IBM Defense Operations Platform
Version 1 Release 6

IBM Defense Operations Platform Product Documentation

IBM Defense Operations Platform
Version 1 Release 6

IBM Defense Operations Platform Product Documentation

Note

Before using this information and the product it supports, read the information in “Notices” on page 189.

This edition applies to IBM Defense Operations Platform version 1, release 6, modification 0. This edition applies to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Chapter 1. Solution overview

IBM® Defense Operations Platform provides an interoperable platform for military organizations and armed forces.

Armed forces worldwide face challenges adapting to increasingly dynamic and complex threats while being constrained by limited resources. Military organizations have moved from the concept of network-centric operations (NCO) towards warfighting benefit. Military leaders now focus on execution instead of networking. This direction values the rapid onboarding of mission capabilities. Rapid onboarding increases coordination and information sharing between military services and across a wide network of coalition partners, suppliers and external agencies.

Technology used by the military must support decisions affecting the lives and welfare of millions of people. Defense departments are continually looking for new capabilities to reduce risks. Technology innovation offers new opportunities, but deploying these innovations has not been an easy task. Progressing from prototype to live rollout can take years. In that time, technology evolves and develops through several generations. Defense departments can miss important opportunities to further reduce risk during this time. In the race to deliver new mission capabilities to demanding users, it is often necessary to compromise on important application components. With thousands of applications deployed, there are frequently thousands of alternative channels for users to interact with software and store information. A standard mission platform solves many of these difficulties.

With many of today's military systems operating as silos, it is difficult to achieve fully integrated, end-to-end capabilities. Interoperability must be built between systems instead of being built-in. While technology is available to help interoperability issues, establishing and maintaining a secure, reliable technical environment where technologies work well together is an extremely complex, expensive, and labor-intensive process. One node change can break the interoperability with others. The complexity and expense of these custom-configured heterogeneous environments can be one of the key factors slowing the process of getting new mission capabilities to the warfighter.

IBM Defense Operations Platform provides an interoperable platform that significantly reduces deployment times for new mission capabilities. Build packages include media, scripts and detailed configuration instructions applicable to command center, field and mobile deployments. These predefined, pretested packages enable IBM Defense Operations Platform to be installed in a day or two. Rapid implementation in a variety of environments allows military users to switch their focus to mission capabilities. The use of a common interoperable platform eliminates the disparity, duplication and problems typically found in traditional vertical integration.

IBM Defense Operations Platform is based on a unified security model which provides a rigorous and consistent approach for a comprehensive security framework.

IBM Defense Operations Platform editions

IBM Defense Operations Platform has been designed to operate across the defense enterprise. There are three deployable editions of the platform.

Each of these editions runs within the same IBM Defense Operations Platform environment, allowing for fast deployment of new or updated capabilities, and helping to ensure communication integrity. Because IBM Defense Operations Platform has been designed to provide many of the reusable core service-oriented architecture (SOA) services common to a variety of defense architectures—for example, NATO or Department of Defense core service standards—the platform can be fully integrated with new or existing compliant systems.

Command Center® Edition

The Command Center Edition is designed for units with strong infrastructure capabilities such as headquarters units, forward-operating bases or very large ships.

Field Edition

The Field Edition is designed for units in transit such as smaller ships, land vehicles, planes and mobile command posts.

Mobile Edition

The Mobile Edition is designed for individual soldier access in the mobile domain, such as through tactical vehicle installations, laptops and personal digital assistants (PDAs).

Workbench Edition

The Workbench Edition provides a set of tools to architect, engineer, implement, build, test, deploy and manage mission capabilities as applications and services across the Command Center Edition, Field Edition, and Mobile Edition . With this tooling, the Workbench Edition provides a development environment allowing the rapid creation, deployment, and management of mission capabilities.

The Workbench Edition requires the Command Center Edition as a development runtime.

Editions updated by IBM Defense Operations Platform 1.6

IBM Defense Operations Platform 1.6 provides updates to the Command Center Edition, Field Edition, and Workbench Edition. No update is provided to the Mobile Edition.

What's new in version 1.6

IBM Defense Operations Platform 1.6 introduces updated platform support and additional tooling.

In addition to updating packaged products to current versions and releases, IBM Defense Operations Platform provides three new tools:

Platform control tool
The platform control tool provides a single tool for an administrator to start, stop, and query the status of IBM Defense Operations Platform components and services. The administrator does not have to learn the different administrative services provided by the products included with IBM Defense Operations Platform. The platform control tool syntax is similar for all IBM Defense Operations Platform products.

Password management tool
IBM Defense Operations Platform provides a version of IBM Security Identity Manager allowing users and administrators to manage user and application IDs. Tools are provided to assist with password management, the ability to create and manage user accounts on multiple systems, and auditing. For example, the password management tool offers an easy way for administrators to change passwords for administrators or administrative accounts required by the underlying products within the IBM Defense Operations Platform.

Usage analysis tool
IBM Defense Operations Platform logs usage data that can them be processed using a usage analysis application.

IBM Defense Operations Platform system services

IBM Defense Operations Platform servers provide a number of services.

Analytics services
Provides data analysis, presentation, and reporting services.

Application build quality assurance services
Provides collaboration, automation and governance services for project information and status updates throughout the development lifecycle.

Application design and development services
Provides services for work-items, project activities, build, team progress dashboards and reports, planning, advanced source control and software configuration management.

Application deployment and management services
Provides services for software assembly, deployment and management.

Application services
Provides Java™ Enterprise Edition services supporting the solution.

Authentication and authorization services
Provides authentication and authorization services to the solution, applications, and other services.

Business monitoring services
Provides aggregation, analysis, and presentation of business process and activity information in real-time.

Collaboration services
Provides services to enable real-time collaboration for users and applications.

Configuration services
Manages the product configuration including inventory and change management.

Database services
Provides the database services for the solution and applications.

Identity management services
Provides services to manage the IBM Defense Operations Platform application and end user IDs.

Installation services
Provides services to install IBM Defense Operations Platform.

Messaging services
Provides message and workflow services.

Mobile services
Provides services enabling mobile users.

Password management services
Provides services to manage solution passwords.

Platform management services
Provides runtime management services including the ability to start, stop, and query the status of IBM Defense Operations Platform services and components.

Platform usage services
Provides services to analyze solution usage.

Standard operating procedure services
Provides services handling the processing of standard operating procedures.

Usage analysis services
Provides logging of usage data such as user log on, log out, timeout, and log in failures.

User directory integration - password synchronization plug-in services
Provides password synchronization where password changes are intercepted at the end points and redirected to the identity management services.

User interface services
Provides services supporting user interaction with the product.

User directory and user directory integration services
Provides mapping between user and group names and values and integration with additional directories.

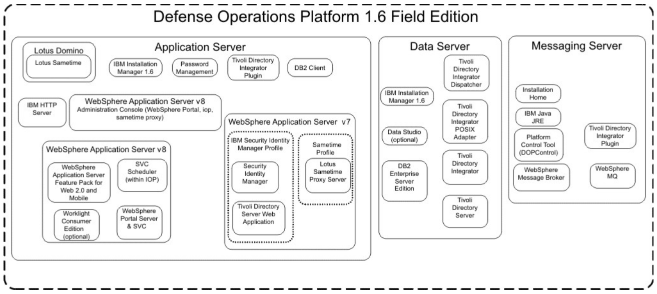
Web services
Provides HTTP, HTTPS, and other web services to the solution.

The following service is only available if the optional Data Studio tool is installed.

Data design services
Provides data design capabilities to application builders.

IBM Defense Operations Platform servers in the Field Edition

IBM Defense Operations Platform is installed on three servers in the Field Edition.


Defense Operations Platform 1.6 Field Edition
Application Server
Lotus Domino
Lotus Sametime
IBM Installation Manager 1.6
Password Management
Tivoli Directory Integrator Plugin
DB2 Client
IBM HTTP Server
WebSphere Application Server v8
Administration Console (WebSphere Portal, iop, sametime proxy)
WebSphere Application Server v8
WebSphere Application Server Feature Pack for Web 2.0 and Mobile
SVC Scheduler (within IOP)
Worklight Consumer Edition (optional)
WebSphere Portal Server & SVC
WebSphere Application Server v7
IBM Security Identity Manager Profile
Security Identity Manager
Tivoli Directory Server Web Application
Sametime Profile
Lotus Sametime Proxy Server
Data Server
IBM Installation Manager 1.6
Data Studio (optional)
DB2 Enterprise Server Edition
Tivoli Directory Integrator Dispatcher
Tivoli Directory Integrator POSIX Adapter
Tivoli Directory Integrator
Tivoli Directory Server
Messaging Server
Installation Home
IBM Java JRE
Platform Control Tool (DOPControl)
WebSphere Message Broker
Tivoli Directory Integrator Plugin
WebSphere MQ

Application server
This server provides the following services:
- Application services
- Business monitoring services
- User Interface services
- Collaboration services
- Mobile services
- Identity management services
- Authentication services
- Password management services
- Platform usage services
- KPI services
- Event ingestion services
- Standard operating procedure services
- Usage analysis services
- User directory integration - password synchronization plug-in services

Data server
This server provides the following services:
- Database services
- Data design services

- User directory services
- User directory integration services
- User directory integration - password synchronization plug-in services

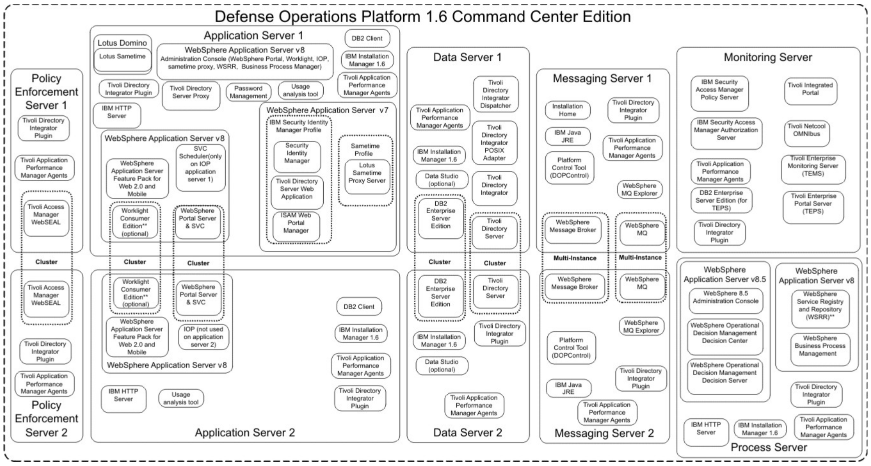
Messaging server

This server provides the following services:

- Installation services
- Messaging services
- Analytics services
- Platform management services
- Messaging services
- Reporting services
- User directory integration - password synchronization plug-in services

IBM Defense Operations Platform servers in the Command Center Edition

IBM Defense Operations Platform is installed on ten servers in the Command Center Edition.


Defense Operations Platform 1.6 Command Center Edition
Policy Enforcement Server 1
Tivoli Directory Integrator Plugin
Tivoli Application Performance Manager Agents
Tivoli Access Manager WebSEAL
Cluster
Tivoli Access Manager WebSEAL
Tivoli Directory Integrator Plugin
Tivoli Application Performance Manager Agents
Policy Enforcement Server 2
Application Server 1
Lotus Domino
Lotus Sametime
WebSphere Application Server v8
Administration Console (WebSphere Portal, Worklight, IOP, sametime proxy, WSRR, Business Process Manager)
DB2 Client
IBM Installation Manager 1.6
Tivoli Application Performance Manager Agents
Tivoli Directory Integrator Plugin
Tivoli Directory Server Proxy
Password Management
Usage analysis tool
IBM HTTP Server
WebSphere Application Server v8
WebSphere Application Server Feature Pack for Web 2.0 and Mobile
SVC Scheduler(only on IOP application server 1)
Worklight Consumer Edition** (optional)
WebSphere Portal Server & SVC
WebSphere Application Server v7
IBM Security Identity Manager Profile
Security Identity Manager
Tivoli Directory Server Web Application
ISAM Web Portal Manager
Sametime Profile
Lotus Sametime Proxy Server
Cluster
Cluster
Worklight Consumer Edition** (optional)
WebSphere Portal Server & SVC
WebSphere Application Server Feature Pack for Web 2.0 and Mobile
IOP (not used on application server 2)
WebSphere Application Server v8
DB2 Client
IBM Installation Manager 1.6
Tivoli Application Performance Manager Agents
Tivoli Directory Integrator Plugin
IBM HTTP Server
Usage analysis tool
Application Server 2
Data Server 1
Tivoli Directory Integrator Dispatcher
Tivoli Application Performance Manager Agents
Tivoli Directory Integrator POSIX Adapter
IBM Installation Manager 1.6
Data Studio (optional)
Tivoli Directory Integrator
DB2 Enterprise Server Edition
Tivoli Directory Server
Cluster
Cluster
DB2 Enterprise Server Edition
Tivoli Directory Server
IBM Installation Manager 1.6
Tivoli Directory Integrator Plugin
Data Studio (optional)
Tivoli Application Performance Manager Agents
Data Server 2
Messaging Server 1
Installation Home
Tivoli Directory Integrator Plugin
IBM Java JRE
Tivoli Application Performance Manager Agents
Platform Control Tool (DOPControl)
WebSphere MQ Explorer
WebSphere Message Broker
WebSphere MQ
Multi-Instance
Multi-Instance
WebSphere Message Broker
WebSphere MQ
WebSphere MQ Explorer
Platform Control Tool (DOPControl)
Tivoli Directory Integrator Plugin
IBM Java JRE
Tivoli Application Performance Manager Agents
Messaging Server 2
Monitoring Server
IBM Security Access Manager Policy Server
Tivoli Integrated Portal
IBM Security Access Manager Authorization Server
Tivoli Netcool OMNIbus
Tivoli Application Performance Manager Agents
Tivoli Enterprise Monitoring Server (TEMS)
DB2 Enterprise Server Edition (for TEPS)
Tivoli Enterprise Portal Server (TEPS)
Tivoli Directory Integrator Plugin
WebSphere Application Server v8.5
WebSphere 8.5 Administration Console
WebSphere Operational Decision Management Decision Center
WebSphere Operational Decision Management Decision Server
WebSphere Application Server v8
WebSphere Service Registry and Repository (WSRR)**
WebSphere Business Process Management
Tivoli Directory Integrator Plugin
IBM HTTP Server
IBM Installation Manager 1.6
Tivoli Application Performance Manager Agents
Process Server

Application server 1

This server provides the following services:

- Application services
- Business monitoring services
- User Interface services
- Collaboration services
- Mobile services
- Identity management services
- Authentication services
- Password management services
- Platform usage services
- KPI services
- Event ingestion services
- Standard operating procedure services
- Usage analysis services

- User directory integration - password synchronization plug-in services
- Monitoring agent services

Application server 2

This server provides the following services:

- Application services
- Business monitoring services
- User Interface services
- Mobile services
- Authentication services
- Platform usage services
- KPI services
- Event ingestion services
- Standard operating procedure services
- Usage analysis services
- User directory integration - password synchronization plug-in services
- Monitoring agent services

Data server 1

This server provides the following services:

- Database services
- Data design services
- User directory services
- User directory integration services
- User directory integration - password synchronization plug-in services
- Monitoring agent services

Data server 2

This server provides the following services:

- Database services
- Data design services
- User directory services
- User directory integration - password synchronization plug-in services
- Monitoring agent services

Messaging server 1

This server provides the following services:

- Installation services
- Messaging services
- Analytics services
- Platform management services
- Reporting services
- User directory integration - password synchronization plug-in services
- Monitoring agent services

Messaging server 2

This server provides the following services:

- Installation services
- Messaging services
- Analytics services

- Platform management services
- Reporting services
- User directory integration - password synchronization plug-in services
- Monitoring agent services

Policy enforcement server 1

This server provides the following services:

- Reverse proxy services
- User directory integration - password synchronization plug-in services
- Monitoring agent services

Policy enforcement server 2

This server provides the following services:

- Reverse proxy services
- User directory integration - password synchronization plug-in services
- Monitoring agent services

Monitoring server

This server provides the following services:

- Process monitoring services
- Event management services
- System monitoring services
- Enterprise system management services
- Enterprise system management administration services
- User directory integration - password synchronization plug-in services
- Access Manager policy server services
- Access Manager authorization server services
- Monitoring agent services
- Database services

Process server

This server provides the following services:

- Process workflow services
- Human task management services
- Operational decision center services
- Operational decision server services
- User directory integration - password synchronization plug-in services
- User directory proxy services
- Business process manager services
- Service Registry and Repository services
- Monitoring agent services

IBM Defense Operations Platform hardware requirements for the Field Edition

Three servers meeting minimum requirements are required to install IBM Defense Operations Platform Field Edition. The messaging server also serves as the installation server.

The servers must have Intel x86-64 or AMD x86-64 processors.

The minimum requirements for servers used by IBM Defense Operations Platform are shown in Table 1. The recommended minimum disk space does not include space for boot and swap partitions. These directories should be defined before IBM Defense Operations Platform is installed.

Table 1. Minimum hardware requirements

Resource	Application server	Messaging server	Data server
CPUs	4	4	4
Memory	14 GB	8 GB	8 GB
Network adapters	1	1	1
Disk space	93 GB	93GB	115 GB
Additional disk space required during installation	90 GB	37 GB (139 GB if the download media is to be stored on the server)	17 GB

For development and non-production environments with very light usage, the messaging server memory can be 4 GB and the data server memory can be 6 GB.

The minimum requirements for the directories on each server, excluding space required for the boot and swap partitions is shown in Table 2.

Table 2. Minimum space requirements for each directory

Directory	Minimum space	Notes®
/	8 GB	
/opt	32 GB	
/usr	8 GB	
/home	5 GB	
/tmp	12 GB	
/chroot	1 GB	
/datahome	22 GB	Only required on the data server.
/loghome	8 GB	
/installMedia	17 GB, 37 GB, or 90 GB	This directory can have a different name. However, if the directory is given a different name, the directory must be defined in the installation property file. This directory can be deleted after installation. The amount of space required is dependent on the server. • Data server: 17 GB • Messaging server: 37 GB • Application server: 90 GB
/distributionMedia	102 GB	This directory can have a different name. However, if the directory is given a different name, the directory must be defined in the installation property file. This directory is only required on the installation server
/var	8 GB	
/SWAP	8 GB	

IBM Defense Operations Platform hardware requirements for the Command Center Edition

Ten servers meeting minimum requirements are required to install IBM Defense Operations Platform Command Center Edition. Messaging server 1 also serves as the installation server.

The servers must have Intel x86-64 or AMD x86-64 processors.

The minimum requirements for servers used by IBM Defense Operations Platform are shown in Table 3. The recommended minimum disk space does not include space for boot and swap partitions.

Important: The configuration of data server 1 and data server 2 should be virtually identical. The configuration includes the hardware, operating system level and patches, network devices, and database versions. Having these servers as identical as possible will help with a smooth database failover process should one be required.

Table 3. Minimum hardware requirements

Resource	Application server 1	Application server 2	Messaging server 1	Messaging server 2	Data server 1	Data server 2	Policy enforcement server 1	Policy enforcement server 2	Monitoring server	Process server
CPUs	4	4	4	4	4	4	1	1	4	4
Memory	14 GB	14 GB	8 GB	8 GB	10 GB	10 GB	1 GB	1 GB	8 GB	8 GB
Network adapters	1	1	1	1	1	1	1	1	1	1
Disk space	103 GB	93 GB	115 GB	115 GB	115 GB	115 GB	63 GB	63 GB	93 GB	93 GB
Additional disk space required during installation	95 GB	70 GB	37 GB (182 GB if the download media is to be stored on the server)	37 GB	27 GB	27 GB	27 GB	27 GB	85 GB	90 GB

The minimum requirements for the directories on each server, excluding space required for the boot and swap partitions is shown in Table 4.

Table 4. Minimum space requirements for each directory

Directory	Minimum space	Notes
`/`	8 GB	
`/opt`	32 GB	
`/usr`	8 GB	
`/home`	5 GB	
`/tmp`	12 GB	
`/chroot`	1 GB	
`/datahome`	22 GB, 10 GB	Only required on the application server 1 (10 GB), application server 2 (10 GB), messaging server 1 (22 GB), messaging server 2 (22 GB), data server 1 (22 GB), data server 2 (22 GB).
`/loghome`	8 GB	

Table 4. Minimum space requirements for each directory (continued)

Directory	Minimum space	Notes
`/installMedia`	90 GB, 85 GB, 37 GB, 27 GB, 95 GB, 70 GB	This directory can have a different name. However, if the directory is given a different name, the directory must be defined in the installation property file. This directory can be deleted after installation. The amount of space required is dependent on the server. • Process server: 90GB • Monitoring server: 85 GB • Data server: 27 GB • Policy enforcement server: 27 GB • Messaging server: 37 GB • Application server 1: 95 GB • Application server 2: 70 GB
`/distributionMedia`	142 GB	This directory can have a different name. However, if the directory is given a different name, the directory must be defined in the installation property file. This directory is only required on the installation server
`/var`	8 GB	
`/SWAP`	8 GB	

In addition, a customer-provided load balancer infrastructure is required to connect to the policy enforcement server.

Prerequisite software requirements

Before installing IBM Defense Operations Platform, all servers must have the appropriate software installed.

IBM Defense Operations Platform requires Red Hat Enterprise Server Linux version 6 at release 6.3 or higher. Specific Linux RPM packages must be installed as part of the steps to prepare the servers.

A workstation with Windows is also required to configure single sign-on for collaboration services.

It is recommended that the servers only have the prerequisite software installed. Any installation of IBM Defense Operations Platform installed on the servers must be removed before installing IBM Defense Operations Platform.

Related tasks:

"Installing Linux packages for the Field Edition" on page 19
Before installing IBM Defense Operations Platform, Linux packages need to be installed on the servers.

"Installing Linux packages for the Command Center Edition" on page 21
Before installing IBM Defense Operations Platform, Linux packages need to be installed on the servers.

