.

1. From a command prompt on the Windows 2000 workstation, enter:

```
C:> ksetup /setdomain REALM.NAME.COM
C:> ksetup /addkdc REALM.NAME.COM kdc1.hostname.com
```

   For example, the administrator for MyCo, Inc entered the following:

```
C:> ksetup /setdomain MYCO.COM
C:> ksetup /addkdc MYCO.COM kdc1.myco.com
```

2. Set the local machine account password by entering this at the Windows 2000 workstation command prompt:

```
C:> ksetup /setmachpassword password
```

   This password must match the password used when you created the host principal, `pc1.myco.com`. For example, the user for MyCo, Inc entered the following:

```
C:> ksetup /setmachpassword secret1
```

3. Map the Kerberos user to a local user by entering this at the Windows 2000 workstation command prompt:

```
C:> ksetup /mapuser jonesm@MYCO.COM maryjones
```

4. Restart the computer for the changes to take effect.

Optionally, you can configure a secondary Kerberos server that you can use as a backup server if your primary Kerberos server goes down or if it is too busy to handle requests. See “Configuring a secondary Kerberos server” for detailed instructions.

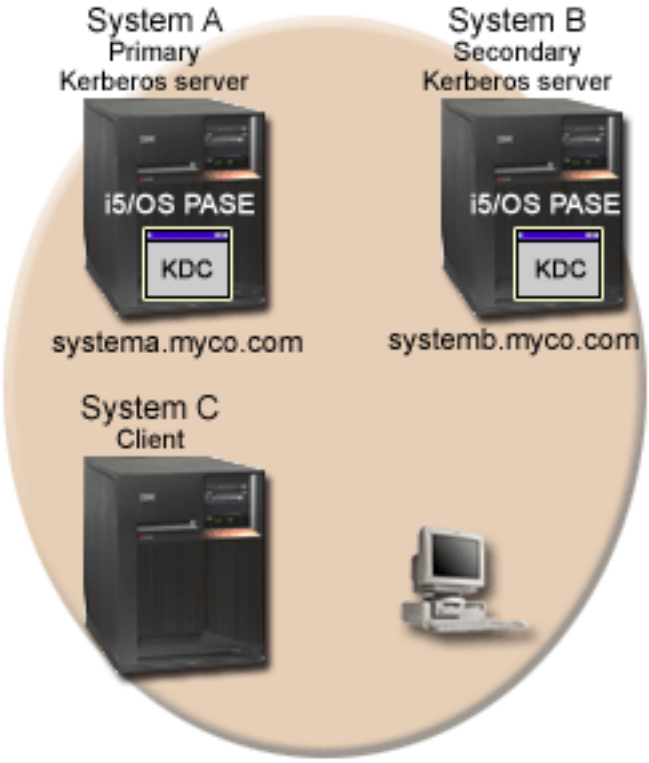
Configuring a secondary Kerberos server

After you have configured the primary Kerberos server in i5/OS PASE, you can optionally configure a secondary Kerberos server to use as a backup server in case your primary Kerberos server goes down or is too busy to handle requests.

For example, you currently use System A as your Kerberos server. Now you want to configure System B to be your secondary (backup) Kerberos server.

Note: A Kerberos server is also known as a key distribution center (KDC).

The following figure illustrates the System i products described in the following instructions.



Details

- The figure illustrates the System i products as they appear after you have completed the steps for configuring a secondary Kerberos server:
  - System A acts as the primary Kerberos server configured in i5/OS PASE.
  - System B acts as the secondary Kerberos server configured in i5/OS PASE.
  - System C acts as the client enabled to use System B as its Kerberos server.

To configure System B to be a secondary Kerberos server in i5/OS PASE, follow these steps:

1. Configure System B as a client.
   a. In a character-based interface on System B, type `call QP2TERM`. This command opens an interactive shell environment where you can work with i5/OS PASE applications.
   b. At the command line, enter the following command:

      ```
      export PATH=$PATH:/usr/krb5/sbin
      ```

      This command points to the Kerberos scripts that are necessary to run the executable files.
   c. At the command line, enter:

      ```
      config.krb5 -E -d rchland.ibm.com -r MYCO.COM -s lp16b1b.rchland.ibm.com
      ```

   d. Enter the administrator password; for example: `secret`

   The config.krb5 command configures the client, primary server, and secondary server. The **-C** flag configures the client on System C. The **-s** flag configures the primary Kerberos server on System A. The **-E** flag configures the secondary Kerberos server on System B.
2. Add an i5/OS principal for Systems A and B to the Kerberos server on System A.
   a. In a character-based interface on System A, enter `call QP2TERM`. This command opens an interactive shell environment where you can work with i5/OS PASE applications.

b. At the command line, enter:

```
export PATH=$PATH:/usr/krb5/sbin
```

This command points to the Kerberos scripts that are necessary to run the executable files.

c. At the command line, enter `kadmin -p admin/admin`.

d. Sign in with administrator's password. For example, `secret`.

e. At the command line, enter the following command:

```
addprinc -randkey -clearpolicy host/systema.myco.com
```

f. At the command line, enter the following command:

```
addprinc -randkey -clearpolicy host/systemb.myco.com
```

3. Propagate the master database from the primary Kerberos server to the secondary Kerberos server.

a. In a character-based interface on System A, enter `call QP2TERM`. This command opens an interactive shell environment where you can work with i5/OS PASE applications.

b. At the command line, enter the following command:

```
export PATH=$PATH:/usr/krb5/sbin
```

This command points to the Kerberos scripts that are necessary to run the executable files.

c. At the command line, enter:

```
/usr/krb5/sbin/config.krb5 -P -r MYCO.COM -d rchland.ibm.com -e rchasrc2.rchland.ibm.com
```

Tip: You can cut and paste the command in the message on the primary Kerberos system.

The **-P** flag propagates the master database from the primary Kerberos server to the secondary Kerberos server. The **-r** flag specifies the realm name. The **-d** flag specifies the name of the DNS domain. The **-e** flag specifies the host name of the secondary Kerberos server.

4. On the secondary Kerberos server, verify that the master database has been propagated successfully.

a. On the secondary Kerberos server, answer `Y` to the following prompt: `Have you successfully run the above command?`

b. Enter the database master password; for example: `pasepwd`. This command picks up the master key.

Configuring network authentication service

Here are the prerequisites and procedures for configuring network authentication service on your systems.

Before you configure network authentication service, you should perform the following tasks:

- Complete all the necessary planning work sheets.
- Verify that when your PCs and System i platforms perform host name resolution, they resolve the same host names for your System i products. Refer to "Host name resolution considerations" on page 80 for this task.
- Configure a Kerberos server on a secure system in your network. If you have configured a Kerberos server in i5/OS PASE, ensure that you have completed all the necessary configuration of the server and client workstations before configuring network authentication on the System i platform. See "Configuring a Kerberos server in i5/OS PASE" on page 89 for details on configuring a Kerberos server in i5/OS PASE.

  You can also have a Kerberos server configured on Microsoft Windows 2000, Windows Server 2003, and z/OS. See the appropriate documentation that corresponds with the Kerberos configuration for the system that will be used as a Kerberos server.

Configure the Kerberos server before you configure network authentication service on the System i platform.

To configure network authentication service, complete the following steps:

1. In iSeries Navigator, expand ***your system*** → **Security**.
2. Right-click **Network Authentication Service** and select **Configure** to start the configuration wizard.

   Note: After you have configured network authentication service, this option will be **Reconfigure**.
3. Review the Welcome page for information about what objects the wizard creates. Click **Next**.
4. On the Specify realm information page, enter the name of the default realm in the **Default realm** field. If you are using Microsoft Active Directory for Kerberos authentication, select **Microsoft Active Directory is used for Kerberos authentication**. Click **Next**.
5. On the Specify KDC information page, enter the name of the Kerberos server for this realm in the **KDC** field and enter 88 in the **Port** field. Click **Next**.
6. On the Specify password information page, select either **Yes** or **No** for setting up a password server. The password server allows principals to change passwords on the Kerberos server. If you select **Yes**, enter the password server name in the **Password server** field. The password server has the default port of 464. Click **Next**.
7. On the Select keytab entries page, select the **i5/OS Kerberos Authentication**. In addition, you can also create keytab entries for the Directory services (LDAP), iSeries NetServer, and iSeries HTTP server if you want these services to use Kerberos authentication.

   Note: Some of these services require additional configuration to use Kerberos authentication. Click **Next**.
8. On the Create i5/OS keytab entry page, enter and confirm a password. Click **Next**.

   Note: This is the same password you will use when you add the i5/OS principals to the Kerberos server.
9. On the Create batch file page, select **Yes** to create this file.

   Note: This page only appears if you selected **Microsoft Active Directory is used for Kerberos authentication** in Step 4 (above).
10. In the **Batch file** field, update the directory path. You can click **Browse** to locate the appropriate directory path and you can edit the path in the field.
11. In the **Include password** field, select **Yes**. This ensures that all passwords associated with the i5/OS service principal are included in the batch file. It is important to note that passwords are displayed in clear text and can be read by anyone with read access to the batch file.

    Note: You can also manually add the service principals that are generated by the wizard to Microsoft Active Directory. If you want to know how to manually add the i5/OS service principals to Microsoft Active Directory, see "Adding i5/OS principals to the Kerberos server" on page 95.
12. On the Summary page, review the network authentication service configuration details. Click **Finish**.

Network authentication service is now configured.

Related concepts

"Managing network authentication service" on page 98
After you have configured network authentication service, you can request tickets, work with key table files, and administer host name resolution. You can also work with credentials files and back up configuration files.

Adding i5/OS principals to the Kerberos server

After you configure network authentication service on your System i platform, you must add your i5/OS principals to the Kerberos server.

Network authentication service provides an i5/OS principal name, **krbsvr400**, for the system and the i5/OS applications. The name of the principal that represents i5/OS is krbsrv400/*System i host name@REALM NAME*, where *System i host name* is either the fully qualified host name or the short host name for the System i platform. This principal name needs to be added to the Kerberos server so that Kerberos client applications can request and receive service tickets. For example, in our configuration scenarios, the administrator for MyCo added the service principal krbsvr400/systema.myco.com@MYCO.COM to the company's Kerberos server.

Depending on the operating system on which you have configured a Kerberos server, the steps for adding the i5/OS principal are different. This information provides instructions on adding the i5/OS principals to a Kerberos server in i5/OS PASE or a Windows 2000 domain. If you have optionally created service principals for either IBM Directory Server for iSeries (LDAP), iSeries NetServer, or HTTP Server you must also add those service principals to the Kerberos server.

1. i5/OS PASE If your Kerberos server is located in i5/OS PASE, you can add i5/OS service principals by using the QP2TERM command, which opens an interactive shell environment that allows you to work with i5/OS PASE applications. To add an i5/OS service principal to a Kerberos server in i5/OS PASE, complete these steps:
   a. In a character-based interface, type call QP2TERM.
   b. At the command line, enter `export PATH=$PATH:/usr/krb5/sbin`. This command points to the Kerberos scripts that are necessary to run the executable files.
   c. At the command line, type `kadmin -p admin/admin`.
   d. Log on with your user name and password.
   e. At the kadmin command line, enter `addprinc -pw secret krbsvr400/System i fully qualified host name@REALM`, where `secret` is the password for the i5/OS service principal. For example, `krbsvr400/systema.myco.com@MYCO.COM` might be a valid i5/OS service principal name.
2. Microsoft Windows Active Directory

   To add an i5/OS service principal to a Kerberos server, you have two options: Allow the Network Authentication Service wizard to add the principals or add them manually.

   The Network Authentication Service wizard allows you to optionally create a batch file, called `NASConfig.bat`. This batch file contains all of the principal names for the services that you selected during configuration. You can also choose to add their associated passwords in this batch file.

   Note: If you include the password, anyone with read access to the batch file can view the passwords. It is recommended that if you include the password, that you delete the batch file from the Kerberos server and from your PC immediately after use. If you do not include the password in the batch file, you will be prompted for a password when the batch file is run on the Windows server.

   Using the batch file generated by the Network Authentication Service wizard

   a. Using FTP on the Windows 2000 workstation that the administrator used to configure network authentication service, open a command prompt and type `ftp` *`server`* where *server* is the host name for the Kerberos server. This will start an FTP session on your PC. You will be prompted for the administrator's user name and password.
   b. At the FTP prompt, type `lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access"`. Press **Enter**.

      Note: This is an example of a directory that might contain the batch file.
      You should receive the message `Local directory now C:\Documents and Settings\All Users\Documents\IBM\Client Access`.
   c. At the FTP prompt, type `binary`. This indicates that the file to be transferred is binary.

d. At the FTP prompt, type `cd \mydirectory`, where *mydirectory* is a directory on the Windows server where you want to place the batch file.
e. At the FTP prompt, type `put NASConfig.bat`. You should receive this message: `226 Transfer complete`.
f. On your Windows 2000 server, open the directory where you transferred the batch file.
g. Find the `NASConfig.bat` file and double-click the file to run it.
h. After the file runs, verify that the i5/OS principal name has been added to the Microsoft Windows Active Directory by completing the following steps:
   1) On your Windows 2000 server, expand **Start** → **Programs** → **Administrative Tools** → **Active Directory Users and Computers** → **Users**.
   2) Verify the System i platform has a user account by selecting the appropriate Windows 2000 domain.

      Note: This Windows domain should be the same as the default realm name that you specified network authentication service configuration.
   3) In the list of users that displays, find the name that corresponds with the service principal that you just added.
   4) Access the properties on your Active Directory users. From the **Account** tab, select the **Account is trusted for delegation**.

      Note: This optional step enables your system to delegate, or forward, a user's credentials to other systems. As a result, the i5/OS service principal can access services on multiple systems on behalf of the user. This is useful in a multi-tier network.

Manually adding the service principal to Microsoft Windows Active Directory You can also add i5/OS principals to the Microsoft Windows Active Directory manually by using the ktpass command. This command is shipped with Windows Support Tools and must be installed on the system being used as the Kerberos server.

a. On your Windows 2000 server, expand **Start** → **Programs** → **Administrative Tools** → **Active Directory Users and Computers**.
b. Select the Windows 2000 domain to which you want to add the i5/OS user account and expand **Action** → **New** → **User**.

   Note: This Windows 2000 domain should be the same as the default realm name that you specified for network authentication service configuration.
c. In the **Name** field, enter a name that will identify the System i platform to this Windows 2000 domain. This will add a new user account for the System i platform. For example, you might enter the name `krbsvr400systema` or `httpsystema` as a valid user account name.
d. Access the properties on the Active Directory user that you created in Step 3. From the **Account** tab, select the **Account is trusted for delegation**. This allows the i5/OS service principal to access other services on behalf of a signed-in user.
e. You need to map the user account you just created to the i5/OS service principal by using the ktpass command. The ktpass tool is provided in the **Service Tools** folder on the Windows 2000 Server installation CD. To map the user account, complete the following task:
   1) At a command prompt, enter

      ```
      ktpass -mapuser krbsvr400systema -pass secret -princ krbsvr400/system-domain-name@REALM
          -mapop set
      ```

      Note: In the command, `krbsvr400systema` represents the user account name that was created in step 3 and `secret` is the password that you entered during network authentication service configuration for the i5/OS principal.

Related concepts

"Troubleshooting" on page 116
This troubleshooting information includes common problems for network authentication service, Enterprise Identity Mapping (EIM), and IBM-supplied applications that support Kerberos authentication.

Creating a home directory

After you have added the i5/OS principal to the Kerberos server, you need to create a /home directory for each user that will connect to the i5/OS applications.

This directory will contain a file that contains the name of the user's Kerberos credentials cache. Each user should either be the owner of his directory or have the appropriate authority to create files within his directory.

To create a home directory for a user, complete the following step:

1. On an i5/OS command line, enter CRTDIR '/home/user profile', where user profile is the i5/OS user profile for the user.

   Note: If you plan to use this user profile as a target EIM association, the user profile must exist and the password can be set to *NONE.

Testing network authentication service configuration

To test the network authentication service configuration, request a ticket-granting ticket for your i5/OS principal.

After you have created the home directories for each user that will connect to the i5/OS applications, you can test the network authentication service configuration by requesting a ticket-granting ticket for your i5/OS principal. Before requesting a ticket, you should ensure that these common errors are fixed:

- Do you have all the prerequisites for network authentication service?
- Does a home directory exist on the i5/OS operating system for the user who issues the ticket request? See "Creating a home directory" for details.
- Do you have the correct password for the i5/OS principal? This password was created during network authentication configuration and should be specified in your planning worksheets.
- Have you added the i5/OS principal to the Kerberos server? See "Adding i5/OS principals to the Kerberos server" on page 95 for details.

To test network authentication service, complete the following steps:

1. On a command line, enter QSH to start the Qshell Interpreter.
2. Enter keytab list to display a list of principals registered in the keytab file. The following results should display:

```
Principal: krbsvr400/systema.myco.com@MYCO.COM
  Key version: 2
  Key type: 56-bit DES using key derivation
  Entry timestamp: 200X/05/29-11:02:58
```

3. Enter kinit -k krbsvr400/fully qualified host name@REALM NAME to request a ticket-granting ticket from the Kerberos server. For example, krbsvr400/systema.myco.com@MYCO.COM might be a valid principal name for the system. This command verifies that your system has been configured properly and the password in the keytab file matches the password stored on the Kerberos server. If this is successful, the QSH command displays without errors.
4. Enter klist to verify that the default principal is krbsvr400/fully qualified host name @REALM NAME. This command displays the contents of a Kerberos credentials cache and verifies that a valid ticket has been created for the i5/OS service principal and placed within the credentials cache on the system.

```
 Ticket cache: FILE:/QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/creds/krbcred

 Default principal: krbsvr400/systema.myco.com@MYCO.COM

Server: krbtgt/MYCO.COM@MYCO.COM
  Valid 200X/06/09-12:08:45 to 20XX/11/05-03:08:45
$
```

What do I do next:

Configuring Enterprise Identity Mapping

This task is optional if you are using network authentication service with your own applications. However, this task is recommended for use with IBM-supplied applications to create a single sign-on environment.

Managing network authentication service

After you have configured network authentication service, you can request tickets, work with key table files, and administer host name resolution. You can also work with credentials files and back up configuration files.

System i user tasks

The System i platform can also operate as a client in a Kerberos-enabled network. Users can sign on to the system and perform Kerberos-related tasks through the Qshell Interpreter. The following tasks use several Qshell commands to perform common tasks for users.

- "Creating a home directory" on page 97
- "Obtaining or renewing ticket-granting tickets" on page 102
- "Changing Kerberos passwords" on page 107
- "Managing keytab files" on page 105
- "Deleting expired credentials cache files" on page 109
- "Displaying credentials cache" on page 104
- "Managing Kerberos service entries in LDAP directories" on page 110

Note: If you are using the PC5250 emulator in iSeries Navigator, you need to change the **Remote sign-on** system value to enable you to bypass the sign-on. To change the **Remote sign-on** system value, follow these steps:

1. In iSeries Navigator, expand ***your system*** → **Configuration and Service** → **System Values** → **Sign-on**.
2. On the Remote page, select **Allow sign-on to be bypassed** and **Source and target user IDs must match**, and click **OK**.

Network authentication service administration tasks

The following tasks that can be performed by an administrator in iSeries Navigator. For more task-based information, see the iSeries Navigator help for network authentication service.

Related tasks

"Configuring network authentication service" on page 93
Here are the prerequisites and procedures for configuring network authentication service on your systems.

Synchronizing system times

Network authentication service uses 5 minutes (300 seconds) as the default for the maximum amount of time that system times can be different. You can change the clock difference by working with the network authentication service properties.

Before synchronizing system times, use the QTIMZON system value to set your system time according to your time zone. You can synchronize these system times by changing the time that is set on the Kerberos server or use the QTIME system value to change the System i system time. However, to keep system times in a network synchronized, you should configure Simple Network Time Protocol (SNTP). SNTP allows multiple systems to base their time on a single time server.