"Configuring single sign-on for collaboration services" on page 44
Import the WebSphere® Portal SSO LTPA token into the application server to allow users to access collaboration services without having to reenter their credentials.

Chapter 2. Installing and configuring

IBM Defense Operations Platform provides installation options to install the product environment and application. After installing IBM Defense Operations Platform, some additional configuration is required.

Installation server

The server used when installing IBM Defense Operations Platform depends on whether IBM Defense Operations Platform is being installed for Command Center Edition or Field Edition.

For the Field Edition, the installation server is the messaging server.

For the Command Center Edition, the installation server is messaging server 1.

Installation checklists

Installation checklists are available for the installation options for IBM Defense Operations Platform. These checklists provide an overview of the installation steps and can be used to track the installation progress.

Checklist - installing the IBM Defense Operations Platform Field Edition

Use this checklist to track the installation steps when installing the IBM Defense Operations Platform Field Edition.

Procedure

__ 1. Review the IBM Defense Operations Platform preventive service planning technote for changes to the product documentation that might affect the installation and usage of IBM Defense Operations Platform..

__ 2. Make sure you have the necessary hardware.

__ 3. Make sure the required software is installed on the hardware.

__ 4. Optional: Use the kickstart file to prepare Red Hat Enterprise Linux on the servers. Operating system preparation can also be done manually as part of the Prepare the servers. steps.

__ 5. Prepare the servers.

   a. Set up TCP/IP networking.

   b. Disable security settings.

   c. Set up ssh services.

   d. Install required Linux packages.

   e. Set other pre-installation requirements.

   f. Prepare the installation server

__ 6. Verify and customize the installation properties as required.

__ 7. Define the topology for the installation by editing the topology properties file.

__ 8. Run the command line installer.

   Important: Make sure you record the installation password. All installation related tasks require the installation password. The installation password is also the initial topology password needed when running the password management tool and platform control tool. The topology password can be changed. The default topology password and installation password is `ibmdop16`.

__ 9. Verify the installation prior to configuring IBM Defense Operations Platform.

__ 10. Configure IBM Defense Operations Platform.

  __ a. Configure single sign-on for collaboration services.

  __ b. Configure the Tivoli Directory Server web administration tool host name

  __ c. Optional: Enable Tivoli Directory Server logging

  __ d. Optional: Configure the session timeout.

  __ e. Optional: Configure the LTPA timeout.

__ 11. Verify that IBM Defense Operations Platform is correctly installed.

__ 12. Install any other applications.

Results

The IBM Defense Operations Platform architecture is installed and ready for use.

Checklist - installing the IBM Defense Operations Platform Command Center Edition

Use this checklist to track the installation steps when installing the IBM Defense Operations Platform Command Center Edition.

Procedure

__ 1. Review the IBM Defense Operations Platform preventive service planning technote for changes to the product documentation that might affect the installation and usage of IBM Defense Operations Platform..

__ 2. Make sure you have the necessary hardware.

__ 3. Make sure the required software is installed on the hardware.

__ 4. Optional: Use the kickstart file to prepare Red Hat Enterprise Linux on the servers. Operating system preparation can also be done manually as part of the Prepare the servers. steps.

__ 5. Prepare the servers.

  a. Set up TCP/IP networking.

  b. Disable security settings.

  c. Set up ssh services.

  d. Install required Linux packages.

  e. Set other pre-installation requirements.

  f. Prepare the servers to run in a high availability environment.

  g. Prepare the installation server

__ 6. Verify and customize the installation properties as required.

__ 7. Define the topology for the installation by editing the topology properties file.

__ 8. Run the command line installer.

  Important: Make sure you record the installation password. All installation related tasks require the installation password. The installation password is also the initial topology password needed when running the password management tool and platform control tool. The topology password can be changed. The default topology password and installation password is `ibmdop16`.

__ 9. Verify the installation prior to configuring IBM Defense Operations Platform.

__ 10. Configure IBM Defense Operations Platform.

  __ a. Configure single sign-on for collaboration services.

  __ b. Configure additional cluster manager relationships.

  __ c. Optional: Configure the session timeout.

__ d. Optional: Configure the LTPA timeout.

__ e. Optional: Configure an optional external network file system.

__ 11. Verify that IBM Defense Operations Platform is correctly installed.

__ 12. Install any other applications.

Results

The IBM Defense Operations Platform architecture is installed and ready for use.

Using kickstart files to prepare Red Hat Enterprise Linux

IBM Defense Operations Platform includes sample Red Hat Enterprise Linux V6 kickstart files to prepare the operating system for virtual or hardware servers.

About this task

IBM Defense Operations Platform server requirements assume that the `minimal` installation option is selected during the installation of Red Hat Enterprise Linux. The `minimal` option provides only the @core and @server-policy packages essential to run Red Hat Enterprise Linux. The @core and @server-policy packages provide the required Linux rpm packages for a single-purpose server or desktop appliance and maximizes performance and security for the installation. The kickstart files included with IBM Defense Operations Platform includes all packages needed for IBM Defense Operations Platform and can be used to prepare the servers for installation.

The kickstart files can be found in the `/rhel-kickstart` directory in the installation media.

The kickstart files provided for the Field Edition are:

- `d2_ks-dopmsg-min.cfg` - kickstart file for the messaging server
- `d2_ks-dopapp-min.cfg` - kickstart file for the application server
- `d2_ks-dopdb-min.cfg` - kickstart file for the data server

The kickstart files provided for the Command Center Edition are:

- `d1_ks-dopmsg1-min.cfg` - kickstart file for the messaging server 1
- `d1_ks-dopmsg2-min.cfg` - kickstart file for the messaging server 2
- `d1_ks-dopapp1-min.cfg` - kickstart file for the application server 1
- `d1_ks-dopapp2-min.cfg` - kickstart file for the application server 2
- `d1_ks-dopdb1-min.cfg` - kickstart file for the data server 1
- `d1_ks-dopdb2-min.cfg` - kickstart file for the data server 2
- `d1_ks-dopdmz1-min.cfg` - kickstart file for the policy enforcement server 1
- `d1_ks-dopdmz2-min.cfg` - kickstart file for the policy enforcement server 2
- `d1_ks-doppro-min.cfg` - kickstart file for the process server
- `d1_ks-dopmon-min.cfg` - kickstart file for the monitoring server

Procedure

Setup each kickstart file.

1. Edit the kickstart file.
2. Change the `lang` value to the language for your installation. The default is `en_US.UTF-8`.
3. Change the `rootpw` value to the root password for the system. The default is `ibmdop16`.
4. Change the `timezone` value to the time zone for your installation. The default is `America/New_York`.
5. Change the `network` information for the target system. The default is different for each server.

6. Optional: Change the file system partition layout. In the default configuration, all file system partitions are created under one disk.

Use the kickstart file to configure the server or virtual machine.

7. Complete the pre-install steps in the kickstart file.
8. Use the kickstart file to install and configure Red Hat Enterprise Linux on the hardware server or virtual machine.
9. Complete the post-install steps in the kickstart file.
10. Create a snapshot of the virtual machine or a backup of the hardware server.

What to do next

After the operating system is configured on all hardware servers or virtual machines using the kickstart files, continue with the other server preparation steps. The kickstart files install the required Linux packages, so those steps can be skipped. After the servers are prepared, install IBM Defense Operations Platform.

Related tasks:

"Preparing the servers"
Before installing IBM Defense Operations Platform, all servers must be correctly prepared or the installation will fail. The precheck step will verify that many of these requirements have been implemented for all servers.

"Installing Linux packages for the Field Edition" on page 19
Before installing IBM Defense Operations Platform, Linux packages need to be installed on the servers.

"Installing Linux packages for the Command Center Edition" on page 21
Before installing IBM Defense Operations Platform, Linux packages need to be installed on the servers.

Preparing the servers

Before installing IBM Defense Operations Platform, all servers must be correctly prepared or the installation will fail. The precheck step will verify that many of these requirements have been implemented for all servers.

About this task

If running in a virtual environment, using a template for these steps can help reduce setup time. Follow the steps in each section for each server or create a RHEL template with these steps.

Setting up TCP/IP networking

Before installing IBM Defense Operations Platform, TCP/IP networking needs to be set up on the servers.

About this task

If you are installing IBM Defense Operations Platform Command Center Edition, you must use IPV4. Server clustering does not support IPV6.

IPv6 networking is supported by IBM Defense Operations Platform Field Edition, but IPv4 must be installed and configured as well. IPv4 addresses do not need to be assigned to the servers, but the IPv4 loopback address (`127.0.0.1`) must be enabled and the `localhost` host name must resolve to `127.0.0.1`.

Configuration changes are shown in Table 5 on page 15. Set up TCP/IP networking on the IBM Defense Operations Platform installation server and target servers by editing the Linux network configuration files. The configuration notes in Table 5 on page 15 are only guidelines. Any network setup conforming to the requirements should work.

Table 5. TCP/IP configuration guidelines

File	Notes

/etc/hosts	The hosts file resolves TCP/IP names to IP addresses. If the configuration does not have a DNS server, all servers and their IP addresses, short host names, and fully-qualified names must be defined in this file. Local loopback addresses and host names are also defined in this file.
	If a DNS server is being used, hosts which are resolved by the DNS do not need to be included in this file.
	Important: When using IPv4, the local loopback address `127.0.0.1` must be mapped to the `localhost` and `localhost.localdomain` host names.
	The following is a sample `/etc/hosts` file using IPv4 addresses.
	`# local loopback definitions -- do not remove`
	`# or alter these!`
	`127.0.0.1 localhost.localdomain localhost`
	`# use the following if IPv6 is enabled in your`
	`# network definitions`
	`::1 localhost6.localdomain localhost6`
	
	`# target runtime servers for the Field Edition`
	`192.168.0.211 dopapp.dop16.com dopapp`
	`192.168.0.212 dopdb.dop16.com dopdb`
	`192.168.0.213 dopmsg.ioc16.com dopmsg`
	
	`# target runtime servers for the`
	`# Command Center Edition`
	`192.168.0.214 doppol1.dop16.com doppol1`
	`192.168.0.215 doppol2.dop16.com doppol2`
	`192.168.0.216 dopapp1.dop16.com dopapp1`
	`192.168.0.217 dopapp2.dop16.com dopapp2`
	`192.168.0.218 dopdb1.dop16.com dopdb1`
	`192.168.0.219 dopdb2.dop16.com dopdb2`
	`192.168.0.220 dopana1.dop16.com dopana1`
	`192.168.0.221 dopana2.dop16.com dopana2`
	`192.168.0.222 dopmon.dop16.com dopmon`
	`192.168.0.223 doppro.dop16.com doppro`
	Use IPv6 address notation to assign IPv6 static addresses .
	Both IPv6 and IPv4 addresses can be defined on the same server.

Table 5. TCP/IP configuration guidelines (continued)

File	Notes
/etc/sysconfig/network-scripts/ifcfg-*adapter_name*	The ifcfg-*adapter_name* file defines the basic network settings for the specified network adapter. The Linux assigned name for the network adapter is specified by *adapter_name*. The typical value for *adapter_name* is eth0 but might be different for your environment. For IPv4 networking the following parameters should be defined. **IPADDR** Specify the IPv4 IP address of the server being configured. **NETMASK** Specify the IPv4 network mask of the server being configured. **GATEWAY** Specify the IPv4 default network IP address of the server being configured. **BOOTPROTO** If static IP addressing is being used, specify none. **NM_CONTROLLED** Specify no to disable the Network Management service from modifying the ifcfg-*adapter_name* file. **ONBOOT** Specify yes to start the adapter automatically. **IPV6INIT** Specify yes if the adapter is to use IPv6 networking. **IPV6ADDR** Specify the server IPv6 IP address if IPV6INIT=yes is specified. **IPV6_DEFAULTGW** Specify the server IPv6 default network gateway IP address if IPV6INIT=yes is specified.
/etc/sysconfig/network	The network file specifies general networking parameters. For IPv4 networking the following parameters should be defined: **NETWORKING** Specify yes to enable IPv4 networking. **NETWORKING_IPV6** Specify yes if IPv6 networking is also desired. **HOSTNAME** Specify the server short host name. Hostname configuration changes made by editing the /etc/sysconfig/network file will not take affect until the server is restarted. If a restart isn't desired, change the hostname for the current shell session by running the **hostname** *new_host_name* command. For example, to change the hostname of the server to dopweb, run the **hostname dopweb** command.

Table 5. TCP/IP configuration guidelines (continued)

File	Notes

`/etc/resolv.conf`	The `resolv.conf` file is used to define DNS servers for the network and a default search domain. If DNS servers are not being used, this file should be empty. If both DNS servers and `/etc/hosts` are being used, the priority of which file is used is specified in the `/etc/nsswitch.conf` file.
	If a DNS server is used, the `resolv.conf` should contain the following lines:
	`search` *`domain_name`*
	`nameserver` *`first_DNS_server`*
	`nameserver` *`second_DNS_server`*
	For example:
	`search yourcompany.com`
	`nameserver 10.75.20.10`
	`nameserver 10.75.20.11`
	The `search` value specifies the default search domain. The first `nameserver` value is the IP address of the DNS server. A second `nameserver` value can be used to specify a secondary DNS server. The second `nameserver` specification is optional.

Procedure

1. Define a fully-qualified name and short host name using a DNS server or by definition in the `/etc/hosts` file. The host names must resolve on each server to the correct IP address.

   The fully-qualified host name for each server must have at least three components. For example: `myhost.mydomain.com` where the top level domain is a standard Internet top-level domain.

   Important: Short host names and fully-qualified host names must be specified in the correct case. For example, MyCompany.MyDomain.com cannot be specified as mycompany.mydomain.com.
2. (For Command Center Edition only) Make sure that the HOSTNAME set in `/etc/sysconfig/network` is set to the short host name and not the fully qualified host name. For example, set `HOSTNAME=xyz` instead of `HOSTNAME=xyz.yourco.com`.
3. Verify the hostname, fully qualified hostname, and domain names are configured on all servers. The servers are correctly configured if the following tests complete successfully.
   a. The **`hostname -s`** command returns the defined short host name for the server.
   b. The **`hostname -f`** command returns the fully qualified domain and host name for the server.
   c. The **`hostname -d`** command returns the domain name of the server.
   d. The results of a **`ping`** command, or **`ping6`** command for IPV6 environments, with the short host name for each server indicates that the server is accessible.
   e. The results of a **`ping`** command, or **`ping6`** command for IPV6 environments, with the fully-qualified name for each server indicates that the server is accessible.
4. Enable local loopback addressing for each server in the `/etc/hosts` file.
5. Verify local loopback addressing. The servers are correctly configured if the following tests complete successfully.
   a. The **`ping -n localhost`** command returns the address `127.0.0.1`.
   b. The **`ping -n localhost.localdomain`** command returns the address `127.0.0.1`.
   c. The **`ping6 -n localhost6`** command in an IPV6 environment returns the address `::1`.

d. The **ping6 -n localhost6.localdomain6** command in an IPV6 environment returns the address `::1`.

6. Add or update the **net.ipv4.tcp_fin_timeout=15** parameter in the `/etc/sysctl.conf` file for the following servers.

   For the Command Center Edition

   - Application server
   - Messaging server
   - Data server
   - Policy enforcement server
   - Process server
   - Monitoring server

   For the Field Edition

   - Application server
   - Messaging server
   - Data server

   Restart the server after changing the `/etc/sysctl.conf` file.

   If this step is not done when the servers are prepared, the IBM Defense Operations Platform installation program will correct the setting for all servers.

Disabling security settings

Before installing IBM Defense Operations Platform, certain security settings must be disabled. These can be re-enabled after IBM Defense Operations Platform is installed.

About this task

If the following steps are not done prior to installing IBM Defense Operations Platform, the installer will disable any firewalls. SELinux will also be disabled unless set to "permissive". If set to "permissive" the setting will be retained. In all cases the installation will proceed successfully.

Procedure

1. Disable SELinux (Security Enforcing Linux) by editing the `/etc/selinux/config` file and changing `SELINUX` to `disabled`. After changing the configuration, restart the server.
2. Disable all Linux firewalls.

Setting up ssh services

Before installing IBM Defense Operations Platform, ssh services need to be set up on the servers. The service needs to be enabled for root login with password authentication.

About this task

TCP/IP port 22 must be configured in the operating system as an available ssh access port for use during installation processing. The TCP/IP port number for platform control tool ssh access is specified in the topology properties file. Only the platform control tool uses the configured port.

Procedure

1. Edit the `/etc/ssh/sshd_config` file.
2. Make sure the following lines are specified as follows. Make sure there is no # sign at the start of these lines.

```
PermitRootLogin yes
PasswordAuthentication yes
```

3. Save the changed file.
4. Start, or restart, the `sshd` service on each server by running the **`service sshd restart`** command.

Installing Linux packages for the Field Edition

Before installing IBM Defense Operations Platform, Linux packages need to be installed on the servers.

About this task

Linux package requirements assumes that the `Minimal` option is selected during Red Hat installation. The `Minimal` option provides only the @core and @server-policy packages which are essential to run Red Hat Enterprise Linux. A minimal installation provides the base for a single-purpose server or desktop appliance and maximizes performance and security for the installation.

The Linux packages in following table must be installed on the IBM Defense Operations Platform servers. These packages are available from Red Hat.

Table 6. Required Linux packages for IBM Defense Operations Platform servers

Application server	Messaging server	Data server
bc.x86_64 compat-db.i686 compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++*i686 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.x86_64 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zip.x86_64 zlib.i686 zlib.x86_64	compat-db.i686 compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++*i686 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 gettext-libs.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXft.i686 libXft.x86_64 libXmu.i686 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 redhat-lsb.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zlib.i686 zlib.x86_64	audit-libs.i686 audit-libs.x86_64 compat-libstdc++*i686 compat-libstdc++*x86_64 dos2unix.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++.i686 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openssh-clients.x86_64 pam.i686 pam-devel.i686 pam_passwdqc.x86_64 tcsh.x86_64 unzip.x86_64 xulrunner.x86_64 xorg-x11-xauth.x86_64 zlib.i686 zlib.x86_64 zip.x86_64

Procedure

1. All required Linux packages can be installed in all severs, or, only the packages required for each server can be installed.
   - To install all packages on all servers, run the following commands on each server. Each **`yum`** command needs to be specified as a single line.

     ```
     yum install -y audit-libs.i686 audit-libs.x86_64 bc.x86_64
     compat-db.i686 compat-db.x86_64 compat-glibc.x86_64
     compat-glibc-headers.x86_64 compat-libstdc++*i686
     compat-libstdc++*x86_64 dos2unix.x86_64 elfutils.x86_64
     elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64
     gettext.x86_64
     gettext-libs.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64
     ```

```
gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64
libaio.i686
libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++.i686 libXft.i686
libXft.x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.i686
libXpm.x86_64 libXpm-devel.i686 libXpm-devel.x86_64 libXtst.i686
libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64
nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64
openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64
pam.i686 pam-devel.i686 redhat-lsb.x86_64 rpm-build.x86_64
unzip.x86_64 xorg-x11-xauth.x86_64 zip.x86_64 zlib.i686 zlib.x86_64
pam_passwdqc.x86_64 tcsh.x86_64 xulrunner.x86_64
zip.x86_64

yum -y update
```

- To install only the packages required by each server, run the following commands. Each **yum** command needs to be specified as a single line.

  On the application server:

  ```
  yum install -y bc.x86_64 compat-db.i686 compat-db.x86_64
  compat-glibc.x86_64 compat-glibc-headers.x86_64
  compat-libstdc++*i686 dos2unix.x86_64 elfutils.x86_64
  elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64  gettext.x86_64
  glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686
  gtk2-engines.x86_64 libaio.i686
  ksh.x86_64libaio.x86_64 libgcc.i686
  libgcc.x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.x86_64
  libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64
  nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64
  openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64
  rpm-build.x86_64 unzip.x86_64 zip.x86_64 zlib.i686 zlib.x86_64
  pam_passwdqc.x86_64 tcsh.x86_64

  yum -y update
  ```

  On the messaging server:

  ```
  yum install -y compat-db.i686 compat-db.x86_64 compat-glibc.x86_64
  compat-glibc-headers.x86_64 compat-libstdc++*i686 dos2unix.x86_64
  elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64
  gettext.x86_64 gettext-libs.x86_64 glibc.i686 glibc.x86_64
  gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64
  ksh.x86_64 expect.x86_64
  libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXft.i686
  libXft.x86_64 libXmu.i686 libXtst.i686 libXtst.x86_64
  nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686
  nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686
  openmotif22.x86_64 openssh-clients.x86_64 redhat-lsb.x86_64
  rpm-build.x86_64 unzip.x86_64 zlib.i686 zlib.x86_64
  pam_passwdqc.x86_64 tcsh.x86_64

  yum -y update
  ```

  On the data server:

  ```
  yum install -y audit-libs.i686 audit-libs.x86_64
  compat-libstdc++*i686 compat-libstdc++*x86_64 dos2unix.x86_64
  gettext.x86_64 glibc.i686 glibc.x86_64 ksh.x86_64 libaio.i686
  libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++.i686
  nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64
  openssh-clients.x86_64 pam.i686 pam-devel.i686 unzip.x86_64
  xorg-x11-xauth.x86_64 zlib.i686 zlib.x86_64
  pam_passwdqc.x86_64 tcsh.x86_64
  zip.86_64 xulrunner.x86_64  expect.x86_64

  yum -y update
  ```

2. Optional: Install the Linux packages for the X Window System on the application server. These packages are required if the password management tool will be used.
   a. Install the packages for the GNOME or KDE desktop.

To install the GNOME desktop run:

```
yum -y groupinstall "X Window System" Desktop
```

To install the KDE desktop run:

```
yum -y groupinstall "X Window System" "KDE Desktop"
```

b. Run `yum -y update`

c. Start the desktop by running `init 5`. To make the GUI desktop the default desktop, do the following.

   1) Edit the `/etc/inittab` file.

   2) Change the `initdefault` property from `3` to `5`. The updated line should be as follows.