To configure SNTP, complete the following steps:

- To configure SNTP on a System i platform, enter `CHGNTPA` on a command line.
- To configure SNTP on Windows systems, use **NET HELP TIME** to display configuration information for a SNTP server.

Related concepts

Simple Network Time Protocol

Adding realms

Before you can add a realm to the i5/OS configuration, you need to configure the Kerberos server for the new realm. To add a realm to the i5/OS network authentication service task, you need the realm name, the name of the Kerberos server, and the port on which it listens.

To add a realm to the network authentication service, follow these steps:

1. In iSeries Navigator, expand ***your system*** → **Security** → **Network Authentication Service**.
2. Right-click **Realms** and select **Add Realm**.
3. In the **Realm to add** field, enter the host name of the realm that you want to add. For example, a valid realm name might be: MYCO.COM.
4. Enter the name of the Kerberos server for the realm that you are adding in the **KDC** field. For example, a valid name might be: kdc1.myco.com.
5. Enter the port number on which the Kerberos server listens for requests. A valid port number can be 1-65535. The default port for the Kerberos server is 88.
6. Click **OK**.

Deleting realms

As the network administrator, you might want to delete an unneeded or unused realm from the network authentication service configuration. You might also need to remove a default realm to recover from some application problems with applications that are integrated on the system.

For example, if you have configured network authentication service without setting up the Kerberos server in your network, QFileSvr.400 and Distributed Data Management (DDM) will assume that you are using Kerberos authentication. Before setting up authentication for these products, you should delete the default realm that you have specified during network authentication service configuration.

To delete a realm to the network authentication service, complete the following steps:

1. In iSeries Navigator, expand ***your system*** → **Security** → **Network Authentication Service** → **Realms**.
2. Right-click the name of the realm that you want to delete and select **Delete**.
3. Click **OK** to confirm the deletion.

Adding a Kerberos server to a realm

You can add a Kerberos server to a realm using network authentication service. Before you add the Kerberos server to the realm, you need to know the name and the port on which it listens.

To add a key distribution center to a realm, complete these steps:

1. In iSeries Navigator, expand *your system* → **Security** → **Network Authentication Service** → **Realms**.
2. Right-click the name of the realm in the right pane and select **Properties**.
3. On the **General** tab, enter the name of the Kerberos server that you want to add to this realm in the **KDC** field. The Kerberos server is required for all realms. For example, kdc2.myco.com might be a valid entry.
4. Enter the port number on which the Kerberos server listens for requests. A valid port number can be 1-65535. The default port for the Kerberos server is 88.
5. Click **Add**. The new Kerberos server will appear in the **Key Distribution Center (KDC) for this realm** list.
6. Click **OK**.

Adding a password server

The password server allows Kerberos principals to change their passwords.

Currently i5/OS PASE does not support the optional configuration of a password server. To change passwords for principals on an i5/OS PASE Kerberos server, you need to enter the PASE environment (call QP2TERM) and issue the kpasswd command. The following instructions allow you to update the network authentication service configuration to point to an additional or new password server for the default realm. To add a password server to a realm, complete the following steps:

1. In iSeries Navigator, expand *your system* → **Security** → **Network Authentication Service** → **Realms**.
2. Right-click the name of the realm in the right pane and select **Properties**.
3. On the **Password Server** tab, enter the name of the password server. For example, a valid name for the password server might be: psvr.myco.com.
4. Enter the port number that corresponds with the password server. A valid port number can be 1-65535. The default port for the password server is 464.
5. Click **Add**. The new password server will be added to the list.
6. Click **OK**.

Related reference

"kpasswd" on page 108
The Qshell command kpasswd changes a password for a Kerberos principal.

Creating a trust relationship between realms

Establishing a trust relationship between realms creates a shortcut for authentication.

This function is optional because by default the Kerberos protocol searches the realm hierarchy looking for trust. This function is useful if you have realms in different domains and want to make this process faster. To set up realm trust, each Kerberos server for each realm must share a key. Before you create a trust relationship in network authentication service, you must set up the Kerberos servers to trust one another. To create a trust relationship among realms, follow these steps:

1. In iSeries Navigator, expand *your system* → **Security** → **Network Authentication Service** → **Realm** .
2. Right-click the name of the realm in the right pane and select **Properties**.
3. On the **Trusted Realms** tab, enter the names of the realms that you want to establish trust. For example, valid names for the trust relationship might be: ORDEPT.MYCO.COM and SHIPDEPT.MYCO.COM.
4. Click **Add**. This will add the trust association in the table.

5. Click **OK**.

Changing host resolution

To resolve host names and realm names, specify an LDAP server, a Domain Name System (DNS), and static mappings.

With network authentication service, you can specify an LDAP server, a Domain Name System (DNS), and static mappings that are added to the configuration file to resolve host names and realm names. You can also select all three of these methods to resolve host names. If you select all of these methods, network authentication service checks the directory server first, the DNS entries second, and finally the static mappings to resolve host names.

To change host resolution, complete the following steps:

1. In iSeries Navigator, expand ***your system*** → **Security**.
2. Right-click **Network Authentication Service** and select **Properties**.
3. On the Host Resolution page, select **Use LDAP lookup**, **Use DNS lookup**, or **Use static mappings**.
4. If you select **Use LDAP lookup** as the host resolution type, enter the name of the directory server and its corresponding port. For example, ldapsrv.myco.com might be a valid name for the directory server. A valid port number can be 1-65535. The default port for the directory server is 389. After you have indicated that you will use an LDAP server to handle host name resolution, you must ensure that the realm has been properly defined in the LDAP server. See "Defining realms in the LDAP server" on page 114 for more information.
5. If you select **Use DNS lookup** as the host resolution type, you must have configured the DNS to map to realm names. After you have indicated that you will use a DNS server to handle host name resolution, you must ensure that the realm has been properly defined in the DNS. See "Defining realms in the DNS database" on page 112 for more information.
6. If you select **Use static mappings** as the host resolution type, enter the realm name and its corresponding DNS name. For example, the host name might be mypc.mycompanylan.com and the realm name might be MYCO.COM. You can also map generic host names to a specific realm. For instance, if all machines that end with myco.lan.com are part of the MYCO.COM, you might enter `myco.lan.com` as the DNS name and MYCO.COM as the realm. This creates an association between the realm name and the DNS name in the configuration file. Click **Add** to create a static mapping between the DNS name and realm name in the configuration file.
7. After you have entered the pertinent information for the selected host resolution type, click **OK**.

Adding encryption settings

You can select the encryption types for ticket-granting tickets (TGT) and ticket-granting service (TGS).

Encryption hides data that flows across a network by making it unidentifiable. A client encrypts data and the server decrypts it. To ensure that encryption works correctly, you must use the same encryption type that is specified on the Kerberos server or the other communicating application. If these encryption types do not match, encryption fails. You can add encryption values for both TGT and TGS.

Note: The default encryption values for the TGT and TGS are des-cbc-crc and des-cbc-md5. During configuration, default encryption values are set. You can add other encryption values for tickets to the configuration by completing these steps:

1. In iSeries Navigator, expand ***your system*** → **Security**.
2. Right-click **Network Authentication Service** and select **Properties**.
3. On the Tickets page, select the encryption value from either the Ticket Granting Ticket or the Ticket Granting Service list of available encryption types.

4. Click either **Add Before** or **Add After** to add the encryption type to the list of selected encryption types. Each of these selected encryption types will be attempted in the order they are listed. If one encryption type fails, the next one in the list will be attempted.
5. Click **OK**.

Obtaining or renewing ticket-granting tickets

The kinit command obtains or renews a Kerberos ticket-granting ticket.

If no ticket options are specified on the kinit command, the options for the Kerberos server that are specified in the Kerberos configuration file are used.

If an existing ticket is not renewed, the credentials cache is re-initialized and contains the new ticket-granting ticket received from the Kerberos server. If the principal name is not specified on the command line, the principal name is obtained from the credentials cache. The new credentials cache becomes the default credentials cache unless the cache name is specified by the `-c` option.

Ticket time values are expressed as *nwndnhnmns*, where *n* represents a number, *w* indicates weeks, *d* indicates days, *h* indicates hours, *m* indicates minutes, and *s* indicates seconds. The components must be specified in this order, but any component can be omitted (for example, *4h5m* represents 4 hours and 5 minutes, and *1w2h* represents 1 week and 2 hours). If only a number is specified, the default is hours.

To obtain a ticket-granting ticket that has a lifetime of 5 hours for principal jday, choose one of the following options:

- On the Qshell command line, enter `kinit -l 5h Jday`
- On an i5/OS control language (CL) command line, enter `call qsys/qkrbkinit parm('-l' '5h' 'jday')`

See the **kinit** usage notes on this Qshell command for specifics on its usage and restrictions.

kinit

The Qshell command kinit obtains or renews the Kerberos ticket-granting ticket.

Syntax

```
kinit [-r time] [-R] [-p] [-f] [-A] [-l time] [-c cache] [-k] [-t keytab] [principal]
```

Default public authority: *USE

Options

-r time
The time interval for renewing a ticket. The ticket can no longer be renewed after the expiration of this interval. The renew time must be greater than the end time. If this option is not specified, the ticket is not renewable (a renewable ticket may still be generated if the requested ticket lifetime exceeds the maximum ticket lifetime).

-R An existing ticket is to be renewed. When you renew an existing ticket, you cannot specify any other ticket options.

-p The ticket can be a proxy. If you do not specify this option, the ticket cannot be a proxy.

-f The ticket can be forwarded. If you do not specify this option, the ticket cannot be forwarded.

-A The ticket will not contain a list of client addresses. If you do not specify this option, the ticket will contain the local host address list. When an initial ticket contains an address list, it can be used only from one of the addresses in the address list.

-l time
The ticket end-time interval. After this interval expires, the ticket cannot be used unless it has been renewed. If you do not specify this option, the interval is set to 10 hours.

-c cache
The name of the credentials cache that the kinit command will use. If you do not specify this option, the command uses the default credentials cache.

-k The key for the ticket principal is to be obtained from a key table. If you do not specify this option, the system prompts you to enter the password for the ticket principal.

-t keytab
The key table name. If you do not specify this option but do specify the `-k` option, the system uses the default key table. The `-t` option implies the `-k` option.

principal
The ticket principal. If you do not specify the principal on the command line, the system obtains the principal from the credentials cache.

Authorities

Object referred to	Authority required
Each directory in the path name preceding the key table file if `-t` option is specified	*X
Key table file when `-t` is specified	*R
Each directory in the path name preceding the credentials cache file to be used	*X
Parent directory of the cache file to be used, if specified by the **KRB5CCNAME** environment variable, and the file is being created	*WX
Credentials cache file	*RW
Each directory in the paths to the configuration files	*X
Configuration files	*R

To enable the Kerberos run time to find your credentials cache file from any executing process, the name of the cache file is normally stored in the home directory in a file named **krb5ccname**. The storage location of the cache file name can be overridden by setting the environment variable **_EUV_SEC_KRB5CCNAME_FILE**. To access this file, the user profile must have ***X** authority to each directory in the path, and ***R** authority to the file where the cache file name is stored. The first time that a user creates a credentials cache, the user profile must have ***WX** authority to the parent directory.

Messages

- The `option_name` option requires a value.
- `command_option` is not a valid command option.
- No options allowed when renewing or validating ticket.
- Unable to obtain name of default credentials cache.
- Unable to resolve credentials cache `file_name`.
- No initial ticket available.
- Principal name must be specified.
- Unable to retrieve ticket from credentials cache `file_name`.
- Initial ticket is not renewable.
- `option_value` option is not valid for `request_name` request.
- Unable to obtain initial credentials.

- Unable to parse principal name.
- Unable to resolve key table `file_name`.
- Password is not correct for `principal_name`.
- Unable to read password.
- Unable to store initial credentials in credentials cache `file_name`.
- Time delta value is not valid.

For an example of how this command is used, see Obtaining or renewing ticket-granting tickets.

Displaying credentials cache

The klist command displays the contents of a Kerberos credentials cache.

To list all the entries in your default credentials cache and to show the ticket flags, choose one of the following options:

- On a Qshell command line, enter `klist -f -a`
- On an i5/OS control language (CL) command line, enter `call qsys/qkrbklist parm('-f' '-a')`

See the **klist** usage notes on this Qshell command for specifics on its usage and restrictions.

klist

The Qshell command klist displays the contents of a Kerberos credentials cache or key table.

Syntax

klist [-a] [-e] [-c] [-f] [-s] [-k] [-t] [-K] [filename]

Default public authority: *USE

Options

-a Show all tickets in the credentials cache, including expired tickets. If you do not specify this option, expired tickets are not listed. This option is valid only when you list a credentials cache.

-e Display the encryption type for the session key and the ticket. This option is valid only when you list a credentials cache.

-c List the tickets in a credentials cache. If neither the `-c` nor the `-k` option is specified, this is the default. This option is mutually exclusive with the `-k` option.

-f Show the ticket flags, using the following abbreviations:

Abbreviation	Meaning
F	Ticket can be forwarded
f	Forwarded ticket
P	Ticket can be a proxy
p	Proxy ticket
D	Ticket can be postdated
d	Postdated ticket
R	Renewable ticket
I	Initial ticket
i	Ticket not valid
A	Preauthentication used
O	Server can be a delegate
C	Transit list checked by the Kerberos server

This option is valid only when you list a credentials cache.

-s Suppress command output, but set the exit status to 0 if a valid ticket-granting ticket is found in the credentials cache. This option is valid only when you list a credentials cache.

-k List the entries in a key table. This option is mutually exclusive with the **-c** option.

-t Display timestamps for key table entries. This option is valid only when you list a key table.

-K Display the encryption key value for each key table entry. This option is valid only when you list a key table.

filename
Specifies the name of the credentials cache or key table. If no file name is specified, the default credentials cache or key table is used

Authorities

Object referred to	Authority required
Each directory in the path name preceding the file if `-k` option is specified as keytab	*X
Keytab file when `-k` is specified	*R
Each directory in the path name preceding the credentials cache file if the `-k` option is not specified	*X
Credentials cache file if the `-k` option is not specified	*R

To enable the Kerberos run time to find your credentials cache file from any running process, the name of the cache file is normally stored in the home directory in a file named **krb5ccname**. The storage location of the cache file name can be overridden by setting the environment variable **_EUV_SEC_KRB5CCNAME_FILE**. To access this file, the user profile must have ***X** authority to each directory in the path and ***R** authority to the file where the cache file name is stored. The first time that a user creates a credentials cache, the user profile must have ***WX** authority to the parent directory.

Messages

- The `option_name` option requires a value.
- `command_option` is not a valid command option.
- `command_option_one` and `command_option_two` cannot be specified together.
- No default credentials cache found.
- Unable to resolve credentials cache `file_name`.
- Unable to retrieve principal name from credentials cache `file_name`.
- Unable to retrieve ticket from credentials cache `file_name`.
- Unable to decode ticket.
- No default key table found.
- Unable to resolve key table `file_name`.

For an example of how this command is used, see Displaying credentials cache.

Managing keytab files

You can maintain the keytab file using either the character-based interface or iSeries Navigator.

As the network administrator, you need to maintain the keytab file, also called the key table, and its contents on the i5/OS operating system. You can manage the keytab file and its associated keytab entries by using either the character-based interface or iSeries Navigator:

- Manage keytab files using the character-based interface. The keytab command is used to add, delete, or list a key from a key table. For example, to add a key for the service principal, krbsvr400, on the host, kdc1.myco.com, in realm MYCO.COM:

- On a Qshell command line, enter `keytab add krbsvr400/kdc1.myco.com@MYCO.COM`
- On an i5/OS control language (CL) command line, enter `call qsys/qkrbkeytab parm('add' 'krbsvr400/kdc1.myco.com@MYCO.COM')`

You will be prompted for the password that was used when the service was defined to the Kerberos server.

- Manage keytab files using iSeries Navigator. You can use iSeries Navigator to add keytab entries to the key table. iSeries Navigator allows you to add keytab entries for the following services:
  - i5/OS Kerberos authentication
  - LDAP
  - HTTP Server powered by Apache
  - iSeries NetServer

  To add a keytab entry to the keytab file, follow these steps:
  1. In iSeries Navigator, expand ***your system*** → **Security**.
  2. Right-click **Network Authentication Service** and select **Manage Keytab**. This launches a portion of the Network Authentication Service wizard that enables you to add keytab entries.
  3. On the Select keytab entries page, select the types of services for which you want to add keytab entries. For example, i5/OS Kerberos Authentication. Click **Next**.
  4. On the Create i5/OS keytab entry page, enter and confirm a password. This password should be the same password that you use when you add the associated service principal to the Kerberos server. If you selected any of the other types of services, such as LDAP, HTTP Server powered by Apache, or iSeries NetServer in Step 3, you will also see pages that enable you to create keytab entries for each of those services.
  5. On the Summary page, view the list of i5/OS services and service principals that will be added as keytab entries to the keytab file.

See the **keytab** usage notes on this Qshell command, for specifics on its usage and restrictions.

keytab

The Qshell command keytab manages a key table.

Syntax

```
keytab add principal [-p password] [-v version] [-k keytab] keytab delete principal [-v version]
[-k keytab] keytab list [principal] [-k keytab]
```

Default public authority: *USE

Options

-k The key table name. If this option is not specified, the default key table is used.

-p Specify the password. If this option is not specified, users are prompted to enter the password when they add an entry to the key table.

-v The key version number. When you add a key, if this option is not specified, the next version number is assigned. When you delete a key, if this option is not specified, all keys for the principal are deleted.

principal
The principal name. When you list the key table, if this option is not specified, all principals are displayed.

Authorities

Object referred to	Authority required
Each directory in the path name preceding the target keytab file to be opened	*X
Parent directory of the target keytab file when add is specified, if the keytab file does not already exist	*WX
Keytab file when list is specified	*R
Target keytab file when add or delete is specified	*RW
Each directory in the paths to the configuration files	*X
Configuration files	*R

Messages

- You must specify *add*, *delete*, *list*, or *merge*.
- *command_option* is not a valid command option.
- *command_option_one* and *command_option_two* cannot be specified together.
- *option_value* option is not valid for *request_name* request.
- The *option_name* option requires a value.
- Unable to parse principal name.
- You must specify the principal name.
- Unable to read password.
- No default key table found.
- Unable to resolve key table *key_table*.
- Unable to read entry from key table *key_table*.
- Unable to remove entry from key table *key_table*.
- Unable to add entry to key table *key_table*.
- No entries found for principal *principal_name*.
- Value is not a valid number.
- The key version must be between 1 and 255.
- Key version *key_version* not found for principal *principal_name*.

For an example of how this command is used, see Managing keytab files.

Changing Kerberos passwords

The kpasswd command changes the password for the specified Kerberos principal using the password change service.

You must supply the current password for the principal as well as the new password. The password server will apply any applicable password policy rules to the new password before changing the password. The password server is configured during the installation and configuration of the Kerberos server. See the documentation that corresponds with that system.

Note: i5/OS PASE does not support a password server. To change a password for a principal stored on the Kerberos server, you must enter the PASE environment (call QP2TERM) and issue the kpasswd command.

During network authentication service configuration, you can specify that name of the password server. If one has not been specified during configuration, you can add a password server.

You may not change the password for a ticket-granting service principal (krbtgt/realm) using the kpasswd command.