      ```
      id:5:initdefault:
      ```

   3) Save the changes.

   4) Restart the server.

3. Optional: If IBM Defense Operations Platform is to be used in Chinese or French, run the appropriate command.

Language	**Command**
Chinese	`yum install -y "@Chinese Support"`
French	`yum install -y "@French Support"`

Related information:

➡ http://www.redhat.com/

Installing Linux packages for the Command Center Edition

Before installing IBM Defense Operations Platform, Linux packages need to be installed on the servers.

About this task

Linux package requirements assumes that the `Minimal` option is selected during Red Hat installation. The `Minimal` option provides only the @core and @server-policy packages which are essential to run Red Hat Enterprise Linux. A minimal installation provides the base for a single-purpose server or desktop appliance and maximizes performance and security for the installation.

The Linux packages in following table must be installed on the IBM Defense Operations Platform servers. These packages are available from Red Hat.

Table 7. Required Linux packages for primary IBM Defense Operations Platform servers

Application server 1	Messaging server 1	Data server 1	Policy enforcement server 1
bc.x86_64 compat-db.i686 compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++*i686 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.x86_64 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zip.x86_64 zlib.i686 zlib.x86_64 compat-libstdc++*x86_64 ksh.x86_64 libstdc++*i686 libstdc++*x86_64	compat-db.i686 compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++*i686 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 gettext-libs.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXft.i686 libXft.x86_64 libXmu.i686 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 redhat-lsb.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zlib.i686 zlib.x86_64 compat-libstdc++*x86_64 ksh.x86_64 libstdc++*i686 libstdc++*x86_64	audit-libs.i686 audit-libs.x86_64 compat-libstdc++*i686 compat-libstdc++*x86_64 dos2unix.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++.i686 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openssh-clients.x86_64 pam.i686 pam-devel.i686 pam_passwdqc.x86_64 tcsh.x86_64 unzip.x86_64 xulrunner.x86_64 xorg-x11-xauth.x86_64 zlib.i686 zlib.x86_64 zip.x86_64 libstdc++*x86_64 xulrunner.x86_64	compat-db.i686 compat-db.x86_64 compat-libstdc++*i686 compat-libstdc++*x86_64 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libgcc.i686 libgcc.x86_64 libstdc++*i686 libstdc++*x86_64 libXp.i686 libXpm.i686 libXpm.x86_64 libXpm-devel.i686 libXpm-devel.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zlib.i686 zlib.x86_64

Table 8. Required Linux packages for standby IBM Defense Operations Platform servers

Application server 2	Messaging server 2	Data server 2	Policy enforcement server 2
bc.x86_64 compat-db.i686 compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++*i686 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.x86_64 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zip.x86_64 zlib.i686 zlib.x86_64 compat-libstdc++*x86_64 ksh.x86_64 libstdc++*i686 libstdc++*x86_64	compat-db.i686 compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++*i686 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 gettext-libs.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXft.i686 libXft.x86_64 libXmu.i686 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 redhat-lsb.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zlib.i686 zlib.x86_64 compat-libstdc++*x86_64 ksh.x86_64 libstdc++*i686 libstdc++*x86_64	audit-libs.i686 audit-libs.x86_64 compat-libstdc++*i686 compat-libstdc++*x86_64 dos2unix.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++.i686 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openssh-clients.x86_64 pam.i686 pam-devel.i686 pam_passwdqc.x86_64 tcsh.x86_64 unzip.x86_64 xulrunner.x86_64 xorg-x11-xauth.x86_64 zlib.i686 zlib.x86_64 zip.x86_64 libstdc++*x86_64 xulrunner.x86_64	compat-db.i686 compat-db.x86_64 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libgcc.i686 libgcc.x86_64 libXp.i686 libXpm.i686 libXpm.x86_64 libXpm-devel.i686 libXpm-devel.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zlib.i686 zlib.x86_64

Table 9. Required Linux packages for IBM Defense Operations Platform monitoring and process servers

Monitoring server	Process server
audit-libs.i686 audit-libs.x86_64 bc.x86_64 compat-db.i686 compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++*i686 compat-libstdc++*x86_64 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 gettext-libs.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++*i686 libstdc++*x86_64 libstdc++.i686 libXft.i686 libXft.x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.i686 libXpm.x86_64 libXpm-devel.i686 libXpm-devel.x86_64 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam.i686 pam_passwdqc.x86_64 pam-devel.i686 redhat-lsb.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 xorg-x11-xauth.x86_64 zip.x86_64 zlib.i686 zlib.x86_64	bc.x86_64 compat-db.i686 compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++*i686 compat-libstdc++*x86_64 dos2unix.x86_64 elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++*i686 libstdc++*x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.x86_64 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam_passwdqc.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64 zip.x86_64 zlib.i686 zlib.x86_64

Procedure

1. All required Linux packages can be installed in all severs, or, only the packages required for each server can be installed.

   - To install all packages on all servers, run the following commands on each server. Each **yum** command needs to be specified as a single line.

     ```
     yum install -y audit-libs.i686 audit-libs.x86_64 bc.x86_64 compat-db.i686
     compat-db.x86_64 compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++*i686
     compat-libstdc++*x86_64 compat-libstdc++*x86_64 dos2unix.x86_64 elfutils.x86_64
     elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 gettext-libs.x86_64 glibc.i686
     glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64 ksh.i86_64
     ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++.i686 libstdc++*x86_64
     libXft.i686 libXft.x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.i686 libXpm.x86_64
     libXpm-devel.i686 libXpm-devel.x86_64 libXtst.i686 libXtst.x86_64 nfs-utils.x86_64
     nfs-utils-lib.x86_64 nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64
     openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64 pam.i686 pam-devel.i686
     pam_passwdqc.x86_64 redhat-lsb.x86_64 rpm-build.x86_64 tcsh.x86_64 unzip.x86_64
     xorg-x11-xauth.x86_64 xulrunner.x86_64 zip.x86_64 zlib.i686 zlib.x86_64

     yum -y update
     ```

- To install only the packages required by each server, run the following commands. Each **yum** command needs to be specified as a single line.

  On application server 1 and application server 2:

  ```
  yum install -y compat-libstdc++*x86_64 ksh.i86_64 libstdc++*i686 libstdc++*x86_64 expect.x86_64
  ```

  ```
  yum install -y bc.x86_64 compat-db.i686 compat-db.x86_64
  compat-glibc.x86_64 compat-glibc-headers.x86_64
  compat-libstdc++*i686 dos2unix.x86_64 elfutils.x86_64
  elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64  gettext.x86_64
  glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64 gtk2-engines.i686
  gtk2-engines.x86_64 libaio.i686
  ksh.x86_64libaio.x86_64 libgcc.i686
  libgcc.x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.x86_64
  libXtst.i686 libXtst.x86_64 nfs-utils.x86_64 nfs-utils-lib.x86_64
  nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64
  openmotif22.i686 openmotif22.x86_64 openssh-clients.x86_64
  rpm-build.x86_64 unzip.x86_64 zip.x86_64 zlib.i686 zlib.x86_64
  pam_passwdqc.x86_64 tcsh.x86_64

  yum -y update
  ```

  On messaging server 1 and messaging server 2:

  ```
  yum install -y compat-libstdc++*x86_64 expect.x86_64
  ksh.x86_64 libstdc++*i686 libstdc++*x86_64 expect.x86_64
  ```

  ```
  yum install -y compat-db.i686 compat-db.x86_64 compat-glibc.x86_64
  compat-glibc-headers.x86_64 compat-libstdc++*i686 dos2unix.x86_64
  elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64
  gettext.x86_64 gettext-libs.x86_64 glibc.i686 glibc.x86_64
  gtk2.i686 gtk2.x86_64 gtk2-engines.i686 gtk2-engines.x86_64
  ksh.x86_64 expect.x86_64
  libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64 libXft.i686
  libXft.x86_64 libXmu.i686 libXtst.i686 libXtst.x86_64
  nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686
  nss-softokn-freebl.x86_64 ntp.x86_64 openmotif22.i686
  openmotif22.x86_64 openssh-clients.x86_64 redhat-lsb.x86_64
  rpm-build.x86_64 unzip.x86_64 zlib.i686 zlib.x86_64
  pam_passwdqc.x86_64 tcsh.x86_64

  yum -y update
  ```

  On data server 1 and data server 2:

  ```
  yum install -y libstdc++*x86_64 xulrunner.x86_64 expect.x86_64
  ```

  ```
  yum install -y audit-libs.i686 audit-libs.x86_64
  compat-libstdc++*i686 compat-libstdc++*x86_64 dos2unix.x86_64
  gettext.x86_64 glibc.i686 glibc.x86_64 ksh.x86_64 libaio.i686
  libaio.x86_64 libgcc.i686 libgcc.x86_64 libstdc++.i686
  nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64
  openssh-clients.x86_64 pam.i686 pam-devel.i686 unzip.x86_64
  xorg-x11-xauth.x86_64 zlib.i686 zlib.x86_64
  pam_passwdqc.x86_64 tcsh.x86_64
  zip.86_64 xulrunner.x86_64  expect.x86_64

  yum -y update
  ```

  On policy enforcement server 1 and policy enforcement server 2

  ```
  yum install -y compat-db.i686 compat-db.x86_64 dos2unix.x86_64
  elfutils.x86_64 elfutils-libs.i686 elfutils-libs.x86_64 expect.x86_64
  gettext.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64
  gtk2-engines.i686 gtk2-engines.x86_64 ksh.x86_64 libgcc.i686
  libgcc.x86_64 libXp.i686 libXpm.i686 libXpm.x86_64
  libXpm-devel.i686 libXpm-devel.x86_64 nss-softokn-freebl.i686
  nss-softokn-freebl.x86_64 ntp.x86_64 openssh-clients.x86_64
  rpm-build.x86_64 unzip.x86_64 zlib.i686
  zlib.x86_64 pam_passwdqc.x86_64 tcsh.x86_64

  yum -y update
  ```

On the monitoring server:

```
yum install audit-libs.i686 audit-libs.x86_64 bc.x86_64
compat-db.i686 compat-db.x86_64
compat-glibc.x86_64 compat-glibc-headers.x86_64 compat-libstdc++*i686
compat-libstdc++*x86_64
dos2unix.x86_64  elfutils.x86_64 elfutils-libs.i686
elfutils-libs.x86_64 expect.x86_64 gettext.x86_64
gettext-libs.x86_64 glibc.i686 glibc.x86_64 gtk2.i686 gtk2.x86_64
gtk2-engines.i686 gtk2-engines.x86_64
ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686 libgcc.x86_64
libstdc++*i686 libstdc++*x86_64
libstdc++.i686 libXft.i686 libXft.x86_64 libXmu.i686 libXmu.x86_64
libXp.i686 libXpm.i686 libXpm.x86_64
libXpm-devel.i686 li Xpm-devel.x86_64 libXtst.i686 libXtst.x86_64
nfs-utils.x86_64 nfs-utils-lib.x86_64
nss-softokn-freebl.i686 nss-softokn-freebl.x86_64 ntp.x86_64
openmotif22.i686 openmotif22.x86_64
openssh-clients. 86_64 pam.i686 pam_passwdqc.x86_64 pam-devel.i686
redhat-lsb.x86_64 rpm-build.x86_64
tcsh.x86_64 unzip.x86_64 xorg-x11-xauth.x86_64  zip.x86_64zlib.i686
zlib.x86_64

yum -y update
```

On the process server:

```
yum install bc.x86_64 compat-db.i686 compat-db.x86_64
compat-glibc.x86_64 compat-glibc-headers.x86_64
compat-libstdc++*i686 compat-libstdc++*x86_64 dos2unix.x86_64
elfutils.x86_64 elfutils-libs.i686
elfutils-libs.x86_64 expect.x86_64 gettext.x86_64 glibc.i686 glibc.x86_64
gtk2.i686 gtk2.x86_64 gtk2-engines.i686
gtk2-engines.x86_64 ksh.x86_64 libaio.i686 libaio.x86_64 libgcc.i686
libgcc.x86_64 libstdc++*i686
libstdc++*x86_64 libXmu.i686 libXmu.x86_64 libXp.i686 libXpm.x86_64
libXtst.i686 libXtst.x86_64
nfs-utils.x86_64 nfs-utils-lib.x86_64 nss-softokn-freebl.i686
nss-softokn-freebl.x86_64 ntp.x86_64
openmotif22.i686 openmotif22.x86_64  openssh-clients.x86_64
pam_passwdqc.x86_64 rpm-build.x86_64
tcsh.x86_64 unzip.x86_64 zip.x86_64 zlib.i686 zlib.x86_64


yum -y update
```

2. Optional: Install the Linux packages for the X Window System on the application server. These packages are required if the password management tool will be used.
   a. Install the packages for the GNOME or KDE desktop.

      To install the GNOME desktop run:

      ```
      yum -y groupinstall "X Window System" Desktop
      ```

      To install the KDE desktop run:

      ```
      yum -y groupinstall "X Window System" "KDE Desktop"
      ```

   b. Run `yum -y update`
   c. Start the desktop by running `init 5`. To make the GUI desktop the default desktop, do the following.
      1) Edit the `/etc/inittab` file.
      2) Change the `initdefault` property from `3` to `5`. The updated line should be as follows.

         ```
         id:5:initdefault:
         ```

      3) Save the changes.
      4) Restart the server.

3. Optional: If IBM Defense Operations Platform is to be used in Chinese or French, run the appropriate command.

Language	Command
Chinese	`yum install -y "@Chinese Support"`
French	`yum install -y "@French Support"`

Related information:

http://www.redhat.com/

Setting other pre-installation requirements

Before installing IBM Defense Operations Platform, additional server setup is required.

Procedure

1. Ensure that all servers have the same time and date set as indicated by the Linux operating system. A time synchronization service can be used.
2. Make sure no version of IBM Java is installed on any of the servers.
3. Set **`UMASK`** to `022`.

Additional server preparation for the Command Center Edition

Before installing IBM Defense Operations Platform Command Center Edition, additional server setup is required.

Procedure

1. Ensure that your network is running IPV4. High availability server clustering does not support IPV6.
2. Ensure that the following is configured correctly so Tivoli® System Automation clustering technology can be successfully installed.
   a. Ensure hostnames are specified correctly.
   b. Ensure values contained in the `TSA.*` configuration properties in the topology properties file are correctly configured. For example, make sure the NIC specified in the `TSA.PRIMARY.USERNIC` property exists and is active during installation.
   c. Ensure the DB2® High-Availability Disaster Recovery (HADR) ports are available. These ports are used to replicate information from the primary databases to the standby databases. By default these ports are in the 55000 range.
3. On messaging server 1 and messaging server 2, ensure the `rpcidmapd`, `nfs` and `rpcbind` services are set to start automatically and that the services are started. The command to change the startup information for a specified service is **`chkconfig`** *service_name* **`on`**, where *service_name* is the name of the service. The command to start a specified service is **`/etc/init.d/`***service_name* **`start`**, where *service_name* is the name of the service.
4. A virtual IP address must be defined to allow load balance web requests across multiple reverse proxy servers. The load balancer distributes workload across reverse proxy servers on policy enforcement server 1 and policy enforcement server 2. The virtual IP address must be mapped to a fully-qualified virtual host name. The virtual host name is a combination of the `PORTAL.VIRTUAL.URL` and `WAS.LTPA.DOMAIN` properties defined in the topology properties file. The default host name is `virtualportal.platform.ibm.com`.

   If only one reverse proxy server is used, either policy enforcement server 1 or policy enforcement server 2, the virtual host name defined by the combination of the `PORTAL.VIRTUAL.URL` and `WAS.LTPA.DOMAIN` properties must be mapped, using a DNS alias or `hosts` file, to one of the reverse proxy servers.

Related tasks:

"Setting up TCP/IP networking" on page 14
Before installing IBM Defense Operations Platform, TCP/IP networking needs to be set up on the servers.

Preparing the installation server

The installation server must be prepared before IBM Defense Operations Platform can be installed.

About this task

In the Field Edition the messaging server is used as the installation server. In the Command Center Edition messaging server 1 is used as the installation server

Procedure

1. Obtain the IBM Defense Operations Platform installation package by ordering the package of DVDs or by obtaining the images from Passport Advantage®.
2. On the installation server, create a directory named `/distributionMedia`, if the directory does not already exist. If you want to use a directory other than `/distributionMedia`, make note of the directory name. You will need to specify the different directory name during installation. In the following steps, `/distributionMedia` is used in the examples.
3. If using physical DVDs, copy the installation images to the installation server.
   a. Mount a DVD.
   b. Copy the DVD contents to the `/distributionMedia` directory, or the directory you created.
   c. Unmount the DVD.
   d. Repeat until the contents of all DVDs are copied to the directory on the installation server.
4. If using ISO images from Passport Advantage, copy the installation images to the installation server.
   a. Create a `/distributionMedia/iso` directory or an `/iso` subdirectory under the directory you created in step 2. The following instructions will use `/distributionMedia/iso` in the examples.
   b. Download or copy each ISO image from Passport Advantage to the `/iso` subdirectory.
   c. Create a directory to mount the ISO image. This can be done by running the following command: **`mkdir /mnt/dop16`**. The following instructions will use `/mnt/dop16` in the examples.
   d. Mount the ISO image by running the following command: **`mount -o loop /distributionMedia/iso/`***iso_filename* **`/mnt/dop16`** where *iso_filename* is the name of one of the ISO image files.
   e. Copy the ISO contents to `/distributionMedia` by running the following command: **`cp -r /mnt/dop16/* /distributionMedia`**.
   f. Repeat mounting and copying ISO contents until all ISO image files have been processed.
   g. Delete the `/distributionMedia/iso` directory unless you want to archive the original ISO images.
5. Unpack the installation package.
   a. Change to the `/installHome` directory, or the directory you created.
   b. Run the **`tar -zxvf dop.tar.gz`** command.

Topology properties files

The topology properties files defines the customer-customizable properties for the deployment of IBM Defense Operations Platform. This file must be edited to meet the needs of the customer's environment. Any properties in the provided topology properties file not documented should not be changed.

After modifying the topology properties file, save a copy to a secure location. The file contains security-sensitive information, such as user names and passwords for the system, in clear text. If an unauthorized person has access to this file, they will have full access to the system.

The topology properties file can be used after installation in the following ways:

- As a repository of password information if a password is forgotten.
- As a repository for passwords when they are changed in the system. The modified topology properties file can be used to update the passwords used by the platform control tool.
- As a backup of installation information if the system needs to be reinstalled. The topology properties file can be used without having to redefine all the installation parameters.

IBM Defense Operations Platform provides the following topology files:

File name	Purpose	Used in
`install_home/dop16/resource/custom.properties`	Defines the location of the installation media, working directories, and other properties. This file can be edited to meet the needs of the customer's environment.	Command Center Edition and Field Edition
`install_home/dop16/topology/dop.d2.properties`	Defines the customer-customizable properties for the deployment including host names and passwords. This file can be edited to meet the needs of the customer's environment.	Field Edition
`install_home/dop16/topology/dop.d1.properties`	Defines the customer-customizable properties for the deployment including host names and passwords. This file can be edited to meet the needs of the customer's environment.	Command Center Edition

Customizing the installation properties

The installation properties file provides definitions required by the installation scripts. These properties can be modified when using the command line installation options.

About this task

On the installation server, go to the directory where the IBM Defense Operations Platform installation package was copied. In these steps, this directory is referred to as *install_home*. The installation server is the messaging server. In the Command Center Edition, messaging server 1 is the installation server.

Procedure

Optional: Edit the `install_home/dop16/resource/custom.properties` file and change the following property values if desired. Any properties values in the file not listed in Table 10 should not be changed. For those installing IBM Defense Operations Platform for the first time, it is recommended that the default values be used.

Table 10. IBM Defense Operations Platform installation properties

Property	Description	Default value
`image.basedir.local`	The name of the directory on the installation server containing the IBM Defense Operations Platform installation files. This is the directory where the installation media files were copied before running the installation tool. This directory is referred to as *install_media* in other installation instructions.	`/distributionMedia`

Table 10. IBM Defense Operations Platform installation properties (continued)

Property	Description	Default value
`image.tempdir.local`	The directory on the installation server used to store temporary files during the installation.	`/tmp/dop/images`
`backup.local`	This directory is for internal use only.	`/tmp/dop/backup`
`Unix.image.basedir.remote`	The directory on the target servers where the packages to be installed on that server will be copied.	`/installMedia/dop/image`
`Unix.script.basedir.remote`	The directory on the target servers where the installation scripts to be run on that server will be copied.	`/installMedia/dop/script`
`connection.timeout`	Time (in milliseconds) to wait for a connection to the target servers before failing.	15000
`waiting.time`	Time (in milliseconds) to wait before retrying a failed connection	20000
`retry.count`	Number of times to retry a failed connection before failing the installation	12

If unchanged, the default values will be used.

Target server information for the Field Edition

The `SERVERS` section of the topology properties file defines properties for the target servers.

Table 11 shows the server property values that must be specified in the topology properties file for your environment.

Table 11. Target server properties

Property	Description
`DB.1.HOST`	The fully-qualified host name of the data server
`DB.1.ACCOUNT.PWD`	The password for the `root` user on the data server
`DB.1.SSH_PORT`	The port number for ssh access to the data server
`APP.1.HOST`	The fully-qualified host name of the application server
`APP.1.ACCOUNT.PWD`	The password for the `root` user on the application server
`APP.1.SSH_PORT`	The port number for ssh access to the application server
`MSG.1.HOST`	The fully-qualified host name of the messaging server
`MSG.1.ACCOUNT.PWD`	The password for the `root` user on the messaging server
`MSG.1.SSH_PORT`	The port number for ssh access to the messaging server

Important: Host name values must be fully-qualified host names entered in the case defined. For example, `DOP16App.DOP16.com` is not the same as `dop16app.dop16.com`.

An ssh port number can be set for each server. However, the configured port numbers will only be used by the platform control tool. Port 22 must be enabled for ssh access on each server. Port 22 is required for ssh access by IBM Defense Operations Platform during installation.