- To change the password for the default principal:
  - On a Qshell command line, enter `kpasswd`
  - On a command line, enter `call qsys/qkrbkpsswd`
- To change the password for another principal:
  - On a Qshell command line, enter `kpasswd jday@myco.com`
- To change the password for another principal in i5/OS PASE:

  Using a character-based interface

  1. In a character-based interface, enter `call QP2TERM`. This command opens an interactive shell environment that allows you to work with i5/OS PASE applications.
  2. At the command line, enter `export PATH=$PATH:/usr/krb5/sbin`. This command points to the Kerberos scripts that are necessary to run the executable files.
  3. At the QSH prompt, enter `kadmin -p admin/admin`. Press Enter.
  4. Sign in with your administrator's username and password.
  5. Enter `kpasswd jday@myco.com`. You will be prompted to change the password for this principal.

  Using a command line

  1. On an command line, enter `call qsys/qkrbkpsswd parm ('jday@myco.com')`

For more details on the use of this command, see the **passwd** usage notes.

kpasswd

The Qshell command kpasswd changes a password for a Kerberos principal.

Syntax

```
kpasswd [-A ] [principal]
```

Default public authority: *USE

Options

-A The initial ticket used by the kpasswd command will not contain a list of client addresses. The ticket will contain the local host address list if this option is not specified. When an initial ticket contains an address list, it can be used only from one of the addresses in the address list.

principal
The principal whose password is to be changed. The principal will be obtained from the default credentials cache if the principal is not specified on the command line.

Messages

- Principal %3$s is not valid.
- Unable to read default credentials cache file_name.
- No default credentials cache.
- Unable to retrieve ticket from credentials cache file_name.
- Unable to read password.
- Password change canceled.
- Password is not correct for principal_name.
- Unable to obtain initial ticket.
- Password change request failed.

For an example of how this command is used, see Changing Kerberos passwords.

Deleting expired credentials cache files

The kdestroy command deletes a Kerberos credentials cache file. Users need to periodically delete old credentials by using the kdestroy command.

The *-e* option causes the kdestroy command to check all of the credentials cache files in the default cache directory /QIBM/UserData/OS400/NetworkAuthentication/creds. Any file that contains only expired tickets that have been expired for the *time_delta* is deleted. The *time_delta* is expressed as *nwndnhnmns*, where *n* represents a number, *w* indicates weeks, *d* indicates days, *h* indicates hours, *m* indicates minutes, and *s* indicates seconds. The components must be specified in this order, but any component can be omitted (for example, *4h5m* represents 4 hours and 5 minutes, and *1w2h* represents 1 week and 2 hours). If only a number is specified, the default is hours.

1. To delete your default credentials cache:
   - On a Qshell command line, enter `kdestroy`
   - On an i5/OS control language (CL) command line, enter `call qsys/qkrbkdstry`
2. To delete all credentials cache files that have expired tickets older than 1 day:
   - On a Qshell command line, enter `kdestroy -e 1d`
   - On a CL command line, enter`call qsys/qkrbkdstry parm ('-e' '1d')`

See the **kdestroy** usage notes on this Qshell command for specifics on its usage and restrictions.

kdestroy

The Qshell command kdestroy destroys a Kerberos credentials cache.

Syntax

```
kdestroy [-c cache_name] [-e time_delta]
```

Default public authority: *USE

Options

-c cache_name
The name of the credentials cache to be destroyed. If no command options are specified, the default credentials cache is destroyed. This option is mutually exclusive with the `-e` option.

-e time_delta
All credentials cache files that contain expired tickets are deleted if the tickets have been expired at least as long as the `time_delta` value.

Authorities

When the credentials cache is of type **FILE** (see **krb5_cc_resolve()** for more information about cache types), the default behavior is that the credentials cache file is created in the /QIBM/UserData/OS400/NetworkAuthentication/creds directory. The placement of the credentials cache file can be changed by setting the KRB5CCNAME environment variable.

If the credentials cache file does not reside in the default directory, the following authorities are required:

Object referred to	Data authority required	Object authority required
Each directory in the path name preceding the credentials cache file	*X	None

Object referred to	Data authority required	Object authority required
Parent directory of the credentials cache file	*WX	None
Credentials cache file	*RW	*OBJEXIST
Each directory in the paths to the configuration files	*X	None
Configuration files	*R	None

If the credentials cache file resides in the default directory, the following authorities are required:

Object Referred to	Data authority required	Object authority required
All directories in the path name	*X	None
Credentials cache file	*RW	None
Each directory in the paths to the configuration files	*X	None
Configuration files	*R	None

To enable the Kerberos protocol to find your credentials cache file from any running process, the name of the cache file is normally stored in the home directory in a file named krb5ccname. A user who wants to use Kerberos authentication on the System i platform must have a home directory defined. By default, the home directory is /home/. This file is used to find the default credentials cache if no command options are specified. The storage location of the cache file name can be overridden by setting the environment variable *_EUV_SEC_KRB5CCNAME_FILE*. To access this file, the user profile must have ***X** authority to each directory in the path and ***R** authority to the file where the cache file name is stored.

Messages

- Unable to resolve credentials cache *cache_file_name*.
- Unable to destroy credentials cache *cache_file_name*.
- The *function_name* function detects an error.
- Unable to retrieve ticket from credentials cache *file_name*.
- The *option_name* option requires a value.
- *command_option* is not a valid command option.
- *command_option_one* and *command_option_two* may not be specified together.
- No default credentials cache found.
- Time delta value *value* is not valid.

For an example of how this command is used, see Deleting expired credentials cache files.

Managing Kerberos service entries in LDAP directories

The ksetup command manages Kerberos service entries in the LDAP server directory.

Purpose

The ksetup command manages Kerberos service entries in the LDAP server directory. The following subcommands are supported:

addhost host-name realm-name

This subcommand adds a host entry for the specified realm. The fully qualified host name should

be used so that it resolves correctly no matter what default DNS domain is in effect on the Kerberos clients. If no realm name is specified, the default realm name is used.

addkdc host-name:port-number realm-name
This subcommand adds an entry in the Kerberos server for the specified realm. If a host entry does not already exist, one is created. If a port number is not specified, it is set to 88. Use the fully qualified host name so that it resolves correctly no matter what default DNS domain is in effect on the Kerberos clients. If no realm name is specified, the default realm name is used.

delhost host-name realm-name
This subcommand deletes a host entry and any associated specification for the Kerberos server from the specified realm. If no realm name is specified, the default realm name is used.

delkdc host-name realm-name
This subcommand deletes an entry in the Kerberos server for the specified host. The host entry itself is not deleted. If no realm name is specified, the default realm name is used.

listhost realm-name
This subcommand lists the entries in the Kerberos server for a realm. If no realm name is specified, the default realm name is used.

exit This subcommand ends the ksetup command.

Restriction: System i products support LDAP clients in the character-based interface, but not in i5/OS PASE.

Examples

To add the host, kdc1.myco.com, to the server, ldapserv.myco.com, as the Kerberos server for realm MYCO.COM, using an Directory Services (LDAP) administrator ID of Administrator and a password of verysecret, complete the following steps:

On a Qshell command line, enter: `ksetup -h ldapserv.myco.com -n CN=Administrator -p verysecret`

Or

1. On an i5/OS control language (CL) command line, enter:
   `call qsys/qkrbksetup parm('-h' 'ldapserv.myco.com' '-n' 'CN=Administrator' '-p' 'verysecret')`
2. When the Directory Services (LDAP) server is successfully contacted, a subcommand prompt is displayed. Enter
   `addkdc kdc1.myco.com MYCO.COM`

See the **ksetup** usage notes on this Qshell command for specifics on its usage and restrictions.

ksetup

The Qshell command ksetup manages Kerberos service entries in the directory server for a Kerberos realm.

Syntax

```
ksetup -h host-name -n bind-name -p bind-password -e
```

Default public authority: *USE

Options

-h The host name for the directory server. If you do not specify this option, the directory server specified in the Kerberos configuration file is used.

-n The distinguished name to use when you bind to the directory server. If you do not specify this option, the LDAP_BINDDN environment variable is used to obtain the name.

-p The password to use when you bind to the directory server. If this option is not specified, the LDAP_BINDPW environment variable is used to obtain the password.

-e Echo each command line to stdout. This is useful when stdin is redirected to a file.

Authorities

Object referred to	Authority required
Each directory in the paths to the configuration files	*X
Configuration files	*R

Messages

- `subcommand` is not a valid subcommand.
- Valid subcommands are `addhost`, `addkdc`, `delhost`, `delkdc`, `listhost`, `listkdc`, `exit`.
- `command_option_one` and `command_option_two` cannot be specified together.
- Unable to initialize LDAP client.
- Unable to bind to directory server.
- Realm name must be specified.
- Host name must be specified.
- Too many positional parameters.
- Host `host` already exists.
- Root domain `domain` is not defined.
- Realm name `realm` is not valid.
- The `LDAP function name` function detects an error.
- Insufficient storage available.
- Host name `host` is not valid.
- Port number `port` is not valid.
- Host `host` is not defined.
- No Kerberos server defined for host `host`.
- Unable to obtain default realm name.

For an example of how this command is used, see Managing Kerberos service entries in LDAP directories.

Defining realms in the DNS database

You can define realms in the DNS database to resolve host names.

Network authentication service allows you to use the DNS server to resolve host names. To do this, you need to add a server (SRV) record and text (TXT) record for each key distribution center in the realm. The Kerberos protocol searches for an SRV record using the realm name as the DNS search name.

To define realms with DNS, complete the following steps:

1. Set the configuration file to use DNS.
2. Add SRV records to your DNS server for each KDC server in the realm. The Kerberos run time searches for an SRV record by using the realm name as the search name. Note that DNS searches are not case-sensitive, so you cannot have two different realms whose names differ only in their case. The general form of the Kerberos SRV record is as follows:

```
service.protocol.realm TTL class SRV priority weight port target
```

The _kerberos service entries define KDC instances, and _kpasswd service entries define password change service instances.

Entries are tried in priority order (0 is the highest priority). Entries with the same priority are tried in random order. The _udp protocol records are required for _kerberos and _kpasswd entries.

3. Add TXT records to associate host names with realm names. The Kerberos protocol searches for a TXT record starting with the host name. If no TXT record is found, the first label is removed and the search is retried with the new name. This process continues until a TXT record is found or the root is reached. Note that the realm name is case-sensitive in the TXT record. The general format of a TXT record is as follows:

```
service.name TTL class TXT realm
```

For our configuration example, you can define the example KDCs for the two realms by adding the following records:

```
_kerberos._udp.deptxyz.bogusname.com IN SRV 0 0 88 kdc1.deptxyz.bogusname.com
_kerberos._tcp.deptxyz.bogusname.com IN SRV 0 0 88 kdc1.deptxyz.bogusname.com
_kerberos._udp.deptabc.bogusname.com IN SRV 0 0 88 kdc2.deptabc.bogusname.com
_kerberos._tcp.deptabc.bogusname.com IN SRV 0 0 88 kdc2.deptabc.bogusname.com
_kpasswd._udp.deptxyz.bogusname.com IN SRV 0 0 464 kdc1.deptxyz.bogusname.com
_kpasswd._tcp.deptxyz.bogusname.com IN SRV 0 0 464 kdc1.deptxyz.bogusname.com
_kpasswd._udp.deptabc.bogusname.com IN SRV 0 0 464 kdc2.deptxyz.bogusname.com
_kpasswd._tcp.deptabc.bogusname.com IN SRV 0 0 464 kdc2.deptxyz.bogusname.com
```

For our configuration example, following the general form of a Kerberos TXT record, we can associate hosts in the deptxyz and deptabc domains to their respective realms with the following statements:

```
_kerberos.deptxyz.bogusname.com  IN  TXT  DEPTXYZ.BOGUSNAME.COM
_kerberos.deptabc.bogusname.com  IN  TXT  DEPTABC.BOGUSNAME.COM
```

Here is a sample **krb5.conf** configuration file that specifies using DNS lookup:

Sample krb5.conf configuration file

```
; krb5.conf - Kerberos V5 configuration file DO NOT REMOVE THIS LINE
;
[libdefaults]
;  The default_realm value
;-default_realm = REALM1.ROCHESTER.IBM.COM
default_realm = DEPTXYZ.BOGUSNAME.COM
; define the system to use DNS lookup
use_dns_lookup = 1
[realms]
;
; We could configure the same realm information here, but it would
; only be used if the DNS lookup failed.
;
[domain_realm]
;  Convert host names to realm names.  Individual host names may be
;  specified.  Domain suffixes may be specified with a leading period
;  and will apply to all host names ending in that suffix.
;
; We will use DNS to resolve what realm a given host name belongs to.
;
[capaths]
;  Configurable authentication paths define the trust relationships
;  between client and servers.  Each entry represents a client realm
;  and consists of the trust relationships for each server that can
;  be accessed from that realm.  A server may be listed multiple times
;  if multiple trust relationships are involved.  Specify '.' for
;  a direct connection.
```

```
;-REALM1.ROCHESTER.IBM.COM = {
;-    REALM2.ROCHESTER.IBM.COM = .
;;}
DEPTXYZ.BOGUSNAME.COM = {
 DEPTABC.BOGUSNAME.COM = .
}
```

Defining realms in the LDAP server

Network authentication service allows you to use the LDAP server to resolve a host name into a Kerberos realm and to find the KDC for a Kerberos realm.

If you are using LDAP to look up this information, you must define the information in the LDAP server. To do this, complete the following two sets of tasks:

1. Set the configuration file to use LDAP.

   Use iSeries Navigator to indicate which directory server you want to use to resolve host names. This updates the **krb5.conf** configuration file located at /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf. The name of the directory server is added to the `libdefaults` section in the configuration file. Here is a sample of this configuration file:

   Sample krb5.conf configuration file

   ```
   ; krb5.conf - Kerberos V5 configuration file DO NOT REMOVE THIS LINE
   ;
   [libdefaults]
   ;  The default_realm value
   ;-default_realm = REALM1.ROCHESTER.IBM.COM
   default_realm = DEPTXYZ.BOGUSNAME.COM
   ; define the system to use LDAP lookup
   use_ldap_lookup = 1
   ldap_server = dirserv.bogusname.com
   [realms]
   ;
   ; We could configure the same realm information here, but it would
   ; only be used if the LDAP lookup failed.
   ;
   [domain_realm]
   ;  Convert host names to realm names.  Individual host names may be
   ;  specified.  Domain suffixes may be specified with a leading period
   ;  and will apply to all host names ending in that suffix.
   ;
   ; We will use LDAP to resolve what realm a given host name belongs to.
   ; We could define them here also, but they would only be used if the
   ; LDAP lookup fails.
   ;
   [capaths]
   ;  Configurable authentication paths define the trust relationships
   ;  between client and servers.  Each entry represents a client realm
   ;  and consists of the trust relationships for each server that can
   ;  be accessed from that realm.  A server may be listed multiple times
   ;  if multiple trust relationships are involved.  Specify '.' for
   ;  a direct connection.
   ;-REALM1.ROCHESTER.IBM.COM = {
   ;-    REALM2.ROCHESTER.IBM.COM = .
   ;;}
   DEPTXYZ.BOGUSNAME.COM = {
    DEPTABC.BOGUSNAME.COM = .
   }
   ```

2. Define Kerberos for the LDAP server. The LDAP server must have a domain object with a name that corresponds to the Kerberos realm name. For example, if the Kerberos realm name is `DEPTABC.BOGUSNAME.COM`, there needs to be an object in the directory named `dc=DEPTABC,dc=BOGUSNAME,dc=com`. If this object does not exist, you may first need to add a suffix to

the LDAP server configuration. For this object name, valid suffixes include dc=DEPTABC,dc=BOGUSNAME,dc=COM or one of the parent entries (dc=BOGUSNAME,dc=COM or dc=COM). For an i5/OS LDAP server, you can add a suffix by using iSeries Navigator.

a. If you want to add a suffix, follow these steps:
   1) In iSeries Navigator, expand *your system* → **Network** → **Servers** → **TCP/IP**.
   2) Right-click **IBM Directory Server** and select **Properties**.
   3) On the Database/Suffix page, specify the suffix you want to add.
b. Use the LDAPADD command to add the domain object for the realm in the LDAP directory.
c. Continuing with our configuration example of two realms, called DEPTABC.BOGUSNAME.COM and DEPTXYZ.BOGUSNAME.COM, place the following lines in an integrated file system file:

```
dn: dc=BOGUSNAME,dc=COM
dc: BOGUSNAME
objectClass: domain

dn: dc=DEPTABC,dc=BOGUSNAME,dc=COM
dc: DEPTABC
objectClass: domain

dn: dc=DEPTXYZ,dc=BOGUSNAME,dc=COM
dc: DEPTXYZ
objectClass: domain
```

d. If the integrated file system file is named **/tmp/addRealms.ldif**, then using the same assumptions as the previous example, enter the following commands:

```
STRQSH
ldapadd -h dirserv.bogusname.com -D cn=Administrator
  -w verysecret -c -f
/tmp/addRealms.ldif
```

e. Define the KDC entries for your realms, and optionally define host name entries to assign each host in your network to a specific realm name. You can do this using the ksetup command, with the addkdc and addhost subcommands. Continuing with our configuration example, you can enter the following commands:

```
STRQSH
ksetup -h dirserv.bogusname.com -n cn=Administrator
  -p verysecret
addkdc kdc1.deptxyz.bogusname.com DEPTXYZ.BOGUSNAME.COM
addkdc kdc2.deptxyz.bogusname.com DEPTXYZ.BOGUSNAME.COM
addkdc kdc1.deptabc.bogusname.com DEPTABC.BOGUSNAME.COM
addhost database.deptxyz.bogusname.com
  DEPTXYZ.BOGUSNAME.COM
```

   Repeat for each host in each realm, as needed.

Defining schema on an LDAP server

The i5/OS LDAP server (IBM Directory Server) is shipped with the LDAP schema already defined. However, if you are using an LDAP server other than IBM Directory Server, you can define your own schema on that server.

LDAP schema

If you decide to define your own schema on an LDAP server, the following information might be useful to you.

Network authentication service requires the following LDAP schema definitions, where:

- Integer values are represented as a signed-numeric character string with a maximum length of 11 characters.

- Boolean values are represented by the character strings “TRUE” and “FALSE”.
- Time values are represented as 15-byte character strings encoded in the format “YYYYMMDDhhmmssZ”. All times are represented as UTC values.

LDAP object classes

Object	Requires	Allows
domain	dc	description seeAlso
ibmCom1986-Krb-KerberosService	serviceName ibmCom1986-Krb-KerberosRealm	ipServicePort description seeAlso
domain	dc objectClass	description seeAlso

LDAP attributes

Attribute	Type	Size	Value
dc	caseIgnoreString	64	single
description	caseIgnoreString	1024	multiple
ibmCom1986-Krb-KerberosRealm	caseExactString	256	single
ipServicePort	integer	11	single
seeAlso	DN	1000	multiple
serviceName	caseIgnoreString	256	single

Troubleshooting

This troubleshooting information includes common problems for network authentication service, Enterprise Identity Mapping (EIM), and IBM-supplied applications that support Kerberos authentication.

1. Complete all prerequisites.
2. Ensure that the user has a user profile on the System i platform and a principal on the Kerberos server. On the System i platform, verify that the user exists by opening the Users and Groups in iSeries Navigator or typing the `WRKUSRPRF` (Work with User Profile) command on a command line. On Windows systems, verify the user exists by accessing the Active Directory Users and Computers folder.
3. Check to see if the System i platform is contacting the Kerberos server by using the kinit command from Qshell Interpreter. If the kinit command fails, check to see if the i5/OS service principal has been registered on the Kerberos server. If it has not, you can add the i5/OS principal to the Kerberos server.

Related tasks

“Adding i5/OS principals to the Kerberos server” on page 95
After you configure network authentication service on your System i platform, you must add your i5/OS principals to the Kerberos server.

Network authentication service errors and recovery

While using the Network Authentication Service wizard or when you are managing network authentication service properties in iSeries Navigator, you might encounter these errors. Use the corresponding recovery methods listed here to troubleshoot.