Target server information for the Command Center Edition

The `SERVERS` section of the topology properties file defines properties for the target servers.

Table 12 shows the server property values that must be specified in the topology properties file for your environment.

Table 12. Target server properties

Property	Description
DB.1.HOST	The fully-qualified host name of the data server 1
DB.1.ACCOUNT.PWD	The password for the root user on the data server 1
DB.1.SSH_PORT	The port number for ssh access to the data server 1
DB.2.HOST	The fully-qualified host name of the data server 2
DB.2.ACCOUNT.PWD	The password for the root user on the data server 2
DB.2.SSH_PORT	The port number for ssh access to the data server 2
APP.1.HOST	The fully-qualified host name of the application server 1
APP.1.ACCOUNT.PWD	The password for the root user on the application server 1
APP.1.SSH_PORT	The port number for ssh access to the application server 1
APP.2.HOST	The fully-qualified host name of the application server 2
APP.2.ACCOUNT.PWD	The password for the root user on the application server 2
APP.2.SSH_PORT	The port number for ssh access to the application server 2
MSG.1.HOST	The fully-qualified host name of the messaging server 1
MSG.1.ACCOUNT.PWD	The password for the root user on the messaging server 1
MSG.1.SSH_PORT	The port number for ssh access to the messaging server 1
MSG.2.HOST	The fully-qualified host name of the messaging server 2
MSG.2.ACCOUNT.PWD	The password for the root user on the messaging server 2
MSG.2.SSH_PORT	The port number for ssh access to the messaging server 2
WEB.1.HOST	The fully-qualified host name of the policy enforcement server 1
WEB.1.ACCOUNT.PWD	The password for the root user on the policy enforcement server 1
WEB.1.SSH_PORT	The port number for ssh access to the policy enforcement server 1
WEB.2.HOST	The fully-qualified host name of the policy enforcement server 2
WEB.2.ACCOUNT.PWD	The password for the root user on the policy enforcement server 2
WEB.2.SSH_PORT	The port number for ssh access to the policy enforcement server 2
MON.1.HOST	The fully-qualified host name of the monitoring server
MON.1.ACCOUNT.PWD	The password for the root user on the monitoring server
MON.1.SSH_PORT	The port number for ssh access to the monitoring server
PRO.1.HOST	The fully-qualified host name of the process server
PRO.1.ACCOUNT.PWD	The password for the root user on the process server
PRO.1.SSH_PORT	The port number for ssh access to the process server

Important: Host name values must be fully-qualified host names entered in the case defined. For example, DOP16App.DOP16.com is not the same as dop16app.dop16.com.

An ssh port number can be set for each server. However, the configured port numbers will only be used by the platform control tool. Port 22 must be enabled for ssh access on each server. Port 22 is required for ssh access by IBM Defense Operations Platform during installation.

Directory services information

The topology properties file defines values used to encrypt user passwords and other sensitive data within the directory.

Encryption is based on two values: LDAP.SEED and LDAP.SALT.

Values must be printable ASCII characters. Printable ASCII characters are characters with code point values from 33 to 126. A blank space cannot be used.

Table 13. Directory services properties

Property	Description
LDAP.SEED	A 12 to 1016 character string, consisting of printable ASCII characters, between code points 33 through 126. A cryptographically-strong string should be used. For example, a long string comprised of mixed-case letters, number and special characters without common words or phrases.
LDAP.SALT	A 12 character string, consisting of printable ASCII characters, between code points 33 and 126. **Important:** LDAP.SALT must be exactly 12 characters in length. A value of more or less characters will cause the installation to fail.

Record the LDAP.SEED and LDAP.SALT values outside of the system. The values will be needed if you need to export or replicate directory entries.

LDAP suffix

The LDAP suffix information used in IBM Defense Operations Platform is defined in the topology properties file.

Only the ou, o, and c LDAP parameters can be changed. The parameters must meet the requirements shown in Table 14.

Table 14. LDAP parameter syntax rules

Parameter	Rules
c	Must be exactly two characters in length containing only the following: • Lowercase letters (a-z) • Uppercase letters (A-Z)

Table 14. LDAP parameter syntax rules (continued)

Parameter	Rules
o	Must be 1-30 characters in length containing only the following: • Lowercase letters (a-z) • Uppercase letters (A-Z) • Numbers (0-9) • Dash (-) • Underscore (_)
ou	Must be 1-30 characters in length containing only the following: • Lowercase letters (a-z) • Uppercase letters (A-Z) • Numbers (0-9) • Dash (-) • Underscore (_)

The values of `ou`, `o`, and `c` must match when specified for the following properties:

- `LDAP.SUFFIX`
- `LDAP.BASE.ENTRY`
- `LDAP.USER.ENTRY`
- `LDAP.GROUP.ENTRY`
- `LDAP.PROXY.DN`

For example:

```
LDAP.SUFFIX ou=SWG,o=IBM,c=US
LDAP.BASE.ENTRY ou=SWG,o=IBM,c=US
LDAP.USER.ENTRY ou=USERS,ou=SWG,o=IBM,c=US
LDAP.GROUP.ENTRY ou=GROUPS,ou=SWG,o=IBM,c=US
LDAP.PROXY.DN ou=SWG,o=IBM,c=US
```

Lightweight Third-Party Authentication domain

IBM Defense Operations Platform uses a Lightweight Third-Party Authentication (LTPA) token to enable single sign-on across many services. The LTPA domain name must be specified in the topology properties file.

Specify the LTPA domain name for your environment in the `WAS.LTPA.DOMAIN` property. The appropriate value can be obtained by running the **`hostname -d`** command on application server in the Field Edition or on application server 1 in the Command Center Edition.

In the Field Edition the value should be the same on the following servers:

- application server
- messaging server

In the Command Center Edition the value should be the same on the following servers:

- application server 1
- application server 2
- messaging server 1
- messaging server 2

The LTPA domain name is the parent portion of the fully qualified hostname of the servers. For example, if the fully-qualified hostname is server.yourco.com then the LTPA domain is yourco.com.

Clustering properties

Properties configuring the clustering topology components must be defined before installing IBM Defense Operations Platform in the Command Center Edition.

Table 15. Clustering properties

Property	Description
TSA.NETWORK.SUBNET	The subnet mask for the network hosting the data servers. This is the subnet mask for the network interface cards (NIC) on both data servers.
TSA.PRIMARY.USENIC	The name of the network interface card (NIC) on data server 1. The NIC name can be found by running the **ifconfig** command on data server 1.
TSA.STANDBY.USENIC	The name of the network interface card (NIC) on data server 2. The NIC name can be found by running the **ifconfig** command on data server 2.
TSA.QUORUM.IP	An IP address for a highly available system that is not part of the IBM Defense Operations Platform environment. This IP address must be reachable from both IBM Defense Operations Platform data server 1 and data server 2. No software will be installed at this location. The only requirement is that the system be available during installation and at runtime.

Password information for the Field Edition

Passwords for various user IDs used in the IBM Defense Operations Platform solution are defined in the topology properties file. For security reasons the default passwords shipped with IBM Defense Operations Platform should be changed.

Passwords can only contain the following characters:

- Lowercase letters (a-z)
- Uppercase letters (A-Z)
- Numbers (0-9)
- Dash (-)
- Period (.)
- Underscore (_)
- Tilde (~)

Dash and period cannot be used as the first character in a password.

Unless otherwise noted, passwords must be 30 characters or less.

Table 16. Password properties

Property	Associated user name	Description
DB.1.ACCOUNT.PWD	root	Root password for the data server
APP.1.ACCOUNT.PWD	root	Root password for the application server
MSG.1.ACCOUNT.PWD	root	Root password for the messaging server
LDAP.DB.PWD	dsrdbm01	LDAP directory database

Table 16. Password properties (continued)

Property	Associated user name	Description
LDAP.ADMIN.DN.PWD	cn=root	LDAP administrator bind
LDAP.BIND.DN.PWD	cn=bind	LDAP bind
LDAP.REPLICA.BIND.DN.PWD	cn=master	LDAP replica bind
ISIM.KEYSTORE.PWD	none	Keystore password
ISIM.POSIX.LINUX.PWD	posixagent	POSIX Linux user
IHS.KEYSTORE.PWD	none	HTTP server keystore
WAS.ADMIN.ACCOUNT.PWD	waswebadmin	Application services administrator. This password must be the same as PORTAL.ADMIN.ACCOUNT.PWD.
WAS.LTPA.PWD	none	LTPA token
PORTAL.ADMIN.ACCOUNT.PWD	waswebadmin	Administrator for the WebSphere Application Server console for the WebSphere Portal server. This password must be the same as WAS.ADMIN.ACCOUNT.PWD.
PORTAL.ADMIN.UID.PWD	wpsadmin	Administrator for the WebSphere Portal server. This password must be the same as DOMINO.ST.ADMIN.PWD.
PORTAL.DB.USER.PWD	db2port1	WebSphere Portal database
DOMINO.USER.PWD	notes	Collaboration user
DOMINO.ORG.PWD	IBM	Collaboration organization
DOMINO.ADMIN.PWD	notes admin	Collaboration administrator
DOMINO.ST.ADMIN.PWD	wpsadmin	Collaboration portal administrator. This password must be the same as PORTAL.ADMIN.UID.PWD.
DOMINO.ST.BIND.PWD	wpsbind	Collaboration LDAP bind
DEFAULT.PWD.DAS	dausr1	Database services administrative server
DEFAULT.PWD.DB2	db2inst1, db2inst2	Database services data server
DEFAULT.PWD.IHS	ihsadmin	HTTP server
DEFAULT.PWD.MQM	mqm	Messaging services user
MQM.CONN.USER.PWD	mqmconn	Messaging services connection
IOP.ADMIN.USER.PWD	ibmadmin	System administration tools This user is granted privileges equivalent to the root user on the target servers. The platform control tool runs under this user name. Because of the access afforded this user, make sure this password is a long value, is different from other passwords, and is kept secure.
IOP.USER.USER.PWD	ibmuser	System general user

Password information for the Command Center Edition

Passwords for various user IDs used in the IBM Defense Operations Platform solution are defined in the topology properties file. For security reasons the default passwords shipped with IBM Defense Operations Platform should be changed.

Passwords can only contain the following characters:

- Lowercase letters (a-z)
- Uppercase letters (A-Z)
- Numbers (0-9)
- Dash (-)
- Period (.)
- Underscore (_)
- Tilde (~)

Dash and period cannot be used as the first character in a password.

Unless otherwise noted, passwords must be 30 characters or less.

Table 17. Password properties

Property	Associated user name	Description
`WEB.1.ACCOUNT.PWD`	root	Root password for the policy enforcement server 1
`WEB.2.ACCOUNT.PWD`	root	Root password for the policy enforcement server 2
`DB.1.ACCOUNT.PWD`	root	Root password for the data server 1
`DB.2.ACCOUNT.PWD`	root	Root password for the data server 2
`APP.1.ACCOUNT.PWD`	root	Root password for the application server 1
`APP.2.ACCOUNT.PWD`	root	Root password for the application server 2
`MSG.1.ACCOUNT.PWD`	root	Root password for the messaging server 1
`MSG.2.ACCOUNT.PWD`	root	Root password for the messaging server 2
`MON.1.ACCOUNT.PWD`	root	Root password for the monitoring server
`PRO.1.ACCOUNT.PWD`	root	Root password for the process server
`LDAP.DB.PWD`	dsrdbm01	LDAP directory database
`LDAP.ADMIN.DN.PWD`	cn=root	LDAP administrator bind
`LDAP.BIND.DN.PWD`	cn=bind	LDAP bind
`LDAP.PROXY.INSTANCE.PWD`	tdsproxy	LDAP proxy instance
`LDAP.PROXY.ADMIN.DN.PWD`	cn=root	LDAP proxy administrator bind
`LDAP.PROXY.BIND.DN.PWD`	cn=bind	LDAP proxy bind
`LDAP.REPLICA.BIND.DN.PWD`	cn=master	LDAP replica bind
`ISIM.KEYSTORE.PWD`	none	Keystore password
`ISIM.POSIX.LINUX.PWD`	posixagent	POSIX Linux user
`IHS.KEYSTORE.PWD`	none	HTTP server keystore

Table 17. Password properties (continued)

Property	Associated user name	Description
WAS.ADMIN.ACCOUNT.PWD	waswebadmin	Application services administrator The WAS.ADMIN.ACCOUNT.PWD value must be the same as the PORTAL.ADMIN.ACCOUNT.PWD value.
WAS.LTPA.PWD	none	LTPA token
PORTAL.ADMIN.ACCOUNT.PWD	waswebadmin	Administrator for the WebSphere Application Server console for the WebSphere Portal server The PORTAL.ADMIN.ACCOUNT.PWD value must be the same as the WAS.ADMIN.ACCOUNT.PWD value.
PORTAL.ADMIN.UID.PWD	wpsadmin	Administrator for the WebSphere Portal server The PORTAL.ADMIN.UID.PWD value must be the same as the DOMINO.ST.ADMIN.PWD value.
PORTAL.DB.USER.PWD	db2port1	WebSphere Portal database
DOMINO.USER.PWD	notes	Collaboration user
DOMINO.ORG.PWD	IBM	Collaboration organization
DOMINO.ADMIN.PWD	notes admin	Collaboration administrator
DOMINO.ST.ADMIN.PWD	wpsadmin	Collaboration portal administrator The DOMINO.ST.ADMIN.PWD value must be the same as the PORTAL.ADMIN.UID.PWD value.
DOMINO.ST.BIND.PWD	wpsbind	Collaboration LDAP bind
DEFAULT.PWD.DAS	dausr1	Database services administrative server
DEFAULT.PWD.DB2	db2inst1, db2inst2	Database services data server
DEFAULT.PWD.IHS	ihsadmin	HTTP server
DEFAULT.PWD.MQM	mqm	Messaging services user
MQM.CONN.USER.PWD	mqmconn	Messaging services connection
IOP.ADMIN.USER.PWD	ibmadmin	System administration tools This user is granted privileges equivalent to the root user on the target servers. The platform control tool runs under this user name. Because of the access afforded this user, make sure this password is a long value, is different from other passwords, and is kept secure.
IOP.USER.USER.PWD	ibmuser	System general user
TAM.SECMASTER.PWD	sec_master	IBM Security Access Manager administrator
DEFAULT.PWD.TAI	taiuser	Trust association user

Table 17. Password properties (continued)

Property	Associated user name	Description
ODM.DB.USER.PWD	db2wodm	IBM Operational Decision Manager database
ODM.ADMIN.UID.PWD	resAdmin1	IBM Operational Decision Manager administrator
ODM.DEPLOYER.UID.PWD	resDeployer1	IBM Operational Decision Manager deployer
ODM.MONITOR.UID.PWD	resMonitor1	IBM Operational Decision Manager monitor
ODM.DB.DC.USER.PWD	wodmdc	IBM Operational Decision Manager database
ODM.rtsAdmin.UID.PWD	rtsAdmin	IBM Operational Decision Manager administrator
ODM.rtsConfig.UID.PWD	rtsConfig	IBM Operational Decision Manager configuration administrator
ODM.rtsUser.UID.PWD	rtsUser	IBM Operational Decision Manager user
OMNIBUS.OWNER.ACCOUNT.PWD	netcool	Tivoli Netcool/OMNIbus owner
OMNIBUS.ADMIN.ACCOUNT.PWD	tipadmin	Tivoli Netcool/OMNIbus administrator
BPM.DB.USER.PWD	db2bpm	IBM Business Process Manager database
WSRR.DB.USER.PWD	db2wsrr	WebSphere Service Registry and Repository database
TEPS.DB.USER.PWD	itmuser	Tivoli Monitoring database
ITM.ADMIN.PWD	sysadmin	Tivoli Monitoring administrator Password must be 5 to 15 characters in length.

Cyber hygiene properties

The topology properties file defines properties for cyber hygiene processing.

Table 18 shows the values that must be specified in the topology properties file for your environment if cyber hygiene is run.

Table 18. Cyber hygiene properties

Property	Description
IOP.CH.DISABLEROOTLOGIN	If cyber hygiene is run, this property determines if the `root` user is permitted to log on to the target servers. **Y** specifies that root log on is disabled **N** specifies that root log on is enabled
IOP.CH.GRUB.PWD	This property specifies the GRUB (GRand Unified Bootloader) password that cyber hygiene will apply to all servers.

Running the Field Edition command line installer

IBM Defense Operations Platform is installed using a script that prepares and checks the servers and installs IBM Defense Operations Platform Field Edition.

Procedure

1. Log on to the installation server as the `root` user.

   For the Field Edition, the installation server is the messaging server.
2. Change to the `/`*`install_home`*`/dop16/bin` directory.
3. Run the **`. ./dop-env.sh`** command.
4. Run the **`./dop.d2.install.sh -p`** *installation_password* command. The *installation_password* is used to provide security to the topology defined for IBM Defense Operations Platform. The password is required to make changes to the IBM Defense Operations Platform installation and is the initial password for the IBM Defense Operations Platform tools.

   Passwords can only contain the following characters:
   - Lowercase letters (a-z)
   - Uppercase letters (A-Z)
   - Numbers (0-9)
   - Dash (-)
   - Period (.)
   - Underscore (_)
   - Tilde (~)

   Dash and period cannot be used as the first character in a password.

   If a *installation_password* is not specified during the step to create the topology keystore, the *installation_password* will be set to `ibmdop16`. A menu of install steps is displayed.
5. A license agreement is presented. Accepting the license is required before the installation can proceed.
6. Select an option from the menu.

Table 19. Installation options

Selection	Installation Phase	Step Description	Average run time
1	Precheck	Validate installation media checksums	15 minutes
2	Prepare	Copy templates to the topology directory	2 minutes
3	Prepare	Create topology keystore	1 minute
4	Prepare	Parameterize all topologies	2 minutes
5	Prepare	(Optional) Encrypt all topologies	1 minute
6	Prepare	Run "Setup/Target" topology	5 minutes
7	Prepare	Run environmental prerequisite checks	15 minutes
8	Install	(Optional) Upload media to target servers If the media is not uploaded using this step it will be uploaded in the next step. By uploading the media as a separate step, a checkpoint can be taken after uploading the media.	30 minutes
9	Install	Run base product installation topology	2 hours
10	Install	Run product configuration topology	3 hours 30 minutes
11	Install	Install Identity Manager component	1 hour 15 minutes
12	Install	(Optional) Install Data Studio tool	15 minutes

Table 19. Installation options (continued)

Selection	Installation Phase	Step Description	Average run time
13	Install	Install platform control tool	15 minutes
14	Install	Install system verification check tool tool	1 hour 15 minutes
15	Install	(Optional) Install and run the cyber hygiene tool once to completion. Before running the cyber hygiene tool, it is recommended that a checkpoint be taken of the system. Cyber hygiene requires property settings in the topology properties file. Make sure the appropriate settings are defined before running the tool.	15 minutes to 30 minutes

7. Continue from step 4 on page 39 selecting installation steps in order. Do not select the next step until the previous installation step has completed. Do not restart any servers until all steps have completed successfully. The installation step can also be specified on the command. For example: **`./dop.d2.install.sh 1 -p`** *installation_password*.

Results

Installation progress is displayed and written to logs located in the `/`*`install_home`*`/dop16/log` directory on the installation server.

Cyber hygiene tool progress on the installation server is displayed on the console and is written to the `/tmp/dop.16.cyber-hygiene.log` file. When complete on the installation server, cyber hygiene may still be running on the other IBM Defense Operations Platform servers. To determine the progress of the cyber hygiene tool, run the **`ps -ef | grep hygiene`** command. When complete, cyber hygiene log files will be stored on the other IBM Defense Operations Platform servers in the `/var/cyber-hygiene/results/` directory. There will be three `.log` files in each directory. For information on how to interpret the logs, see the `/opt/IBM/iop/tools/ch/scripts-to-remotely-run-ch_DOP-1.6.doc` file on the installation server which will be available after cyber hygiene is run.

What to do next

If you need to rerun the cyber hygiene step (option 15), do the following before rerunning the step:

1. On the installation server, edit the `/install_home/dop16/topology/dop.d2.cyberhygiene.xml` file.
2. Change the instance of `Ready` or `Uncertain` half-way down the file in the line containing `type="runTool"` and `id="run_ch_i1"` to `New`.
3. Run **`./dop.d2.install.sh 15 -p`** *installation_password* where *installation_password* is the topology password.

If the `xml` file is not edited before the cyber hygiene step is rerun, the cyber hygiene step will report successful completion after about 10 seconds, but will do nothing.

Running the Command Center Edition command line installer

IBM Defense Operations Platform is installed using a script that prepares and checks the servers and installs IBM Defense Operations Platform Command Center Edition.

Procedure

1. Log on to the installation server as the `root` user.

   For the Command Center Edition, the installation server is messaging server 1.
2. Change to the `/`*`install_home`*`/dop16/bin` directory.

3. Run the **. ./dop-env.sh** command.
4. Run the **./dop.d1.install.sh -p** *installation_password* command. The *installation_password* is used to provide security to the topology defined for IBM Defense Operations Platform. The password is required to make changes to the IBM Defense Operations Platform installation and is the initial password for the IBM Defense Operations Platform tools.

   Passwords can only contain the following characters:

   - Lowercase letters (a-z)
   - Uppercase letters (A-Z)
   - Numbers (0-9)
   - Dash (-)
   - Period (.)
   - Underscore (_)
   - Tilde (~)

   Dash and period cannot be used as the first character in a password.

   If a *installation_password* is not specified during the step to create the topology keystore, the *installation_password* will be set to `ibmdop16`. A menu of install steps is displayed.
5. A license agreement is presented. Accepting the license is required before the installation can proceed.
6. Select an option from the menu.

Table 20. Installation options

Selection	Installation Phase	Step Description	Average run time
1	Precheck	Validate installation media checksums	15 minutes
2	Prepare	Copy templates to the topology directory	2 minutes
3	Prepare	Create topology keystore	1 minute
4	Prepare	Parameterize all topologies	2 minutes
5	Prepare	Encrypt all topologies	1 minutes
6	Prepare	Run "Setup/Target" topology	5 minutes
7	Prepare	Run environmental prerequisite checks	15 minutes
8	Install	(Optional) Upload media to target servers If the media is not uploaded using this step it will be uploaded in the next step. By uploading the media as a separate step, a checkpoint can be taken after uploading the media.	1 hour
9	Install	Run base product installation topology	3 hours 45 minutes
10	Install	Run configure products topology	8 hours 15 minutes
11	Install	Install Identity Management component	1 hour 15 minutes
12	Install	Prepare and configure System Automation Cluster Management	15 minutes
13	Install	(Optional) Install Data Studio tool	15 minutes
14	Install	Install platform control tool	15 minutes
15	Install	Install system verification check tool tool	1 hour 30 minutes

Table 20. Installation options (continued)

Selection	Installation Phase	Step Description	Average run time
16	Install	(Optional) Install and run the cyber hygiene tool once to completion. Before running the cyber hygiene tool, it is recommended that a checkpoint be taken of the system. Cyber hygiene requires property settings in the topology properties file. Make sure the appropriate settings are defined before running the tool.	15 minutes to 30 minutes

7. Continue from step 4 on page 41 selecting installation steps in order. Do not select the next step until the previous installation step has completed. Do not restart any servers until all steps have completed successfully. The installation step can also be specified on the command. For example: **`./dop.d1.install.sh 1 -p`** *installation_password*.

Results

Installation progress is displayed and written to logs located in the `/`*`install_home`*`/dop16/log` directory on the installation server.

Cyber hygiene tool progress on the installation server is displayed on the console and is written to the `/tmp/dop.16.cyber-hygiene.log` file. When complete on the installation server, cyber hygiene may still be running on the other IBM Defense Operations Platform servers. To determine the progress of the cyber hygiene tool, run the **`ps -ef | grep hygiene`** command. When complete, cyber hygiene log files will be stored on the other IBM Defense Operations Platform servers in the `/var/cyber-hygiene/results/` directory. There will be three `.log` files in each directory. For information on how to interpret the logs, see the `/opt/IBM/iop/tools/ch/scripts-to-remotely-run-ch_DOP-1.6.doc` file on the installation server which will be available after cyber hygiene is run.

What to do next

If you need to rerun the cyber hygiene step (option 16), do the following before rerunning the step:

1. On the installation server, edit the `/install_home/dop16/topology/dop.d1.cyberhygiene.xml` file.
2. Change the instance of `Ready` or `Uncertain` half-way down the file in the line containing `type="runTool"` and `id="run_ch_i1"` to `New`.
3. Run **`./dop.d1.install.sh 15 -p`** *installation_password* where *installation_password* is the topology password.

If the `xml` file is not edited before the cyber hygiene step is rerun, the cyber hygiene step will report successful completion after about 10 seconds, but will do nothing.

Verifying the installation prior to post-installation configuration

After running the installer, verify that IBM Defense Operations Platform has been correctly installed before starting the post-installation configuration steps.

Procedure

1. Use the platform control tool to stop all components.
2. Check that all components have stopped successfully by reviewing the displayed messages.
3. Shut down the Linux operating system on all servers.
4. Power-down and power-up all runtime servers or reboot all servers.
5. Use the platform control tool to start all components.

6. Use the platform control tool to query the status of all components.
7. Run all the tests in the system verification check tool.
8. Check that all tests have run successfully.

What to do next

If any errors are noted, resolve the errors and rerun these steps.

Related tasks:

"Using the system verification check tool" on page 64
The system verification check tool is used to determine the operational status of services comprising the IBM Defense Operations Platform system.

"Querying the status of the components in the Field Edition" on page 55
The platform control tool can be used to determine the status of the components running in the IBM Defense Operations Platform Field Edition.

"Querying the status of the components in the Command Center Edition" on page 60
The platform control tool can be used to determine the status of the components running in the IBM Defense Operations Platform Command Center Edition.

"Starting the components in the Field Edition" on page 53
The platform control tool can be used to start the components running in the IBM Defense Operations Platform Field Edition.

"Starting the components in the Command Center Edition" on page 57
The platform control tool can be used to start the components running in the IBM Defense Operations Platform Command Center Edition.

"Stopping the components in the Field Edition" on page 54
The platform control tool can be used to stop components running in the IBM Defense Operations Platform Field Edition.

"Stopping the components in the Command Center Edition" on page 59
The platform control tool can be used to stop components running in the IBM Defense Operations Platform Command Center Edition.

Post-installation IBM Defense Operations Platform configuration

After installing IBM Defense Operations Platform, several post-installation configuration steps need to be done to complete the installation.

Configuring collaboration services for IPv6

If your installation uses IPv6 networking, configuration steps are required for collaboration services.

About this task

The IBM Defense Operations Platform architecture needs to be installed before configuring IPv6 networking for collaboration services.

Procedure

1. Follow the steps in the Lotus® Domino® documentation to configure Lotus Domino for IPv6 addressing.
2. Follow the steps in the Lotus Sametime® Standard documentation to configure Lotus Sametime Standard for IPv6 addressing.
3. Follow the steps in the WebSphere Portal documentation to configure trust for the Sametime Contact List portlet if you are not using an IPv4 network with an IPv4 address assigned to the application server.

Related information:

➪ Configuring Lotus Domino for IPv6 addressing

➪ Configuring the Sametime Community Server to support IPv6

➪ Configuring trust for the Sametime Contact List portlet

Configuring single sign-on for collaboration services

Import the WebSphere Portal SSO LTPA token into the application server to allow users to access collaboration services without having to reenter their credentials.

Before you begin

To complete this task a Lotus Notes 8.5.x client is required. An existing Notes Client can be used or one can be installed on a Windows client using the `notes_designer_admin853_w32en.exe` file in the `/distributionMedia` folder on the installation server. The workstation must be able to connect to the application server over TCP/IP using the fully-qualified host name.

About this task

The IBM Defense Operations Platform architecture needs to be installed before importing the Lightweight Third-Party Authentication (LTPA) token.

This token was created during the installation of the IBM Defense Operations Platform architecture.

Procedure

1. Install a Lotus Notes 8.5.x client on a workstation. An existing installation can be used. The workstation must be able to connect to the application server over TCP/IP using the fully-qualified host name.
2. Copy the `/opt/IBM/ISP/stproxy.ltpa` file from the application server to the workstation running Lotus Notes. This is the LTPA token that will be imported into the collaboration service directory.
3. Copy the `/local/notesdata/admin.id` file from the application server to the workstation running Lotus Notes. This is the ID file for the collaboration service administrator. You will use this ID to login to the collaboration services directory.
4. On the workstation, start the Lotus Notes client and log on with the `admin.id` file.
   a. On the Lotus Notes log on panel, click **User Name**.
   b. Navigate to the directory where you copied that `admin.id` file and select it.
   c. Enter the password defined in the topology properties file for the `DOMINO.ADMIN.PWD` property.
   d. Click **Yes** if a security warning is displayed.
5. Open the `names.nsf` file.
   a. Click **File** > **Open** > **Lotus Notes Application**.
   b. Enter the fully-qualified host name of the application server in **Look In**.
   c. Enter `names.nsf` in **File Name**.
   d. Click **Open**.
6. Navigate to **Web** > **Web Configurations**.
7. Select `Web SSO Configuration for LTPA Token` and click **Edit Document**.
8. Click **Keys** > **Import WebSphere LTPA Keys**. Click **OK** if a warning is received about overwriting existing keys.
9. Enter the path to where the `stproxy.ltpa` file was copied. Click **OK**.
10. Enter the password for the LTPA token. The password is defined in the topology properties file `WAS.LTPA.PWD` property.

11. In **Token Format** select `LtpaToken2`.
12. Click **OK** > **Save and Close**.
13. In the Field Edition, restart the collaboration service using the platform control tool.
    a. Log on to the management server and open a terminal window.
    b. Run **`su -ibmadmin`**.
    c. Run **`DOPControl -a stop -c collab -p`** *password* where *password* is the password for the platform control tool defined when the platform control tool was installed.
    d. Run **`DOPControl -a start -c collab -p`** *password* where *password* is the password for the platform control tool defined when the platform control tool was installed.
14. In the Command Center Edition, restart the collaboration service using the platform control tool.
    a. Log on to the management server and open a terminal window.
    b. Run **`su -ibmadmin`**.
    c. Run **`DOPControl -a stop -c collabpri -p`** *password* where *password* is the password for the platform control tool defined when the platform control tool was installed.
    d. Run **`DOPControl -a start -c collabpri -p`** *password* where *password* is the password for the platform control tool defined when the platform control tool was installed.

Setting the session timeout

The session timeout determines the time a user can remain idle before the session is terminated and the user must log in again. The session time out includes administrators logged in through the portal service.

About this task

When IBM Defense Operations Platform is installed, no session time out is defined. Users will stay logged in until they log out even if the session is idle.

If your organization has security policies requiring that sessions log out after a period of inactivity, use the following steps to define a session timeout for your IBM Defense Operations Platform system.

Procedure

Configure server timeouts.

1. In the Field Edition, using a web browser go to `http://`*`application_server`*`:9062/ibm/console` where *application_server* is the host name of the application server.
2. In the Command Center Edition, using a web browser go to `http://`*`application_server`*`:9062/ibm/console` where *application_server* is the host name of application server 1.
3. Log on as the `admin` user with the password defined for `PORTAL.ADMIN.ACCOUNT.PWD` in the topology properties file.
4. Click **Servers** > **Server Type** > **WebSphere Application Servers** > **WebSphere Portal**.
5. Click **Container Settings** > **Session management** > **Set Timeout**.
6. Enter the desired timeout value in minutes.
7. Click **OK**.
8. Click **Save**.
9. Click **Servers** > **Server Type** > **WebSphere Application Servers** > **STProxyServer1**.
10. Click **Container Settings** > **Session management** > **Set Timeout**.
11. Enter the desired timeout value in minutes.
12. Click **OK**.
13. Click **Save**.

If running the Command Center Edition, configure the following additional servers.

14. Click **Servers** > **Server Type** > **WebSphere Application Servers** > **WebSphere_Portal_PortalNode2**.
15. Click **Container Settings** > **Session management** > **Set Timeout**.
16. Enter the desired timeout value in minutes.
17. Click **OK**.
18. Click **Save**.

Restart the server.

19. Stop and restart the application server in the Field Edition or application server 1 in the Command Center Edition using the platform control tool.

Configuring a secondary collaboration services LDAP server in the Command Center Edition

A secondary LDAP server is required for collaboration services when running the Command Center Edition.

Procedure

1. Install a Lotus Notes 8.5.x client on a workstation. An existing installation can be used. The workstation must be able to connect to the application server 1 over TCP/IP using the fully-qualified host name.
2. Copy the `/local/notesdata/admin.id` file from application server 1 to the workstation running Lotus Notes. This is the ID file for the collaboration service administrator. You will use this ID to login to the collaboration services directory.
3. On the workstation, start the Lotus Notes client and log on with the `admin.id` file.
   a. On the Lotus Notes log on panel, click **User Name**.
   b. Navigate to the directory where you copied the `admin.id` file and select it.
   c. Enter the password defined in the topology properties file for the `DOMINO.ADMIN.PWD` property.
   d. Click **Yes** if a security warning is displayed.
4. Open the `names.nsf` file.
   a. Click **File** > **Open** > **Lotus Notes Application**.
   b. Enter the fully-qualified host name of the application server 1 in **Look In**.
   c. Enter `names.nsf` in **File Name**.
   d. Click **Open**.
5. Open the `da.nsf` file.
   a. Click **File** > **Open** > **Lotus Notes Application**.
   b. Enter the fully-qualified host name of application server 1 in **Look In**.
   c. Enter `da.nsf` in **File Name**.
   d. Click **Open**.
6. Duplicate the existing directory assistance entry.
7. Update the duplicate directory assistance entry.
   a. On the **Basics** tab set **Group Authorization** to `No`.
   b. For **Search Order** specify `2`.
   c. On the **LDAP** tab change the **LDAP host** from your primary LDAP hostname to your secondary LDAP hostname.
8. Open the `stconfig.nsf` file.
   a. Click **File** > **Open** > **Lotus Notes Application**.
   b. Enter the fully-qualified host name of application server 1 in **Look In**.
   c. Enter `stconfig.nsf` in **File Name**.
   d. Click **Open**.

9. Click **By Form**.
10. Duplicate the `LDAPServer` form.
11. Update the duplicated form.
    a. For **LDAP Connection** specify the fully-qualified hostname of your secondary LDAP.
    b. For **Search Order** specify `2`.
12. Restart collaboration services.
    a. Log on to messaging server 1 or messaging server 2 as the `ibmadmin` user. If logged on as a different user, change to the `ibmadmin` user by running the **`su - ibmadmin`** command.
    a. Run the following commands:

```
DOPControl -a stop -c colsby -p password
DOPControl -a stop -c colpri -p password
DOPControl -a start -c colpri -p password
DOPControl -a start -c colsby -p password
```

    where *password* is the topology password defined when the IBM Defense Operations Platform was installed.

Configuring additional cluster manager relationships in the Command Center Edition

After installing IBM Defense Operations Platform Command Center Edition, cluster manager relationships need to be configured.

About this task

If this configuration is not done, an uncontrolled failure of the primary data server, or its network interface, will not switch the databases to the standby data server. When the failover fails, IBM Defense Operations Platform will become inoperable.

Procedure

1. Log on to messaging server 1.
2. Open a terminal window.
3. If not logged on as the `root` user, run the **`su - root`** command to change to the root user.
4. Run **`cd`** *install_home***`/dop16/bin`** where *install_home* is the directory where the installation files were copied when installing IBM Defense Operations Platform.
5. Run **`. ./dop-env.sh`**
6. Run **`./ba.sh installTopology -t dop.ha.tsapatch -p`** *installation_password* where *installation_password* is the installation password defined when IBM Defense Operations Platform was installed.

Configuring the optional external network file system in the Command Center Edition

The optional external network file system is configured using a script.

About this task

The external network file system is used to provide a more robust failover solution for messaging services.

Procedure

1. Log on to the installation server as the `root` user.
2. Change to the `/`*`install_home`*`/dop16/bin` directory.
3. Run the **`./dop-env.sh`** command.

4. Run the **./dop.ha.wmqextnfs.sh -p** *installation_password* command. The *installation_password* is the one specified when IBM Defense Operations Platform was installed or was subsequently modified. If not specified, *installation_password* will default to `ibmdop16`. A menu of install steps is displayed.
5. Select an option from the menu.

Table 21. External network file system configuration options

Selection	Phase	Step Description	Average run time
1	Prepare	Copy template to topology directory	1 minute
2	Prepare	Parameterize topology	1 minute
3	Prepare	Encrypt topology	1 minute
4	Install	Setup the external network file system	7 minutes

6. Continue from step 4 selecting installation steps in order. Do not select the next step until the previous installation step has completed. The installation step can also be specified on the command. For example: **./dop.d1.wmqextnfs.sh 1 -p** *installation_password*.

Results

Installation progress is displayed and written to logs located in the `/install_home/dop16/log` directory on the installation server.

Configuring the Tivoli Directory Server web administration tool host name

The host name for the data server needs to be configured in the Tivoli Directory Server Web Administration Tool before the tool can be used.

Procedure

1. Access the Tivoli Directory Server Web Administration Tool at: `http://APPLICATION_SERVER_HOST:9081/IDSWebApp` where *APPLICATION_SERVER_HOST* is the host name of the application server.
2. Log on as the `superadmin` user and click **Console administration** > **Manage console server**. Enter the fully-qualified DNS name for the data server in **Hostname** and click **OK**.

Enabling Tivoli Directory Server logging

Enable Tivoli Directory Server logging to help debug Tivoli Directory Server errors.

Procedure

1. Access the Tivoli Directory Server Web Administration Tool at: `http://APPLICATION_SERVER_HOST:9081/IDSWebApp` where *APPLICATION_SERVER_HOST* is the host name of the application server.
2. Click **Server Administration** > **Logs** > **Modify Log Settings** > **Select Server Audit Log**.
3. Click **Edit Settings**.
4. Change the following settings:
   - Under **Server audit log** select **Enable server audit logging**.
   - Under **Audit log level** select **All attempts**.
   - Under **Audit performance** select **Enable audit for performance data**.
   - Under **Operations to log** select all items.
5. Click **Finish**.

Removing installation files from the production system

While installing IBM Defense Operations Platform, the installation service configuration, installation media, and log files are written to the servers. After the installation completes and the installation has been verified, files that are only used in the installation process can be removed from the production system servers.

The following can be archived and removed from all servers:

- The directory defined by the `Unix.image.basedir.remote` property in the topology properties file. The default location is `/installMedia/dop/image`.
- The directory defined by the `Unix.script.basedir.remote` property in the topology properties file. The default location is `/installMedia/dop/script`.

The following can be archived and deleted from the installation server, which is the messaging server in the Field Edition and messaging server 1 in the Command Center Edition.

- The directory defined by the `image.basedir.local` property in the `custom.properties` file. The default location is `/distributionMedia`.
- The directory defined by the `image.tempdir.local` property in the `custom.properties` file. The default location is `/tmp/dop/images`.
- The directory defined by the `backup.local` property in the `custom.properties` file. The default location is `/tmp/dop/backup`.

Since the topology properties file on the installation server contains passwords in clear text, this file should be stored in a secure location.

The topologies property files are:

- Field Edition: *`install_home`*`/dop16/topology/dop.d2.properties`
- Command Center Edition: *`install_home`*`/dop16/topology/dop.d1.properties`

Verifying the installation

After installing IBM Defense Operations Platform Command Center Edition or Field Edition, verify that the product has been correctly installed. Verification ensures all components are started and operating as expected.

About this task

Two verification procedures are provided. The quick verification procedure can be used immediately after installing IBM Defense Operations Platform and any time a quick verification of the overall system is desired. The full verification procedure take significantly more time, but should be done before IBM Defense Operations Platform is considered fully-operational.

Procedure

Quick verification

1. Run all the tests in the system verification check tool.
2. Check that all tests have run successfully.
3. Use the platform control tool to start any components that need to be started.

Full verification

4. Use the platform control tool to stop all components.
5. Check that all components have stopped successfully by reviewing the displayed messages.
6. Shut down the Linux operating system on all servers.
7. Power-down and power-up all runtime servers or reboot all servers.

8. Use the platform control tool to start all components.
9. Use the platform control tool to query the status of all components.
10. Run all the tests in the system verification check tool.
11. Check that all tests have run successfully.

What to do next

If any errors are noted, resolve the errors and rerun these steps.

Related tasks:

"Using the system verification check tool" on page 64
The system verification check tool is used to determine the operational status of services comprising the IBM Defense Operations Platform system.

"Querying the status of the components in the Field Edition" on page 55
The platform control tool can be used to determine the status of the components running in the IBM Defense Operations Platform Field Edition.

"Querying the status of the components in the Command Center Edition" on page 60
The platform control tool can be used to determine the status of the components running in the IBM Defense Operations Platform Command Center Edition.

"Starting the components in the Field Edition" on page 53
The platform control tool can be used to start the components running in the IBM Defense Operations Platform Field Edition.

"Starting the components in the Command Center Edition" on page 57
The platform control tool can be used to start the components running in the IBM Defense Operations Platform Command Center Edition.

"Stopping the components in the Field Edition" on page 54
The platform control tool can be used to stop components running in the IBM Defense Operations Platform Field Edition.

"Stopping the components in the Command Center Edition" on page 59
The platform control tool can be used to stop components running in the IBM Defense Operations Platform Command Center Edition.

Installing IBM Defense Operations Platform Workbench Edition

IBM Defense Operations Platform Workbench Edition includes products that provide additional functionality to the IBM Defense Operations Platform.

IBM Defense Operations Platform Workbench Edition includes the following products:

- Rational Build Forge Enterprise Edition 7.1.3
- Lotus Expeditor 6.2.3
- Rational Requirements Composer 4.0
- Rational License Key Server 8.1.3
- IBM Java SDK/JRE 7.0.5
- IBM Forms Experience Builder 8.5
- IBM Integration Designer 8.5
- InfoSphere Data Architect 9.1
- Rational RequisitePro 7.1.4
- IBM Forms Server 8.0.1
- Rational Asset Manager Enterprise Edition 7.5.2
- Rational Quality Manager 4.0.4
- Rational Team Concert 4.0.4

- Rational Software Architect for WebSphere Software 8.5.5
- Rational Functional Tester 8.5
- Rational Service Tester for SOA Quality 8.5
- Rational Performance Tester 8.5 Security AppScan Standard 8.7

These products are installed using the installation instructions and installers provided by the products. IBM Defense Operations Platform does not provide specific installation instructions or methods to install these products in the IBM Defense Operations Platform environment.

The products included with the Workbench Edition are for use only with IBM Defense Operations Platform.

Chapter 3. Managing the solution

You can perform the following types of administrative tasks for IBM Defense Operations Platform.

Accessing IBM Defense Operations Platform administration consoles

The IBM Defense Operations Platform is comprised of a number of products. Each of these products has one or more administration consoles. To make it easier to find the installed administration consoles, IBM Defense Operations Platform provides pages where the consoles can be accessed.

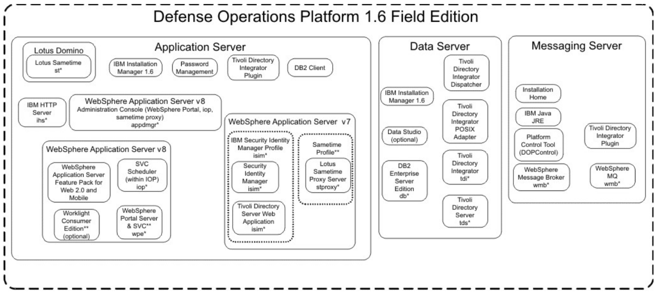
Procedure

- To access the administration consoles installed with the Field Edition, go to `https://`*`Application_Server`*`/dop/DOP16_D2_Admin_URLs.htm` where *Application_Server* is the host name of the application server. The host name of the application server can be found in the *`install_Home`*`/dop16/topology/dop.d2.properties` file in the `APP.1.HOST` property.
- To access the administration consoles installed with the Command Center Edition, go to `https://`*`Process_Server`*`/dop/DOP16_D1_Admin_URLs.htm` where *Process_Server* is the host name of the process server. The host name of the process server can be found in the *`install_Home`*`/dop16/topology/dop.d1.properties` file in the `PRO.1.HOST` property.