Table 36. Network authentication service errors and recovery

Error	Recovery
KRBWIZ_CONFIG_FILE_FORMAT_ERROR: The Format of the Network Authentication Service configuration file is in error.	Reconfigure network authentication service. See “Configuring network authentication service” on page 93 for details.
KRBWIZ_ERROR_READ_CONFIG_FILE: Error reading Network Authentication Service configuration file.	Reconfigure network authentication service. See “Configuring network authentication service” on page 93 for details.
KRBWIZ_ERROR_WRITE_CONFIG_FILE: Error writing Network Authentication Service configuration file.	The service used to write the configuration file is unavailable. Try again later.
KRBWIZ_PASSWORD_MISMATCH: New password and confirm new password not the same	Re-enter new password and confirm new password.
KRBWIZ_PORT_ERROR: The port number must be between 1 and 65535.	Re-enter a port number between 1 and 65 535.
KRBWIZ_ERROR_WRITE_KEYTAB: Error writing key table file	The service used to write the keytab may be temporarily unavailable. Try again later.
KRBWIZ_NOT_AUTHORIZED_CONFIGURE: Not authorized to configure Network Authentication Service.	Ensure that you have the following authorities: *ALLOBJ and *SECADM.
KrbPropItemExists: Item already exists.	Enter a new item.
KrbPropKDCInListRequired: Must have a KDC in the list.	Specified Kerberos server does not exist in the list. Select a Kerberos from the list.
KrbPropKDCValueRequired: A KDC name must be entered.	Enter a valid name for the Kerberos server. The Kerberos server must be configured on a secure system in the network.
KrbPropPwdServerRequired: A password server name must be entered.	Enter a valid name for the password server.
KrbPropRealmRequired: A realm name must be entered.	Enter the name of the realm in which this system belongs.
KrbPropRealmToTrustRequired: A name must be entered for the realm to trust.	Enter the name of the realm for which a trust relationship is being established.
KrbPropRealmValueRequired: A realm name must be entered.	Enter a valid name for the realm.
CPD3E3F: Network Authentication Service error &2 occurred.	See the specific recovery information that corresponds with this message.

Application connection problems and recovery

Here are some of the common errors in Kerberos-enabled i5/OS interfaces and their recovery methods.

Table 37. Common errors in Kerberos-enabled i5/OS interfaces

Problem	Recovery
You receive this error: Unable to obtain name of default credentials cache.	Determine if the user who signed on to the System i platform has a directory in the /home directory. If the directory for the user does not exist, create a home directory for the credentials cache.
CPD3E3F: Network Authentication Service error &2 occurred.	See the specific recovery information that corresponds with this message.

Table 37. Common errors in Kerberos-enabled i5/OS interfaces (continued)

Problem	Recovery
DRDA/DDM connection fails on a System i platform that was previously connected.	Check to see if the default realm specified during network authentication service configuration exists. If a default realm and Kerberos server have not been configured, the network authentication service configuration is incorrect and DRDA/DDM connections will fail. To recover from this error, you can do one of the following tasks: 1. If you are not using Kerberos authentication, follow these steps: Delete the default realm specified in the network authentication service configuration. 2. If you are using Kerberos authentication, follow these steps: a. Reconfigure network authentication service specifying the default realm and Kerberos server that you created in Step 1. b. Configure iSeries Access for Windows applications to use Kerberos authentication. This sets Kerberos authentication on all iSeries Access for Windows applications, including DRDA/DDM. (See "Scenario: Enabling single sign-on for i5/OS" on page 51.)
QFileSvr.400 connection fails on a System i platform that was previously connected.	Check to see if the default realm specified during network authentication service configuration exists. If a default realm and Kerberos server have not been configured, the network authentication service configuration is incorrect and QFileSvr.400 connections will fail. To recover from this error, you can do one of the following tasks: 1. If you are not using Kerberos authentication, follow these steps: Delete the default realm specified in the network authentication service configuration. 2. If you are using Kerberos authentication, follow these steps: a. Configure a default realm and Kerberos server on a secure system on the network. See the documentation that corresponds with that system. b. Reconfigure network authentication service specifying the default realm and Kerberos server that you create in Step 1. c. Configure iSeries Access for Windows applications to use Kerberos authentication. This will set Kerberos authentication on all iSeries Access for Windows applications, including DRDA/DDM. (See "Scenario: Enabling single sign-on for i5/OS" on page 51.)
CWBSY1011: Kerberos client credentials not found.	The user does not have a ticket-granting ticket (TGT). This connection error occurs on the client PC when a user does not log into a Windows 2000 domain. To recover from this error, log into the Windows 2000 domain.

Table 37. Common errors in Kerberos-enabled i5/OS interfaces (continued)

Problem	Recovery
Error occurred while verifying connection settings. URL does not have host. **Note:** This error occurs when you are using Enterprise Identity Mapping (EIM).	To recover from this error, follow these steps: 1. In iSeries Navigator, expand ***your system*** → **Network** → **Servers** → **TCP/IP**. 2. Right-click **Directory** and select **Properties**. 3. On the General page, validate that the administrator's distinguished name and password match those you entered during EIM configuration.
Error occurred while changing local directory server configuration. GLD0232: Configuration cannot contain overlapping suffixes. **Note:** This error occurs when you are using Enterprise Identity Mapping (EIM).	To recover from this error, follow these steps: 1. In iSeries Navigator, expand ***your system*** → **Network** → **Servers** → **TCP/IP**. 2. Right-click **Directory** and select **Properties**. 3. On the Database/Suffixes page, remove any **ibm-eimDomainName** entries and re-configure EIM.
Error occurred while verifying connection settings. An exception occurred while calling an i5/OS program. The called program is eimConnect. Details are: com.ibm.as400.data.PcmlException. **Note:** This error occurs when you are using Enterprise Identity Mapping (EIM).	To recover from this error, follow these steps: 1. In iSeries Navigator, expand ***your system*** → **Network** → **Servers** → **TCP/IP**. 2. Right-click **Directory** and select **Properties**. 3. On the Database/Suffixes page, remove any **ibm-eimDomainName** entries and reconfigure EIM.
Kerberos ticket from remote system cannot be authenticated. **Note:** This error occurs when you are configuring Management Central systems to use Kerberos authentication.	Verify that Kerberos is configured properly on all your systems. This error might indicate a security violation. Try the request again. If the problem persists contact service.
Cannot retrieve Kerberos service ticket. **Note:** This error occurs when you are configuring Management Central systems to use Kerberos authentication.	Verify that the Kerberos principal krbsvr400/*System i fully qualified host name@REALM* is in the Kerberos server as well as the keytab file for each of your systems. To verify whether the Kerberos principal is entered in the Kerberos server, see "Adding i5/OS principals to the Kerberos server" on page 95. To verify whether the Kerberos service principal names are entered in the keytab file, see "Managing keytab files" on page 105 for details.
Kerberos principal is not in a trusted group. **Note:** This error occurs when you are configuring Management Central systems to use Kerberos authentication.	Add the Kerberos principal for the system that is trying to connect to this system to your trusted group file. To recover from this error, follow these steps: 1. Set the central system to use Kerberos authentication. 2. Collect system values inventory. 3. Compare and update. 4. Restart Management Central servers on the central system and the target systems. 5. Add Kerberos service principal to the trusted group file for all endpoint systems. 6. Allow trusted connections. 7. Restart Management Central servers on the central system and the target systems. 8. Test authentication on Management Central servers.

API trace tool

You can set up the API trace tool to troubleshoot problems with Kerberos and Generic Security Services API calls.

Network authentication service provides an API trace tool that an administrator can use to create a file that contains all the Kerberos and Generic Security Services (GSS) API calls. With this tool, you can troubleshoot more advanced errors involving your own Kerberos-enabled applications and errors that might occur during network authentication service configuration and during Kerberos ticket requests. Using environment variables, you can create the tool and have it generate a log file in a user's home directory.

Note: The home directory must exist before completing these steps.

Setting up the API trace tool

To write the API trace tool to a file, complete these steps on the System i platform on which network authentication service is configured.

To set up the API trace tool, complete the following steps:

1. Create an envar file in the home directory of the user to trace. For example, you can specify `/home/user_profile_name/envar`.
2. In the character-based interface, use `edtf /home/user_profile_name/envar` to edit the file.
3. Add the following lines to the envar file, being careful that they start in column 1.

```
_EUV_SVC_MSG_LOGGING=STDOUT_LOGGING
_EUV_SVC_MSG_LEVEL=VERBOSE
_EUV_SVC_STDOUT_FILENAME=/home/user_profile_name/trace.txt
_EUV_SVC_DBG_MSG_LOGGING=1
_EUV_SVC_DBG_TRACE=1
_EUV_SVC_DBG=*.9
```

4. Retry the failing command.
5. View the trace referenced by _EUV_SVC_STDOUT_FILENAME.

After you complete tracing the failing command, remove or rename the envar file, or else every Kerberos command that users enter will get traced.

Accessing the API trace log file

After you have set up the API trace tool, you can access the log file to begin troubleshooting.

To access this log file, complete the following steps:

1. On the character-based interface, enter `wrklnk ('home/user profile')`, where `user profile` is the user profile's name.
2. On the **Work with Object Link** dialog box, select Option 5 to display the contents of the trace.txt file stored in that directory.

This shows a portion of an example log file:

```
Browse : /home/day/trace.txt
 Record :       1   of    5430 by  14           Column :    1    140 by  79
 Control :

 ************Beginning of data**************
030515 08:53:13 (00000003) DBG1 KRB/KRB_GENERAL: Version 5, Release 3, Service level V5R3M0
030515 08:53:13 (00000003) DBG1 KRB/KRB_GENERAL: STDOUT handle=4, STDERR handle==-1,
DEBUG handle=4
030515 08:53:13 (00000003) DBG6 KRB/KRB_GENERAL: Using variant character table for code set 37
030515 08:53:13 (00000003) DBG1 KRB/KRB_API: --> krb5_init_context()
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Updating profile from
QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/krb5.conf
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   [libdefaults]
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   default_keytab_name = /
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   default_realm = MYCO.COM
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   [realms]
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   MYCO.COM = {
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   kdc = kdc1.myco.com:88
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   kpasswd_server = kdc1.myco.com:464
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   }
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   [domain_realm]

F3=Exit   F10=Display Hex   F12=Exit  F15=Services  F16=Repeat find
F19=Left   F20=Right
```

For information about specific error messages that are found in the API trace, see the corresponding API in the information center. You can use the following methods for locating information about these APIs:

- API finder
- Network Authentication Service Application Programming Interfaces (APIs)
- Generic Security Service Application Programming Interfaces (GSS APIs)

Troubleshooting Kerberos server in i5/OS PASE

You can access status and informational log files to troubleshoot Kerberos server in i5/OS PASE.