Starting, stopping, and querying status in the Field Edition

The platform control tool allows a user to stop, start, and query IBM Defense Operations Platform components running in the Field Edition. A platform control tool tool is also available for IBM Defense Operations Platform running in the Command Center Edition.

Figure 1 shows the products and components comprising IBM Defense Operations PlatformField Edition and their platform control tool components.


Defense Operations Platform 1.6 Field Edition
Application Server
Lotus Domino
Lotus Sametime st*
IBM Installation Manager 1.6
Password Management
Tivoli Directory Integrator Plugin
DB2 Client
IBM HTTP Server ihs*
WebSphere Application Server v8 Administration Console (WebSphere Portal, iop, sametime proxy) appdmgr*
WebSphere Application Server v8
WebSphere Application Server Feature Pack for Web 2.0 and Mobile
SVC Scheduler (within IOP) iop*
Worklight Consumer Edition** (optional)
WebSphere Portal Server & SVC** wpe*
WebSphere Application Server v7
IBM Security Identity Manager Profile isim*
Security Identity Manager isim*
Tivoli Directory Server Web Application isim*
Sametime Profile**
Lotus Sametime Proxy Server stproxy*
Data Server
IBM Installation Manager 1.6
Data Studio (optional)
DB2 Enterprise Server Edition db*
Tivoli Directory Integrator Dispatcher
Tivoli Directory Integrator POSIX Adapter
Tivoli Directory Integrator tdi*
Tivoli Directory Server tds*
Messaging Server
Installation Home
IBM Java JRE
Platform Control Tool (DOPControl)
WebSphere Message Broker wmb*
Tivoli Directory Integrator Plugin
WebSphere MQ wmb*

*DOPControl Component Name
** Managed by WebSphere Application Server v8 administration console

Figure 1. Field Edition components

Related concepts:

"Starting, stopping, managing and querying status in the Command Center Edition" on page 57
The platform control tool allows a user to stop, start, and query IBM Defense Operations Platform services running in the Command Center Edition. A platform control tool tool is also available for IBM Defense Operations Platform running in the Field Edition.

Starting the components in the Field Edition

The platform control tool can be used to start the components running in the IBM Defense Operations Platform Field Edition.

About this task

The `DOPControl` command must be run as the `ibmadmin` user. If not logged on as the `ibmadmin`, run the `su - ibmadmin` command to switch to the `ibmadmin` user.

Attention: Starting individual components should only be done by experienced IBM Defense Operations Platform administrators. Unpredictable results can occur if components are not started in the required order.

Procedure

On the messaging server run the following command to start all the IBM Defense Operations Platform components.

```
DOPControl -a start -c all -p password
```

where *password* is the topology password defined when the IBM Defense Operations Platform was installed. If the *password* value contains special characters, the *password* value must be enclosed in single quotation marks. For example: `'pass$phrase'`
The components are started in the required order. Prerequisite components are started before dependent components. For example, database and directory components are started first.

Attention: Starting all components can take 45 minutes or longer.
To start only one component, run the following command.

```
DOPControl -a start -c component -p password
```

where *component* is an ID listed under **Target Options** in the `DOPControl` help and where *password* is the topology password defined when the IBM Defense Operations Platform was installed. If the *password* value contains special characters, the *password* value must be enclosed in single quotation marks. For example: `'pass$phrase'`
Optionally the `nostatus` option can be added to the command. This will suppress any output returned from the command.

Results

The requested IBM Defense Operations Platform components are started.

What to do next

After running the `DOPControl` command, check the logs in the `/opt/IBM/ISP/mgmt/logs` directory. The logs contain the results of the most recent `DOPControl` command.

Related tasks:

"Stopping the components in the Field Edition"
The platform control tool can be used to stop components running in the IBM Defense Operations Platform Field Edition.

"Querying the status of the components in the Field Edition" on page 55
The platform control tool can be used to determine the status of the components running in the IBM Defense Operations Platform Field Edition.

"Getting help for the platform control tool in the Field Edition" on page 56
Information is available about the options for running the platform control tool in the Field Edition.

Stopping the components in the Field Edition

The platform control tool can be used to stop components running in the IBM Defense Operations Platform Field Edition.

About this task

The DOPControl command must be run as the ibmadmin user. If not logged on as the ibmadmin, run the su - ibmadmin command to switch to the ibmadmin user.

Attention: Stopping individual components should only be done by experienced IBM Defense Operations Platform administrators. Unpredictable results can occur if components are not stopped in the required order.

Procedure

On the messaging server run the following command to stop all the IBM Defense Operations Platform components.

```
DOPControl -a stop -c all -p password
```

where *password* is the topology password defined when the IBM Defense Operations Platform was installed. If the *password* value contains special characters, the *password* value must be enclosed in single quotation marks. For example: 'pass$phrase'

Attention: Stopping all components can take 45 minutes or longer.
To stop only one component, run the following command.

```
DOPControl -a stop -c component -p password
```

where *component* is an ID listed under **Target Options** in the DOPControl help and where *password* is the topology password defined when the IBM Defense Operations Platform was installed. If the *password* value contains special characters, the *password* value must be enclosed in single quotation marks. For example: 'pass$phrase'
Optionally the nostatus option can be added to the command. This will suppress any output returned from the command.

Results

The requested IBM Defense Operations Platform components are stopped.

What to do next

After running the DOPControl command, check the logs in the /opt/IBM/ISP/mgmt/logs directory. The logs contain the results of the most recent DOPControl command.

Related tasks:

"Starting the components in the Field Edition" on page 53
The platform control tool can be used to start the components running in the IBM Defense Operations Platform Field Edition.

"Querying the status of the components in the Field Edition"
The platform control tool can be used to determine the status of the components running in the IBM Defense Operations Platform Field Edition.

"Getting help for the platform control tool in the Field Edition" on page 56
Information is available about the options for running the platform control tool in the Field Edition.

Querying the status of the components in the Field Edition

The platform control tool can be used to determine the status of the components running in the IBM Defense Operations Platform Field Edition.

About this task

The DOPControl command must be run as the ibmadmin user. If not logged on as the ibmadmin, run the su - ibmadmin command to switch to the ibmadmin user.

Procedure

On the messaging server run the following command to query the status all the IBM Defense Operations Platform components.

```
DOPControl -a status -c all -p  password
```

where *password* is the topology password defined when the IBM Defense Operations Platform was installed. If the *password* value contains special characters, the *password* value must be enclosed in single quotation marks. For example: 'pass$phrase'
To check only one component, run the following command.

```
DOPControl -a status -c component -p password
```

where *component* is an ID listed under **Target Options** in the DOPControl help and where *password* is the topology password defined when the IBM Defense Operations Platform was installed. If the *password* value contains special characters, the *password* value must be enclosed in single quotation marks. For example: 'pass$phrase'

Results

Components that are started will display **[on]**. Components that are not started will display **[off]**.

What to do next

After running the DOPControl command, check the logs in the /opt/IBM/ISP/mgmt/logs directory. The logs contain the results of the most recent DOPControl command.

Related tasks:

"Starting the components in the Field Edition" on page 53
The platform control tool can be used to start the components running in the IBM Defense Operations Platform Field Edition.

"Stopping the components in the Field Edition" on page 54
The platform control tool can be used to stop components running in the IBM Defense Operations Platform Field Edition.

"Getting help for the platform control tool in the Field Edition"
Information is available about the options for running the platform control tool in the Field Edition.

Getting help for the platform control tool in the Field Edition

Information is available about the options for running the platform control tool in the Field Edition.

About this task

The DOPControl command must be run as the ibmadmin user. If not logged on as the ibmadmin, run the su - ibmadmin command to switch to the ibmadmin user.

Procedure

On the messaging server run the one of the following commands to see options for the DOPControl command.

```
DOPControl -a help
or DOPControl -h
```

The command can also be run without the path. For example, `DOPControl -h`.

Results

The options for the `DOPControl` command are displayed.

Related tasks:

"Starting the components in the Field Edition" on page 53
The platform control tool can be used to start the components running in the IBM Defense Operations Platform Field Edition.

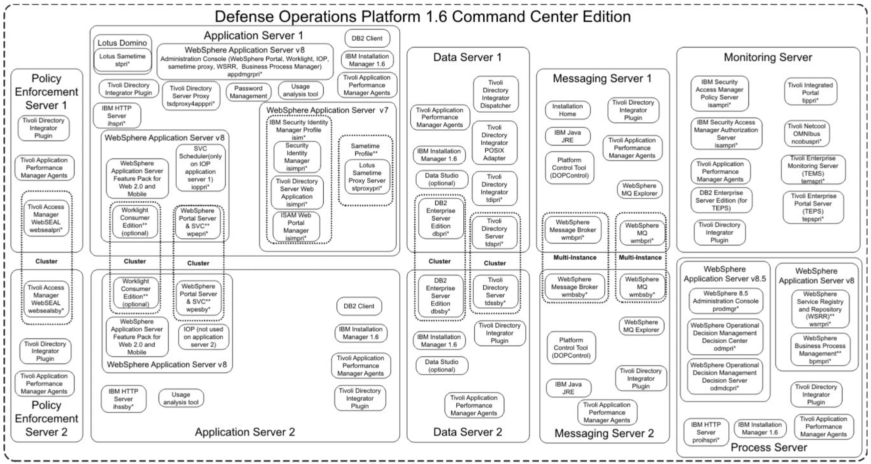
"Stopping the components in the Field Edition" on page 54
The platform control tool can be used to stop components running in the IBM Defense Operations Platform Field Edition.

"Querying the status of the components in the Field Edition" on page 55
The platform control tool can be used to determine the status of the components running in the IBM Defense Operations Platform Field Edition.

Starting, stopping, managing and querying status in the Command Center Edition

The platform control tool allows a user to stop, start, and query IBM Defense Operations Platform services running in the Command Center Edition. A platform control tool tool is also available for IBM Defense Operations Platform running in the Field Edition.

Figure 2 shows the products and components comprising IBM Defense Operations PlatformCommand Center Edition and their platform control tool components.


Defense Operations Platform 1.6 Command Center Edition
Policy Enforcement Server 1
Tivoli Directory Integrator Plugin
Tivoli Application Performance Manager Agents
Tivoli Access Manager WebSEAL websealpri*
Cluster
Tivoli Access Manager WebSEAL websealsby*
Tivoli Directory Integrator Plugin
Tivoli Application Performance Manager Agents
Policy Enforcement Server 2
Application Server 1
Lotus Domino
Lotus Sametime stpri*
WebSphere Application Server v8
Administration Console (WebSphere Portal, Worklight, IOP, sametime proxy, WSRR, Business Process Manager) appdmgrpri*
DB2 Client
IBM Installation Manager 1.6
Tivoli Application Performance Manager Agents
Tivoli Directory Integrator Plugin
Tivoli Directory Server Proxy tsdproxy4apppri*
Password Management
Usage analysis tool
IBM HTTP Server ihspri*
WebSphere Application Server v8
WebSphere Application Server Feature Pack for Web 2.0 and Mobile
SVC Scheduler(only on IOP application server 1) ioppri*
Worklight Consumer Edition** (optional)
WebSphere Portal Server & SVC** wpepri*
WebSphere Application Server v7
IBM Security Identity Manager Profile isim*
Security Identity Manager isimpri*
Tivoli Directory Server Web Application isimpri*
ISAM Web Portal Manager isimpri*
Sametime Profile**
Lotus Sametime Proxy Server stproxypri*
Cluster
Cluster
Worklight Consumer Edition** (optional)
WebSphere Portal Server & SVC** wpesby*
WebSphere Application Server Feature Pack for Web 2.0 and Mobile
IOP (not used on application server 2)
WebSphere Application Server v8
DB2 Client
IBM Installation Manager 1.6
Tivoli Application Performance Manager Agents
Tivoli Directory Integrator Plugin
IBM HTTP Server ihssby*
Usage analysis tool
Application Server 2
Data Server 1
Tivoli Application Performance Manager Agents
Tivoli Directory Integrator Dispatcher
Tivoli Directory Integrator POSIX Adapter
IBM Installation Manager 1.6
Data Studio (optional)
Tivoli Directory Integrator tdipri*
DB2 Enterprise Server Edition dbpri*
Tivoli Directory Server tdspri*
Cluster
Cluster
DB2 Enterprise Server Edition dbsby*
Tivoli Directory Server tdssby*
IBM Installation Manager 1.6
Tivoli Directory Integrator Plugin
Data Studio (optional)
Tivoli Application Performance Manager Agents
Data Server 2
Messaging Server 1
Installation Home
Tivoli Directory Integrator Plugin
IBM Java JRE
Tivoli Application Performance Manager Agents
Platform Control Tool (DOPControl)
WebSphere MQ Explorer
WebSphere Message Broker wmbpri*
WebSphere MQ wmbpri*
Multi-Instance
Multi-Instance
WebSphere Message Broker wmbsby*
WebSphere MQ wmbsby*
WebSphere MQ Explorer
Platform Control Tool (DOPControl)
Tivoli Directory Integrator Plugin
IBM Java JRE
Tivoli Application Performance Manager Agents
Messaging Server 2
Monitoring Server
IBM Security Access Manager Policy Server isampri*
Tivoli Integrated Portal tippri*
IBM Security Access Manager Authorization Server isampri*
Tivoli Netcool OMNIbus ncobuspri*
Tivoli Application Performance Manager Agents
Tivoli Enterprise Monitoring Server (TEMS) temspri*
DB2 Enterprise Server Edition (for TEPS)
Tivoli Enterprise Portal Server (TEPS) tepspri*
Tivoli Directory Integrator Plugin
WebSphere Application Server v8.5
WebSphere 8.5 Administration Console prodmgr*
WebSphere Operational Decision Management Decision Center odmpri*
WebSphere Operational Decision Management Decision Server odmdcpri*
WebSphere Application Server v8
WebSphere Service Registry and Repository (WSRR)** wsrrpri*
WebSphere Business Process Management** bpmpri*
Tivoli Directory Integrator Plugin
IBM HTTP Server proihspri*
IBM Installation Manager 1.6
Tivoli Application Performance Manager Agents
Process Server

*DOPControl Component Name
** Managed by WebSphere Application Server v8 administration console

Figure 2. Command Center Edition components

Related concepts:

"Starting, stopping, and querying status in the Field Edition" on page 53
The platform control tool allows a user to stop, start, and query IBM Defense Operations Platform components running in the Field Edition. A platform control tool tool is also available for IBM Defense Operations Platform running in the Command Center Edition.

Starting the components in the Command Center Edition

The platform control tool can be used to start the components running in the IBM Defense Operations Platform Command Center Edition.

About this task

The DOPControl command must be run as the ibmadmin user. If not logged on as the ibmadmin, run the su - ibmadmin command to switch to the ibmadmin user.

Attention: Starting individual components should only be done by experienced IBM Defense Operations Platform administrators. Unpredictable results can occur if components are not started in the required order.

Procedure

1. Log on to messaging server 1 or messaging server 2 as the ibmadmin user. If logged on as a different user, change to the ibmadmin user by running the su - ibmadmin command. Under normal operations use the platform control tool on messaging server 1. If messaging server 1 is unavailable you can run the platform control tool on messaging server 2 . Do not use the platform control tool on messaging server 1 and messaging server 2 at the same time or unpredictable results can occur.
2. Run the following command to start all the IBM Defense Operations Platform components.

   ```
   DOPControl -a start -c all -p password
   ```

   where *password* is the topology password defined when the IBM Defense Operations Platform was installed. If the *password* value contains special characters, the *password* value must be enclosed in single quotation marks. For example: 'pass$phrase'

   The components are started in the required order. Prerequisite components are started before dependent components. For example, database and directory components are started first.

   Attention: Starting all components can take 45 minutes or longer.

   To start only one component, run the following command.

   ```
   DOPControl -a start component -p password
   ```

   where *component* is an ID listed in the DOPControl help and where *password* is the topology password defined when the IBM Defense Operations Platform was installed. If the *password* value contains special characters, the *password* value must be enclosed in single quotation marks. For example: 'pass$phrase'

   Optionally the nostatus option can be added to the command. This will suppress any output returned from the command.

Results

The requested IBM Defense Operations Platform components are started.

Related tasks:

"Stopping the components in the Command Center Edition" on page 59
The platform control tool can be used to stop components running in the IBM Defense Operations Platform Command Center Edition.

"Managing HADR components in the Command Center Edition" on page 61
The platform control tool provides IBM Defense Operations Platform Command Center Edition system administration components. These Command Center Edition components allow the administrator to address unique conditions. These commands should be used with caution.

"Querying the status of the components in the Command Center Edition" on page 60
The platform control tool can be used to determine the status of the components running in the IBM Defense Operations Platform Command Center Edition.

"Getting help for the platform control tool in the Command Center Edition" on page 63
Information is available about the options for running the platform control tool in the Command Center Edition.

Stopping the components in the Command Center Edition

The platform control tool can be used to stop components running in the IBM Defense Operations Platform Command Center Edition.

About this task

The `DOPControl` command must be run as the `ibmadmin` user. If not logged on as the `ibmadmin`, run the `su - ibmadmin` command to switch to the `ibmadmin` user.

Attention: Stopping individual components should only be done by experienced IBM Defense Operations Platform administrators. Unpredictable results can occur if components are not stopped in the required order.

Procedure

1. Log on to messaging server 1 or messaging server 2 as the `ibmadmin` user. If logged on as a different user, change to the `ibmadmin` user by running the `su - ibmadmin` command. Under normal operations use the platform control tool on messaging server 1. If messaging server 1 is unavailable you can run the platform control tool on messaging server 2 . Do not use the platform control tool on messaging server 1 and messaging server 2 at the same time or unpredictable results can occur.
2. Run the following command to stop all the IBM Defense Operations Platform components.

   ```
   DOPControl -a stop -c all -p password
   ```

   where *password* is the topology password defined when the IBM Defense Operations Platform was installed. If the *password* value contains special characters, the *password* value must be enclosed in single quotation marks. For example: `'pass$phrase'`

   Attention: Stopping all components can take 45 minutes or longer.

   To stop only one component, run the following command.

   ```
   DOPControl -a stop -c component -p password
   ```

   where *component* is an ID listed in the `DOPControl` help and where *password* is the topology password defined when the IBM Defense Operations Platform was installed. If the *password* value contains special characters, the *password* value must be enclosed in single quotation marks. For example: `'pass$phrase'`

   Optionally the `nostatus` option can be added to the command. This will suppress any output returned from the command.

Results

The requested IBM Defense Operations Platform components are stopped.

Related tasks:

"Starting the components in the Command Center Edition" on page 57
The platform control tool can be used to start the components running in the IBM Defense Operations Platform Command Center Edition.

"Managing HADR components in the Command Center Edition" on page 61
The platform control tool provides IBM Defense Operations Platform Command Center Edition system administration components. These Command Center Edition components allow the administrator to address unique conditions. These commands should be used with caution.

"Querying the status of the components in the Command Center Edition" on page 60
The platform control tool can be used to determine the status of the components running in the IBM Defense Operations Platform Command Center Edition.

"Getting help for the platform control tool in the Command Center Edition" on page 63
Information is available about the options for running the platform control tool in the Command Center

Edition.

Querying the status of the components in the Command Center Edition

The platform control tool can be used to determine the status of the components running in the IBM Defense Operations Platform Command Center Edition.

About this task

The `DOPControl` command must be run as the `ibmadmin` user. If not logged on as the `ibmadmin`, run the `su - ibmadmin` command to switch to the `ibmadmin` user.

Procedure

1. Log on to messaging server 1 or messaging server 2 as the `ibmadmin` user. If logged on as a different user, change to the `ibmadmin` user by running the `su - ibmadmin` command. Under normal operations use the platform control tool on messaging server 1. If messaging server 1 is unavailable you can run the platform control tool on messaging server 2 . Do not use the platform control tool on messaging server 1 and messaging server 2 at the same time or unpredictable results can occur.
2. Run the following command to query the status all the IBM Defense Operations Platform components.

   ```
   DOPControl -a status -c all -p  password
   ```

   where *password* is the topology password defined when the IBM Defense Operations Platform was installed. If the *password* value contains special characters, the *password* value must be enclosed in single quotation marks. For example: `'pass$phrase'`

   To check only one component, run the following command.

   ```
   DOPControl -a status -c component -p password
   ```

   where *component* is an ID in the `DOPControl` help and where *password* is the topology password defined when the IBM Defense Operations Platform was installed. If the *password* value contains special characters, the *password* value must be enclosed in single quotation marks. For example: `'pass$phrase'`

Results

Components that are started will display **[on]**. Components that are not started will display **[off]**.

Related tasks:

"Starting the components in the Command Center Edition" on page 57
The platform control tool can be used to start the components running in the IBM Defense Operations Platform Command Center Edition.

"Stopping the components in the Command Center Edition" on page 59
The platform control tool can be used to stop components running in the IBM Defense Operations Platform Command Center Edition.

"Managing HADR components in the Command Center Edition" on page 61
The platform control tool provides IBM Defense Operations Platform Command Center Edition system administration components. These Command Center Edition components allow the administrator to address unique conditions. These commands should be used with caution.

"Getting help for the platform control tool in the Command Center Edition" on page 63
Information is available about the options for running the platform control tool in the Command Center Edition.

Managing HADR components in the Command Center Edition

The platform control tool provides IBM Defense Operations Platform Command Center Edition system administration components. These Command Center Edition components allow the administrator to address unique conditions. These commands should be used with caution.

About this task

The `DOPControl` command must be run as the `ibmadmin` user. If not logged on as the `ibmadmin`, run the `su - ibmadmin` command to switch to the `ibmadmin` user.

Attention: Managing high availability disaster recovery (HADR) components should only be done by experienced IBM Defense Operations Platform administrators.

Procedure

1. Log on to messaging server 1 or messaging server 2 as the `ibmadmin` user. If logged on as a different user, change to the `ibmadmin` user by running the `su - ibmadmin` command. Under normal operations use the platform control tool on messaging server 1. If messaging server 1 is unavailable you can run the platform control tool on messaging server 2 . Do not use the platform control tool on messaging server 1 and messaging server 2 at the same time or unpredictable results can occur.
2. Run the following command with the desired system administration command option.

   ```
   DOPControl -a action -c component -p password
   ```

   where *action* can be one of the following values:

   `activate`
   Activate DB2 HADR components.

   `deactivate`
   Deactivate DB2 HADR components.

   `resume` Resume DB2 HADR components.

   `suspend`
   Suspend DB2 HADR components.

   The *component* value is dependent on the specified action. Valid *component* values can be found by running `DOPControl -h`.

   Password is the topology password defined when the IBM Defense Operations Platform was installed. If the *password* value contains special characters, the *password* value must be enclosed in single quotation marks. For example: `'pass$phrase'`

   Optionally the `nostatus` option can be added to the command. This will suppress any output returned from the command.

Results

The requested action is taken.

Related tasks:

"Starting the components in the Command Center Edition" on page 57
The platform control tool can be used to start the components running in the IBM Defense Operations Platform Command Center Edition.

"Stopping the components in the Command Center Edition" on page 59
The platform control tool can be used to stop components running in the IBM Defense Operations Platform Command Center Edition.

"Querying the status of the components in the Command Center Edition" on page 60
The platform control tool can be used to determine the status of the components running in the IBM Defense Operations Platform Command Center Edition.

"Getting help for the platform control tool in the Command Center Edition" on page 63
Information is available about the options for running the platform control tool in the Command Center Edition.

Manually mounting and unmounting the WebSphere Message Broker directory

The /opt/ibm/ioc/shared/wmq directory is shared between the primary and standby WebSphere Message Broker instances. This directory should be automatically mounted by the operating system for network sharing. However, there are cases where manually mounting or unmounting might be required.

Procedure

1. Log on to messaging server 1 or messaging server 2 as the ibmadmin user. If logged on as a different user, change to the ibmadmin user by running the su - ibmadmin command. Under normal operations use the platform control tool on messaging server 1. If messaging server 1 is unavailable you can run the platform control tool on messaging server 2 . Do not use the platform control tool on messaging server 1 and messaging server 2 at the same time or unpredictable results can occur.
2. Run the following command with the desired system administration command option.

   ```
   DOPControl -a action -c component -p password
   ```

   where *action* is one of the following values:

   mount Mount the /opt/ibm/ioc/shared/wmq directory. This action should be used when automatic mounting fails or when an umount action was previously run.

   unmount
   Unmount the shared messages directory. Use this option to stop network sharing of the /opt/ibm/ioc/shared/wmq directory.

   and *component* is one of the following values:

   shmsgpri
   Specifies that the /opt/ibm/ioc/shared/wmq directory is to be mounted, or unmounted, on messaging server 1.

   shmsgsby
   Specifies that the /opt/ibm/ioc/shared/wmq directory is to be mounted, or unmounted, on messaging server 2.

   Password is the topology password defined when the IBM Defense Operations Platform was installed. If the *password* value contains special characters, the *password* value must be enclosed in single quotation marks. For example: 'pass$phrase'

   Optionally the nostatus option can be added to the command. This will suppress any output returned from the command.

Results

The requested action is taken.

Related tasks:

"Starting the components in the Command Center Edition" on page 57
The platform control tool can be used to start the components running in the IBM Defense Operations Platform Command Center Edition.

"Stopping the components in the Command Center Edition" on page 59
The platform control tool can be used to stop components running in the IBM Defense Operations Platform Command Center Edition.

"Querying the status of the components in the Command Center Edition" on page 60
The platform control tool can be used to determine the status of the components running in the IBM

Defense Operations Platform Command Center Edition.

"Getting help for the platform control tool in the Command Center Edition"
Information is available about the options for running the platform control tool in the Command Center Edition.

Getting help for the platform control tool in the Command Center Edition

Information is available about the options for running the platform control tool in the Command Center Edition.

About this task

The `DOPControl` command must be run as the `ibmadmin` user. If not logged on as the `ibmadmin`, run the `su - ibmadmin` command to switch to the `ibmadmin` user.

Procedure

On messaging server 1 or messaging server 2 run the one of the following commands to see options for the `DOPControl` command.

```
DOPControl -a help

or

DOPControl -h
```

Results

The options for the **`IOCControl`** command are displayed.

Related tasks:

"Starting the components in the Command Center Edition" on page 57
The platform control tool can be used to start the components running in the IBM Defense Operations Platform Command Center Edition.

"Stopping the components in the Command Center Edition" on page 59
The platform control tool can be used to stop components running in the IBM Defense Operations Platform Command Center Edition.

"Managing HADR components in the Command Center Edition" on page 61
The platform control tool provides IBM Defense Operations Platform Command Center Edition system administration components. These Command Center Edition components allow the administrator to address unique conditions. These commands should be used with caution.

"Querying the status of the components in the Command Center Edition" on page 60
The platform control tool can be used to determine the status of the components running in the IBM Defense Operations Platform Command Center Edition.

Determining the status of IBM Defense Operations Platform services and components

IBM Defense Operations Platform provides a number of system verification check tool tests that can be used to determine the operational status of various IBM Defense Operations Platform services and components.

The tests are logically grouped by function. For example, collaboration and monitoring.

Each test provides help documentation containing troubleshooting steps to resolve issues with the component, server, or service.

Using the system verification check tool

The system verification check tool is used to determine the operational status of services comprising the IBM Defense Operations Platform system.

About this task

The system verification check tool tool verifies system capabilities.

For details on individual tests and troubleshooting if the tests fails, click **Help** for the test.

Properties provides additional information about the test for use when calling IBM Software Support.

Procedure

1. Log on to the IBM Defense Operations Platform administration console.
2. Click any WebSphere Portal link at the top of the page.
3. Log on as the WebSphere Portal administrator. The administrator is defined in the `PORTAL.ADMIN.UID` property in the topology properties file. The default administrator is `wpsadmin`.
4. Click **Administration** in the top banner.
5. Click the **System Verification Check** tab.
6. Select the test or tests to be run by doing one of the following:
   - Click a specific test to be run.
   - Click **Run All Tests** to test the capabilities of all selections.

Results

The ✓ icon will be displayed when a test completes successfully. The ✗ icon will be displayed when a test fails. If a test fails, follow the problem determination instructions for the test to resolve the errors.

These instructions can also be accessed by clicking the ✗ icon or **Help**.

If a specific test was run, the run results of the test are displayed at the bottom of the portlet along with the test execution time. If **Run All Tests** was selected, this information is not displayed.

What to do next

The tool can be reset, and all results cleared, by clicking **Reset**.

Related tasks:

"Accessing IBM Defense Operations Platform administration consoles" on page 53
The IBM Defense Operations Platform is comprised of a number of products. Each of these products has one or more administration consoles. To make it easier to find the installed administration consoles, IBM Defense Operations Platform provides pages where the consoles can be accessed.

Application Server (REST BPM_DE.AppTarget.BPMNode1.0) Test

The Application Server (REST BPM_DE.AppTarget.BPMNode1.0) test tests access to the WebSphere Application Server REST service on the target server.

Resources

The Application Server (REST BPM_DE.AppTarget.BPMNode1.0) test uses the following resource:

- WebSphere Application Server on process server.

Problem determination

If the Application Server (REST BPM_DE.AppTarget.BPMNode1.0) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the IBM Business Process Manager server, specify `status` for *action* and `bpm` for *component*.
   - To start the IBM Business Process Manager server, specify `start` for *action* and `bpm` for *component*.
   - To stop the IBM Business Process Manager server, specify `stop` for *action* and `bpm` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the process server review the following WebSphere Application Server logs:
      - `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/logs/BPM_DE.AppTarget.BPMNode1.0/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/logs/BPM_DE.AppTarget.BPMNode1.0/SystemErr.log`
3. Verify that the file system on the process server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the BPM_DE.AppTarget.BPMNode1.0 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the process server system log on as `ibmadmin`.

   b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.

   a. If message `ADMU0509I: The Application Server "BPM_DE.AppTarget.BPMNode1.0" cannot be reached. It appears to be stopped.` is displayed, start the server using the following command: `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/startServer.sh BPM_DE.AppTarget.BPMNode1.0`. Skip this step if message `ADMU0508I: The Application Server`

   `"BPM_DE.AppTarget.BPMNode1.0" is STARTED.` is displayed. If you had to start the server, a message similar to the following will be displayed: `ADMU3000I: Server BPM_DE.AppTarget.BPMNode1.0 open for e-business; process id is 26654`.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:

   a. nodeagent
   b. BPM_DE.AppTarget.BPMNode1.0

   Stop servers in this order:

   a. BPM_DE.AppTarget.BPMNode1.0
   b. nodeagent

   The BPM_DE.AppTarget.BPMNode1.0 server is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/stopServer.sh -all -username WAS_ADMIN_USER -password WAS_ADMIN_PWD` where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   The nodeagent is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/stopNode.sh -username WAS_ADMIN_USER -password WAS_ADMIN_PWD` where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the BPM_DE.AppTarget.BPMNode1.0 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

   a. Log on to the WebSphere Application Server Administrative Console at `http://APPLICATION_SERVER_HOST:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.

   b. View the status of the BPM_DE.AppTarget.BPMNode1.0 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➔ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/startNode.sh` command in a command window.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:

   a. nodeagent
   b. BPM_DE.AppTarget.BPMNode1.0

   Stop servers in this order:

   a. BPM_DE.AppTarget.BPMNode1.0
   b. nodeagent

   To stop the BPM_DE.AppTarget.BPMNode1.0 server, select the server and click **Stop**.

   The nodeagent is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/stopNode.sh -username`

WAS_ADMIN_USER -password *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally admin) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Application Server (REST IopServer1) Test

The Application Server (REST IopServer1) test tests access to the WebSphere Application Server REST service on the target server.

Resources

The Application Server (REST IopServer1) test uses the following resource:

- WebSphere Application Server on the application server.

Problem determination

If the Application Server (REST IopServer1) test fails, do the following to find and resolve the access problem.

Procedure

1. If running the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use iop and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```
   b. To start the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```
   c. To stop the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a stop -c component -p topology_password
   ```
2. If running the Command Center Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the primary server, specify status for *action* and ioppri for *component*.
   - To check the status of the standby server, specify status for *action* and iopsby for *component*.
   - To start the primary server, specify start for *action* and ioppri for *component*.
   - To start the standby server, specify start for *action* and iopsby for *component*.
   - To stop the primary server, specify stop for *action* and ioppri for *component*.
   - To stop the standby server, specify stop for *action* and iopsby for *component*.

   Specify your topology password for *topology_password*.
   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:

- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log

b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
   - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
   - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log

c. On the application server review the following WebSphere Application Server logs:
   - /opt/IBM/WebSphere/AppServer/profiles/IopProfile1/logs/IopServer1/SystemOut.log
   - /opt/IBM/WebSphere/AppServer/profiles/IopProfile1/logs/IopServer1/SystemErr.log

4. Verify that the file system on the application server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the IopServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:

   a. On the application server system log on as ibmadmin.

   b. In a command window, run: /opt/IBM/WebSphere/AppServer/profiles/IopProfile1/bin/serverStatus.sh -all -username *WAS_ADMIN_USER* -password *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally admin) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   c. If message ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped. is displayed, start the nodeagent using the following command: /opt/IBM/WebSphere/AppServer/profiles/IopProfile1/bin/startNode.sh . Skip this step if message ADMU0508I: The Application Server "nodeagent" is STARTED. is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: ADMU3000I: Server nodeagent open for e-business; process id is 26654.

   a. If message ADMU0509I: The Application Server "IopServer1" cannot be reached. It appears to be stopped. is displayed, start the IopServer1 server using the following command: /opt/IBM/WebSphere/AppServer/profiles/IopProfile1/bin/startServer.sh IopServer1. Skip this step if message ADMU0508I: The Application Server "IopServer1" is STARTED. is displayed. If you had to start IopServer1, a message similar to the following will be displayed: ADMU3000I: Server IopServer1 open for e-business; process id is 26654.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. IopServer1

Stop servers in this order:

a. IopServer1

b. nodeagent

The IopServer1 server is stopped by running the following command in a command window on the application server: /opt/IBM/WebSphere/AppServer/profiles/IopProfile1/bin/stopServer.sh -all -username *WAS_ADMIN_USER* -password *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally admin) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

The nodeagent is stopped by running the following command in a command window on the application server: /opt/IBM/WebSphere/AppServer/profiles/IopProfile1/bin/stopNode.sh -username *WAS_ADMIN_USER* -password *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally admin) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

6. Verify that the IopServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.
   b. View the status of the IopServer1 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ❔ icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/IopProfile1/bin/startNode.sh` command in a command window.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:
   a. nodeagent
   b. IopServer1

   Stop servers in this order:
   a. IopServer1
   b. nodeagent

   To stop the IopServer1 server, select the server and click **Stop**.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/IopProfile1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Application Server (REST IopServer2) Test

The Application Server (REST IopServer2) test tests access to the WebSphere Application Server REST service on the target server.

Resources

The Application Server (REST IopServer2) test uses the following resource:
- WebSphere Application Server on application server 2.

Problem determination

If the Application Server (REST IopServer2) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.

- To check the status of the primary server, specify `status` for *action* and `ioppri` for *component*.
- To check the status of the standby server, specify `status` for *action* and `iopsby` for *component*.
- To start the primary server, specify `start` for *action* and `ioppri` for *component*.
- To start the standby server, specify `start` for *action* and `iopsby` for *component*.
- To stop the primary server, specify `stop` for *action* and `ioppri` for *component*.
- To stop the standby server, specify `stop` for *action* and `iopsby` for *component*.

Specify your topology password for *topology_password*.

```
su - ibmadmin

DOPControl -a action -c component -p topology_password
```

2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On application server 2 review the following WebSphere Application Server logs:
      - `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/logs/IopServer2/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/logs/IopServer2/SystemErr.log`

3. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.

4. Verify that the IopServer2 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the application server system log on as `ibmadmin`.

   b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.

   a. If message `ADMU0509I: The Application Server "IopServer2" cannot be reached. It appears to be stopped.` is displayed, start the IopServer2 server using the following command: `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/bin/startServer.sh IopServer2`. Skip this step if message `ADMU0508I: The Application Server "IopServer2" is STARTED.` is displayed. If you had to start IopServer2, a message similar to the following will be displayed: `ADMU3000I: Server IopServer2 open for e-business; process id is 26654`.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:
   a. nodeagent
   b. IopServer2

Stop servers in this order:

a. IopServer2

b. nodeagent

The IopServer2 server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/bin/stopServer.sh -all -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/bin/stopNode.sh -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the IopServer2 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

   a. Log on to the WebSphere Application Server Administrative Console at `http://`*APPLICATION_SERVER_HOST*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.

   b. View the status of the IopServer2 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➔ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. IopServer2

Stop servers in this order:

a. IopServer2

b. nodeagent

To stop the IopServer2 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/IopProfile2/bin/stopNode.sh -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Application Server (REST isim1) Test

The Application Server (REST isim1) test tests access to the WebSphere Application Server REST service on the target server.

Resources

The Application Server (REST isim1) test uses the following resource:

- WebSphere Application Server on the application server.

Problem determination

If the Application Server (REST isim1) test fails, do the following to find and resolve the access problem.

Procedure

1. If running in the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use `isim` and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```
   b. To start the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```
   c. To stop the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a stop -c component -p topology_password
   ```
2. If running in the Command Center Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of IBM Security Identity Manager, specify `status` for *action* and `isim` for *component*.
   - To stop IBM Security Identity Manager, specify `stop` for *action* and `isim` for *component*.
   - To start IBM Security Identity Manager, specify `start` for *action* and `isim` for *component*.

   Specify your topology password for *topology_password*.
   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the application server review the following WebSphere Application Server logs:
      - `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/isim1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/isim1/SystemErr.log`
4. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.

5. Verify that the isim1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the application server system log on as `ibmadmin`.
   b. In a command window, run: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.
   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.
   a. If message `ADMU0509I: The Application Server "isim1" cannot be reached. It appears to be stopped.` is displayed, start the isim1 server using the following command: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh isim1`. Skip this step if message `ADMU0508I: The Application Server "isim1" is STARTED.` is displayed. If you had to start isim1, a message similar to the following will be displayed: `ADMU3000I: Server isim1 open for e-business; process id is 26654`.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:
   a. nodeagent
   b. isim1

   Stop servers in this order:
   a. isim1
   b. nodeagent

   The isim1 server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.
6. Verify that the isim1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9061/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.
   b. View the status of the isim1 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. isim1

Stop servers in this order:

a. isim1

b. nodeagent

To stop the isim1 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopNode.sh -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Application Server (REST odmServer1) Test

The Application Server (REST odmServer1) test tests access to the WebSphere Application Server REST service on the target server.

Resources

The Application Server (REST odmServer1) test uses the following resource:

- WebSphere Application Server on process server.

Problem determination

If the Application Server (REST odmServer1) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of IBM Operational Decision Manager, specify `status` for *action* and `odm` for *component*.
   - To check the status of IBM Operational Decision Manager, Decision Center specify `status` for *action* and `odmdc` for *component*.
   - To start IBM Operational Decision Manager, specify `start` for *action* and `odm` for *component*.
   - To start IBM Operational Decision Manager, Decision Center specify `start` for *action* and `odmdc` for *component*.
   - To stop IBM Operational Decision Manager, specify `stop` for *action* and `odm` for *component*.
   - To stop IBM Operational Decision Manager, Decision Center specify `stop` for *action* and `odmdc` for *component*.

   Specify your topology password for *topology_password*.

```
su - ibmadmin
```

```
DOPControl -a action -c component -p topology_password
```

2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the process serverreview the following WebSphere Application Server logs:
      - `/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/logs/odmServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/logs/odmServer1/SystemErr.log`
3. Verify that the file system on the process server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the odmServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the process server system log on as `ibmadmin`.

   b. In a command window, run: `/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/serverStatus.sh -all -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654.`

   a. If message `ADMU0509I: The Application Server "odmServer1" cannot be reached. It appears to be stopped.` is displayed, start the server using the following command: `/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/startServer.sh odmServer1`. Skip this step if message `ADMU0508I: The Application Server "odmServer1" is STARTED.` is displayed. If you had to start the server, a message similar to the following will be displayed: `ADMU3000I: Server odmServer1 open for e-business; process id is 26654.`

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:

   a. nodeagent

   b. odmServer1

   Stop servers in this order:

   a. odmServer1

   b. nodeagent

   The odmServer1 server is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/stopServer.sh -all`

`-username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

The nodeagent is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the odmServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`PROCESS_SERVER_HOST`*`:9060/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *PROCESS_SERVER_HOST* is the host name for the process server.

   b. View the status of the odmServer1 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➔ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. odmServer1

Stop servers in this order:

a. odmServer1

b. nodeagent

To stop the odmServer1 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Application Server (REST odmdc1) Test

The Application Server (REST odmdc1) test tests access to the WebSphere Application Server REST service on the target server.

Resources

The Application Server (REST odmdc1) test uses the following resource:

- WebSphere Application Server on process server.

Problem determination

If the Application Server (REST odmdc1) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of IBM Operational Decision Manager, specify `status` for *action* and `odm` for *component*.
   - To check the status of IBM Operational Decision Manager, Decision Center specify `status` for *action* and `odmdc` for *component*.
   - To start IBM Operational Decision Manager, specify `start` for *action* and `odm` for *component*.
   - To start IBM Operational Decision Manager, Decision Center specify `start` for *action* and `odmdc` for *component*.
   - To stop IBM Operational Decision Manager, specify `stop` for *action* and `odm` for *component*.
   - To stop IBM Operational Decision Manager, Decision Center specify `stop` for *action* and `odmdc` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin
   ```

   ```
   DOPControl -a action -c component -p topology_password
   ```
2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the process serverreview the following WebSphere Application Server logs:
      - `/opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/logs/odmdc1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/logs/odmdc1/SystemErr.log`
3. Verify that the file system on the process server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the odmdc1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:

   a. On the process server system log on as `ibmadmin`.

   b. In a command window, run: `/opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654.`

a. If message `ADMU0509I: The Application Server "odmdc1" cannot be reached. It appears to be stopped.` is displayed, start the server using the following command: `/opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/bin/startServer.sh odmdc1`. Skip this step if message `ADMU0508I: The Application Server "odmdc1" is STARTED.` is displayed. If you had to start the server, a message similar to the following will be displayed: `ADMU3000I: Server odmdc1 open for e-business; process id is 26654`.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. odmdc1

Stop servers in this order:

a. odmdc1

b. nodeagent

The odmdc1 server is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/bin/stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

The nodeagent is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the odmdc1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`PROCESS_SERVER_HOST`*`:9060/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *PROCESS_SERVER_HOST* is the host name for the process server.

   b. View the status of the odmdc1 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. odmdc1

Stop servers in this order:

a. odmdc1

b. nodeagent

To stop the odmdc1 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Application Server (REST STProxyServer1) Test

The Application Server (REST STProxyServer1) test tests access to the WebSphere Application Server REST service on the target server.

Resources

The Application Server (REST STProxyServer1) test uses the following resource:

- WebSphere Application Server on the application server.

Problem determination

If the Application Server (REST STProxyServer1) test fails, do the following to find and resolve the access problem.

Procedure

1. If running in the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use `stproxy` and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```
   b. To start the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```
   c. To stop the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a stop -c component -p topology_password
   ```
2. If running in the Command Center Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the Sametime server, specify `status` for *action* and `stproxy` for *component*.
   - To start the Sametime server, specify `start` for *action* and `stproxy` for *component*.
   - To stop the Sametime server, specify `stop` for *action* and `stproxy` for *component*.