During configuration of a Kerberos server in i5/OS PASE, the authentication server and the administration server are created. These servers write status and informational messages to a log file located in the /var/krb5/log directory. This log file, krb5kdc.log, contains messages that can help the administrator troubleshoot problems with configuration and authentication requests.

Access Kerberos server log files in i5/OS PASE. On the System i platform that you have the Kerberos server configured in i5/OS PASE, complete these steps:

1. At a character-based interface, type `QP2TERM`. This command opens an interactive shell environment that allows you to work with i5/OS PASE applications.
2. At the command line, type `cd /var/krb5/log`.
3. At the command line, type `cat /krb5kdc.log`. This will open the krb5kdc.log file that contains error messages for the i5/OS PASE KDC.

Example krb5kdc.log file

The following sample log contains several messages:

```
$
AS_REQ (3 etypes {16 3 1}) 10.1.1.2(88): NEEDED_PREAUTH:
jday@SYSTEMA.MYCO.COM for kadmin/changepw@SYSTEMA.MYCO.COM,
Additional pre-authentication required

Apr 30 14:18:08 systema.myco.com /usr/krb5/sbin/krb5kdc[334](info):
AS_REQ (3 etypes {16 3 1}) 10.1.1.2(88): ISSUE: authtime 1051730288,
etypes {rep=16 tkt=16 ses=16}, jday@SYSTEMA.MYCO.COM for
kadmin/changepw@SYSTEMA.MYCO.COM

Apr 30 14:18:56 systema.myco.com /usr/krb5/sbin/krb5kdc[334](Notice):
AS_REQ (3 etypes {16 3 1}) 10.1.1.2(88): NEEDED_PREAUTH:
jday@SYSTEMA.MYCO.COM for kadmin/changepw@SYSTEMA.MYCO.COM,
Additional pre-authentication required

Apr 30 14:18:56 systema.myco.com /usr/krb5/sbin/krb5kdc[334](info):
DISPATCH: replay found and re-transmitted
$
```

Network authentication service commands

These commands help you configure and use network authentication service.

Table 38. Network authentication service commands

Command	Description
config.krb	Configures network authentication service servers and clients.
kadmin	Administers the network authentication service database.
kadmind_daemon	Starts the network authentication service administration server.
kdb5_util	Allows an administrator to perform low-level maintenance procedures on the network authentication service database.
kdestroy	Destroys a credentials cache (also called a key table).
kinit	Obtains or renews a ticket-granting ticket.
klist	Displays the contents of a credentials cache or key table.
kpasswd	Changes the password for a principal.
krb5kdc	Starts the network authentication service multithreaded key distribution center (KDC).
ksetup	Manages the network authentication service entries in the LDAP directory for a network authentication service realm.
ksu	Switches to another user ID.
ktutil	Allows an administrator to read, write, or edit entries in a keytab file.
kvno	Displays the current key version number for a principal.
start.krb5	Starts the network authentication service server.
stop.krb5	Stops the network authentication service server.
unconfig.krb5	Unconfigures the network authentication service clients and services.

For more information about these commands, see the *IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide*.

Related information for network authentication service

Listed here are information center topics as well as external Web sites that relate to network authentication service.

Manuals

If you order the AIX Expansion Pack CD, you can access the network authentication service documentation. Although the manuals are written for the AIX, Solaris, and Linux® operating systems, you can use many of the network authentication service commands on the i5/OS operating system. When you install the network authentication service product on your AIX system, the documentation is installed in the /usr/lpp/krb5/doc/pdf/en_US directory.

In addition, if you install the Network Authentication Enablement product (5722-NAE) on your system, you can access the same manuals in both PDF and HTML formats from the /usr/lpp/krb5/doc/ directory.

- *IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide*.
- *IBM Network Authentication Service AIX, Linux, and Solaris Application Development Reference*.

Note: You can find this documentation in the AIX 5L Expansion Pack and Bonus Pack CD.

Web sites

The following Web sites and information provide more information about setting up a Kerberos server with a particular operating system.

- Windows 2000 server
- z/OS Security Server Network Authentication Service Administration

Other information center topics

- Network Authentication Service Application Programming Interfaces (APIs)
- Generic Security Service Application Programming Interfaces (GSS APIs)
- Enterprise Identity Mapping (EIM)
- Single sign-on

Request for Comments (RFCs)

Requests for Comments (RFCs) are written definitions of protocol standards and proposed standards used for the Internet. The following RFCs might be helpful for understanding the Kerberos protocol and its related functions:

RFC 1509
In RFC 1509: Generic Security Service API : C-bindings, the Internet Engineering Task Force (IETF) formally defines GSS APIs.

RFC 1510
In RFC 1510: The Kerberos Network Authentication Service (V5), the Internet Engineering Task Force (IETF) formally defines the Kerberos V5 protocol.

RFC 1964
In RFC 1964, The Kerberos Version 5 GSS-API Mechanism, the Internet Engineering Task Force (IETF) defines Kerberos Version 5 and GSS API specifications.

RFC 2743

In RFC 2743: Generic Security Service Application Program Interface Version 2, Update 1, the Internet Engineering Task Force (IETF) formally defines GSS APIs.

To view the preceding RFCs listed, visit the RFC index search engine located on the RFC editor  Web site. Search for the RFC number you want to view. The search engine results display the corresponding RFC title, author, date, and status.

Saving PDF files

To save a PDF on your workstation for viewing or printing:

1. Right-click the PDF in your browser (right-click the link above).
2. Click the option that saves the PDF locally.
3. Navigate to the directory in which you want to save the PDF.
4. Click **Save**.

Downloading Adobe Reader

You need Adobe Reader installed on your system to view or print these PDFs. You can download a free copy from the Adobe Web site (www.adobe.com/products/acrobat/readstep.html)  .

Chapter 2. Special terms and conditions

This information contains special terms, conditions, and trademarks applicable to network authentication service.

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the information. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this information at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Department LZKS

11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written.

These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

The following copyright and permission notice applies to portions of this information that were obtained from the Massachusetts Institute of Technology.

Copyright © 1985-1999 by the Massachusetts Institute of Technology.

Export of software employing encryption from the United States of America may require a specific license from the United States Government. It is the responsibility of any person or organization contemplating export to obtain such a license before exporting.

WITHIN THAT CONSTRAINT, permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of M.I.T. not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. Furthermore if you modify this software you must label your software as modified software and not distribute it in such a fashion that it might be confused with the original MIT software. M.I.T. makes no representations about the suitability of this software for any purpose. It is provided ″as is″ without express or implied warranty.

The following copyright and permission notice applies to the OpenVision Kerberos Administration system located in kadmin/create, kadmin/dbutil, kadmin/passwd, kadmin/server, lib/kadm5, and portions of lib/rpc:

Copyright, OpenVision Technologies, Inc., 1996, All Rights Reserved WARNING: Retrieving the OpenVision Kerberos Administration system source code, as described below, indicates your acceptance of the following terms. If you do not agree to the following terms, do not retrieve the OpenVision Kerberos administration system. You may freely use and distribute the Source Code and Object Code compiled from it, with or without modification, but this Source Code is provided to you ″AS IS″ EXCLUSIVE OF ANY WARRANTY, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY OTHER WARRANTY, WHETHER EXPRESS OR IMPLIED. IN NO EVENT WILL OPENVISION HAVE ANY LIABILITY FOR ANY LOST PROFITS, LOSS OF DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, THOSE RESULTING FROM THE USE OF THE SOURCE CODE, OR THE FAILURE OF THE SOURCE CODE TO PERFORM, OR FOR ANY OTHER REASON.

OpenVision retains all copyrights in the donated Source Code. OpenVision also retains copyright to derivative works of the Source Code, whether created by OpenVision or by a third party. The OpenVision copyright notice must be preserved if derivative works are made based on the donated Source Code. OpenVision Technologies, Inc. has donated this Kerberos Administration system to MIT for inclusion in the standard Kerberos 5 distribution. This donation underscores our commitment to continuing Kerberos technology development and our gratitude for the valuable work which has been performed by MIT and the Kerberos community.

Kerberos V5 includes documentation and software developed at the University of California at Berkeley, which includes this copyright notice:

Copyright © 1983 Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

Permission is granted to make and distribute verbatim copies of this manual provided the copyright notices and this permission notice are preserved on all copies.

Permission is granted to copy and distribute modified versions of this manual under the conditions for verbatim copying, provided also that the entire resulting derived work is distributed under the terms of a permission notice identical to this one. Permission is granted to copy and distribute translations of this manual into another language, under the above conditions for modified versions.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

- AIX
- IBM
- Tivoli
- VisualAge

Kerberos is a trademark of the Massachusetts Institute of Technology (MIT).

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the U.S., other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

| IBM Corporation

Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, IBM License Agreement for Machine Code, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Programming Interface Information

This Network authentication service publication documents intended Programming Interfaces that allow the customer to write programs to obtain the services of IBM i5/OS.

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

| AIX
| AIX 5L
| Distributed Relational Database Architecture
| DRDA
| eServer
| i5/OS
| IBM
| IBM (logo)
| iSeries
| NetServer
| OS/400
| System i
| System p
| System z
| Tivoli
| VisualAge
| z/OS

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

| Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.

Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED ″AS-IS″ AND WITHOUT WARRANTY OF ANY KIND, EITHER

EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Printed in USA