   Specify your topology password for *topology_password*.
   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

c. On the application server review the following WebSphere Application Server logs:
   - `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/logs/STProxyServer1/SystemOut.log`
   - `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/logs/STProxyServer1/SystemErr.log`

4. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the STProxyServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:

   a. On the application server system log on as `ibmadmin`.

   b. In a command window, run: `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.

   a. If message `ADMU0509I: The Application Server "STProxyServer1" cannot be reached. It appears to be stopped.` is displayed, start the STProxyServer1 server using the following command: `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/bin/startServer.sh STProxyServer1`. Skip this step if message `ADMU0508I: The Application Server "STProxyServer1" is STARTED.` is displayed. If you had to start STProxyServer1, a message similar to the following will be displayed: `ADMU3000I: Server STProxyServer1 open for e-business; process id is 26654`.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. STProxyServer1

Stop servers in this order:

a. STProxyServer1

b. nodeagent

The STProxyServer1 server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/bin/stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

6. Verify that the STProxyServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.
   b. View the status of the STProxyServer1 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/bin/startNode.sh` command in a command window.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:
   a. nodeagent
   b. STProxyServer1

   Stop servers in this order:
   a. STProxyServer1
   b. nodeagent

   To stop the STProxyServer1 server, select the server and click **Stop**.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServerv7/profiles/STPAppProfile1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Application Server (REST WebSphere_Portal) Test

The Application Server (REST WebSphere_Portal) test tests access to the WebSphere Application Server REST service on the target server.

Resources

The Application Server (REST WebSphere_Portal) test uses the following resource:
- WebSphere Application Server on the application server.

Problem determination

If the Application Server (REST WebSphere_Portal) test fails, do the following to find and resolve the access problem.

Procedure

1. If running in the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use wpe and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:

      ```
      su - ibmadmin

      DOPControl -a status -c component -p topology_password
      ```

   b. To start the component run the following commands:

      ```
      su - ibmadmin

      DOPControl -a start -c component -p topology_password
      ```

   c. To stop the component run the following commands:

      ```
      su - ibmadmin

      DOPControl -a stop -c component -p topology_password
      ```

2. If running in the Command Center Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the primary WebSphere Portal server, specify status for *action* and wpepri for *component*.
   - To check the status of the standby WebSphere Portal server, specify status for *action* and wpesby for *component*.
   - To start the primary WebSphere Portal server, specify start for *action* and wpepri for *component*.
   - To start the standby WebSphere Portal server, specify start for *action* and wpesby for *component*.
   - To stop the primary WebSphere Portal server, specify stop for *action* and wpepri for *component*.
   - To stop the standby WebSphere Portal server, specify stop for *action* and wpesby for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```

3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log

   c. On the application server review the following WebSphere Application Server logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log

4. Verify that the file system on the application server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the WebSphere_Portal server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the application server system log on as ibmadmin.

b. In a command window, run: `/opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.

a. If message `ADMU0509I: The Application Server "WebSphere_Portal" cannot be reached. It appears to be stopped.` is displayed, start the WebSphere_Portal server using the following command: `/opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_Portal`. Skip this step if message `ADMU0508I: The Application Server "WebSphere_Portal" is STARTED.` is displayed. If you had to start WebSphere_Portal, a message similar to the following will be displayed: `ADMU3000I: Server WebSphere_Portal open for e-business; process id is 26654`.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. WebSphere_Portal

Stop servers in this order:

a. WebSphere_Portal

b. nodeagent

The WebSphere_Portal server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

6. Verify that the WebSphere_Portal server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.

b. View the status of the WebSphere_Portal server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent
b. WebSphere_Portal

Stop servers in this order:

a. WebSphere_Portal
b. nodeagent

To stop the WebSphere_Portal server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Application Server (REST WebSphere_Portal_PortalNode2) Test

The Application Server (REST WebSphere_Portal_PortalNode2) test tests access to the WebSphere Application Server REST service on the target server.

Resources

The Application Server (REST WebSphere_Portal_PortalNode2) test uses the following resource:

- WebSphere Application Server on application server 2.

Problem determination

If the Application Server (REST WebSphere_Portal_PortalNode2) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of the primary WebSphere Portal server, specify `status` for *action* and `wpepri` for *component*.
   - To check the status of the standby WebSphere Portal server, specify `status` for *action* and `wpesby` for *component*.
   - To start the primary WebSphere Portal server, specify `start` for *action* and `wpepri` for *component*.
   - To start the standby WebSphere Portal server, specify `start` for *action* and `wpesby` for *component*.
   - To stop the primary WebSphere Portal server, specify `stop` for *action* and `wpepri` for *component*.
   - To stop the standby WebSphere Portal server, specify `stop` for *action* and `wpesby` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin
   ```

   ```
   DOPControl -a action -c component -p topology_password
   ```
2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

c. On application server 2 review the following WebSphere Application Server logs:
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

3. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the WebSphere_Portal_PortalNode2 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:

   a. On the application server system log on as `ibmadmin`.

   b. In a command window, run: `/opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.

   a. If message `ADMU0509I: The Application Server "WebSphere_Portal_PortalNode2" cannot be reached. It appears to be stopped.` is displayed, start the WebSphere_Portal_PortalNode2 server using the following command: `/opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_Portal_PortalNode2`. Skip this step if message `ADMU0508I: The Application Server "WebSphere_Portal_PortalNode2" is STARTED.` is displayed. If you had to start WebSphere_Portal_PortalNode2, a message similar to the following will be displayed: `ADMU3000I: Server WebSphere_Portal_PortalNode2 open for e-business; process id is 26654`.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:

   a. nodeagent

   b. WebSphere_Portal_PortalNode2

   Stop servers in this order:

   a. WebSphere_Portal_PortalNode2

   b. nodeagent

   The WebSphere_Portal_PortalNode2 server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the WebSphere_Portal_PortalNode2 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.
   b. View the status of the WebSphere_Portal_PortalNode2 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` command in a command window.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:
   a. nodeagent
   b. WebSphere_Portal_PortalNode2

   Stop servers in this order:
   a. WebSphere_Portal_PortalNode2
   b. nodeagent

   To stop the WebSphere_Portal_PortalNode2 server, select the server and click **Stop**.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Application Server (REST WSRRServer1) Test

The Application Server (REST WSRRServer1) test tests access to the WebSphere Application Server REST service on the target server.

Resources

The Application Server (REST WSRRServer1) test uses the following resource:

- WebSphere Application Server on process server.

Problem determination

If the Application Server (REST WSRRServer1) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.

- To check the status of the WebSphere Service Registry and Repository server, specify `status` for *action* and `wsrr` for *component*.
- To start the WebSphere Service Registry and Repository server, specify `start` for *action* and `wsrr` for *component*.
- To stop the WebSphere Service Registry and Repository server, specify `stop` for *action* and `wsrr` for *component*.

Specify your topology password for *topology_password*.

```
su - ibmadmin

DOPControl -a action -c component -p topology_password
```

2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the process serverreview the following WebSphere Application Server logs:
      - `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/logs/WSRRServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/logs/WSRRServer1/SystemErr.log`
3. Verify that the file system on the process server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the WSRRServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the process server system log on as `ibmadmin`.

   b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654.`

   a. If message `ADMU0509I: The Application Server "WSRRServer1" cannot be reached. It appears to be stopped.` is displayed, start the server using the following command: `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/startServer.sh WSRRServer1`. Skip this step if message `ADMU0508I: The Application Server "WSRRServer1" is STARTED.` is displayed. If you had to start the server, a message similar to the following will be displayed: `ADMU3000I: Server WSRRServer1 open for e-business; process id is 26654.`

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. WSRRServer1

Stop servers in this order:

a. WSRRServer1

b. nodeagent

The WSRRServer1 server is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/stopServer.sh -all -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

The nodeagent is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/stopNode.sh -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the WSRRServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

   a. Log on to the WebSphere Application Server Administrative Console at `http://`*APPLICATION_SERVER_HOST*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.

   b. View the status of the WSRRServer1 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. WSRRServer1

Stop servers in this order:

a. WSRRServer1

b. nodeagent

To stop the WSRRServer1 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/stopNode.sh -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Application Server (REST WorklightServer1) Test

The Application Server (REST WorklightServer1) test tests access to the WebSphere Application Server REST service on the target server.

Note: IBM Worklight® is only available for installation through an IBM Services engagement.

Resources

The Application Server (REST WorklightServer1) test uses the following resource:

- WebSphere Application Server on the application server.

Problem determination

If the Application Server (REST WorklightServer1) test fails, do the following to find and resolve the access problem.

Procedure

1. If running in the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use `wrklt` and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
   ```
   su - ibmadmin
   
   DOPControl -a status -c component -p topology_password
   ```
   b. To start the component run the following commands:
   ```
   su - ibmadmin
   
   DOPControl -a start -c component -p topology_password
   ```
   c. To stop the component run the following commands:
   ```
   su - ibmadmin
   
   DOPControl -a stop -c component -p topology_password
   ```
2. If running in the Command Center Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of IBM Worklight, specify `status` for *action* and `wrklt` for *component*.
   - To start IBM Worklight, specify `start` for *action* and `wrklt` for *component*.
   - To stop IBM Worklight, specify `stop` for *action* and `wrklt` for *component*.

   Specify your topology password for *topology_password*.
   ```
   su - ibmadmin
   
   DOPControl -a action -c component -p topology_password
   ```
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the aplication server review the following WebSphere Application Server logs:
   - `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/logs/WorklightServer1/SystemOut.log`
   - `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/logs/WorklightServer1/SystemErr.log`

4. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the WorklightServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the application server system log on as `ibmadmin`.
   b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.
   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.
   a. If message `ADMU0509I: The Application Server "WorklightServer1" cannot be reached. It appears to be stopped.` is displayed, start the WorklightServer1 server using the following command: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startServer.sh WorklightServer1`. Skip this step if message `ADMU0508I: The Application Server "WorklightServer1" is STARTED.` is displayed. If you had to start WorklightServer1, a message similar to the following will be displayed: `ADMU3000I: Server WorklightServer1 open for e-business; process id is 26654`.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:
   a. nodeagent
   b. WorklightServer1

   Stop servers in this order:
   a. WorklightServer1
   b. nodeagent

   The WorklightServer1 server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.
6. Verify that the WorklightServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.
   b. View the status of the WorklightServer1 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

The ❓ icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. WorklightServer1

Stop servers in this order:

a. WorklightServer1

b. nodeagent

To stop the WorklightServer1 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Application Server (REST WorklightServer2) Test

The Application Server (REST WorklightServer2) test tests access to the WebSphere Application Server REST service on the target server.

Note: IBM Worklight is only available for installation through an IBM Services engagement.

Resources

The Application Server (REST WorklightServer2) test uses the following resource:

- WebSphere Application Server on application server 2.

Problem determination

If the Application Server (REST WorklightServer2) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of IBM Worklight, specify `status` for *action* and `wrklt` for *component*.
   - To start IBM Worklight, specify `start` for *action* and `wrklt` for *component*.
   - To stop IBM Worklight, specify `stop` for *action* and `wrklt` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin
   ```

   ```
   DOPControl -a action -c component -p topology_password
   ```

2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log
   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log
   c. On application server 2 review the following WebSphere Application Server logs:
      - /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/logs/WorklightServer2/SystemOut.log
      - /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/logs/WorklightServer2/SystemErr.log
3. Verify that the file system on the application server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the WorklightServer2 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the application server 2 system log on as ibmadmin.
   b. In a command window, run: /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/serverStatus.sh -all -username *WAS_ADMIN_USER* -password *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally admin) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.
   c. If message ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped. is displayed, start the nodeagent using the following command: /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/startNode.sh . Skip this step if message ADMU0508I: The Application Server "nodeagent" is STARTED. is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: ADMU3000I: Server nodeagent open for e-business; process id is 26654.
   a. If message ADMU0509I: The Application Server "WorklightServer2" cannot be reached. It appears to be stopped. is displayed, start the WorklightServer2 server using the following command: /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/startServer.sh WorklightServer2. Skip this step if message ADMU0508I: The Application Server "WorklightServer2" is STARTED. is displayed. If you had to start WorklightServer2, a message similar to the following will be displayed: ADMU3000I: Server WorklightServer2 open for e-business; process id is 26654.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:
   a. nodeagent
   b. WorklightServer2

   Stop servers in this order:
   a. WorklightServer2
   b. nodeagent

   The WorklightServer2 server is stopped by running the following command in a command window on the application server: /opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/

   `stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the WorklightServer2 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.
   b. View the status of the WorklightServer2 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➔ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/startNode.sh` command in a command window.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:
   a. nodeagent
   b. WorklightServer2

   Stop servers in this order:
   a. WorklightServer2
   b. nodeagent

   To stop the WorklightServer2 server, select the server and click **Stop**.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Application Server (WebSphere Application Server v7 Administration console) Test

The Application Server (WebSphere Application Server v7 Administration console) test accesses the WebSphere Application Server on the application server.

Resources

The Application Server (WebSphere Application Server v7 Administration console) test uses the following resource:

- IBM Operational Decision Manageron the application serverWebSphere Application Server server server1

Problem determination

If the Application Server (WebSphere Application Server v7 Administration console) test fails, do the following to find and resolve the access problem.

Procedure

1. If running in the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use `isim` and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```
   b. To start the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```
   c. To stop the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a stop -c component -p topology_password
   ```
2. If running in the Command Center Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the server, specify `status` for *action* and `isim` for *component*.
   - To start the server, specify `start` for *action* and `isim` for *component*.
   - To stop the server, specify `stop` for *action* and `isim` for *component*.

   Specify your topology password for *topology_password*.
   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the application server review the following WebSphere Application Server logs:
   - Error log: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/server1/SystemErr.log`
   - Output log: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/server1/SystemOut.log`
   - Start log: `opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/se/startServer.log`
4. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that WebSphere Application Server is running.

a. Log on to a terminal session on the application server as the `ibmadmin` user.

b. Run the **`/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/serverStatus.sh server1`** command.

c. If WebSphere Application Server is not running, run the following command as the `ibmadmin` user on the application server (Field Edition) or application server 1 (Command Center Edition).

```
/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh server1
```

Alternately the DOPControl command can be used to start the `isim` component.

What to do next

Resolve any issues or errors found and retry the test.

Application Server (WebSphere Application Server v8 Administration console) Test

The Application Server (WebSphere Application Server v8 Administration console) test accesses the WebSphere Application Server on the application server.

Resources

The Application Server (WebSphere Application Server v8 Administration console) test uses the following resource:

- IBM Operational Decision Manageron the application serverWebSphere Application Server server dmgr

Problem determination

If the Application Server (WebSphere Application Server v8 Administration console) test fails, do the following to find and resolve the access problem.

Procedure

1. If running in the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use `appdmgr` and specify your topology password for *topology_password*.

   a. To check the status of the component run the following commands:

   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```

   b. To start the component run the following commands:

   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```

   c. To stop the component run the following commands:

   ```
   su - ibmadmin

   DOPControl -a stop -c component -p topology_password
   ```

2. If running in the Command Center Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.

   - To check the status of the server, specify `status` for *action* and `appdmgr` for *component*.
   - To start the server, specify `start` for *action* and `appdmgr` for *component*.
   - To stop the server, specify `stop` for *action* and `appdmgr` for *component*.

   Specify your topology password for *topology_password*.

```
su - ibmadmin
```

```
DOPControl -a action -c component -p topology_password
```

3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the application server review the following WebSphere Application Server logs:
      - Error log: `/opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemErr.log`
      - Output log: `/opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/SystemOut.log`
      - Start log: `opt/IBM/WebSphere/AppServer/profiles/dmgr/logs/dmgr/startServer.log`
4. Verify that the file system on the application server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that WebSphere Application Server is running.
   a. Log on to a terminal session on the application server as the `ibmadmin` user.

   b. Run the **/opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/serverStatus.sh dmgr** command.

   c. If WebSphere Application Server is not running, run the following command as the `ibmadmin` user on the application server (Field Edition) or application server 1 (Command Center Edition).

   ```
   /opt/IBM/WebSphere/AppServer/profiles/dmgr/bin/startServer.sh dmgr
   ```

   Alternately the DOPControl command can be used to start the `appdmgr` component.

What to do next

Resolve any issues or errors found and retry the test.

Application Server (WebSphere Application Server v8.5 Administration console) Test

The Application Server (WebSphere Application Server v8.5 Administration console) test accesses the WebSphere Application Server on the process server.

Resources

The Application Server (WebSphere Application Server v8.5 Administration console) test uses the following resource:

- IBM Operational Decision Manageron the process serverWebSphere Application Server server dmgr

Problem determination

If the Application Server (WebSphere Application Server v8.5 Administration console) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the server, specify `status` for *action* and `prodmgr` for *component*.

- To start the server, specify `start` for *action* and `prodmgr` for *component*.
- To stop the server, specify `stop` for *action* and `prodmgr` for *component*.

Specify your topology password for *topology_password*.

```
su - ibmadmin

DOPControl -a action -c component -p topology_password
```

2. Check that there is network connectivity between the application server) and the process server. This can be done by sending **ping** commands with both the short and fully-qualified host name of the process server from the application server and vice versa. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the application server review the following WebSphere Application Server logs:
      - Error log: `/opt/IBM/WebSphere/AppServer85/profiles/dmgr/logs/dmgr/SystemErr.log`
      - Output log: `/opt/IBM/WebSphere/AppServer85/profiles/dmgr/logs/dmgr/SystemOut.log`
      - Start log: `opt/IBM/WebSphere/AppServer85/profiles/dmgr/logs/dmgr/startServer.log`
4. Verify that the file system on the process server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that WebSphere Application Server is running.
   a. Log on to a terminal session on the process server as the `ibmadmin` user.

   b. Run the **/opt/IBM/WebSphere/AppServer85/profiles/dmgr/bin/serverStatus.sh dmgr** command.

   c. If WebSphere Application Server is not running, run the following command as the `ibmadmin` user on the process server.

   ```
   /opt/IBM/WebSphere/AppServer85/profiles/dmgr/bin/startServer.sh dmgr
   ```

   Alternately the DOPControl command can be used to start the `prodmgr` component.

What to do next

Resolve any issues or errors found and retry the test.

Collaboration (Lotus Domino console) Test

Collaboration (Lotus Domino console) test determines if the Domino Directory is accessible through its URL.

Resources

The Collaboration (Lotus Domino console) test uses the following resource:
- Domino Server (on the application server).

Problem determination

If the Collaboration (Lotus Domino console) test fails, do the following to find and resolve the problem.

Procedure

1. If running in a the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use `st` and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```
   b. To start the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```
   c. To stop the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a stop -c component -p topology_password
   ```
2. If running in the Command Center Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the server, specify `status` for *action* and `st` for *component*.
   - To start the server, specify `start` for *action* and `st` for *component*.
   - To stop the server, specify `stop` for *action* and `st` for *component*.

   Specify your topology password for *topology_password*.
   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
3. Review the log files for runtime exceptions.
   a. On the application server review the following Lotus Domino logs:
      - `/local/notesdata/console.out`
      - `/local/notesdata/log.nsf`
      - All logs in the `/local/notesdata/IBM_TECHNICAL_SUPPORT/` directory.
4. Verify that the file systems on the application server system have not reached capacity. This can be determined using the **`df -h`** command.
5. Verify that the Lotus Domino Process components are running.
   a. Login to the Lotus Domino Directory console at `http://`*`APP_SERVER_HOST`*`:84/names.nsf` where *APP_SERVER_HOST* is the host name of the application server. Login using the Domino administrator username and password.
   b. If the console cannot be accessed, on the application server, run the `ps -ef | grep notes` command to determine if the Lotus Domino processes are running. The Lotus Domino processes are:
      - server
      - event
      - update
      - replica
      - router
      - adminp
      - calconn
      - sched
      - http

- rnrmgr
- staddin

6. If some, but not all, processes are running, stop the running processes before restarting all the processes.
   a. On the application server, login as the `notes` user.
   b. Change to the `/local/notesdata` directory.
   c. Run the `"nohup /opt/IBM/lotus/bin/server -q >console.out 2>&1 &"` command to stop all running Lotus Domino processes.
   d. Check that all processes have stopped by running the `ps -ef | grep notes` command.
   e. If any Lotus Domino processes are still running, stop them using the **`kill -9`** *pid* where *pid* is the process identifier of the Lotus Domino process.
7. If the Lotus Domino processes are not running, start the Lotus Domino Server components.
   a. On the application server, login as the `notes` user.
   b. Change to the `/local/notesdata` directory.
   c. Run the `"nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &"` command to start all Lotus Domino Server components.

What to do next

Resolve any issues or errors found and retry the test.

Collaboration (Lotus Sametime console) Test

Collaboration (Lotus Sametime console) test determines if the Sametime Console is accessible through its URL.

Resources

The Collaboration (Lotus Sametime console) test uses the following resource:

- Sametime Server (on the application server).

Problem determination

If the Collaboration (Lotus Sametime console) test fails, do the following to find and resolve the problem.

Procedure

1. If running in the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use `st` and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```
   b. To start the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```
   c. To stop the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a stop -c component -p topology_password
   ```

2. If running in the Command Center Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the server, specify `status` for *action* and `st` for *component*.
   - To start the server, specify `start` for *action* and `st` for *component*.
   - To stop the server, specify `stop` for *action* and `st` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
3. Collect and review the Sametime Community Server configuration and log files.
   a. Log on the application server as a *notes* user.
   b. Change to the `/local/notesdata` directory.
   c. Run the `sh stdiagzip.sh` command. This command will collect all pertinent log files and write them to the `/local/notesdata/` directory.
   d. Review the logs in the `/local/notesdata/` directory.
4. Verify that the file systems on the application server system have not reached capacity. This can be determined using the **`df -h`** command.
5. Verify that the Sametime Process components are running.
   a. Login to the Sametime Home page at `http://`*`APP_SERVER_HOST`*`:84/stcenter.nsf` where *APP_SERVER_HOST* is the host name of the application server. Login using the Domino administrator username and password.
   b. On the Sametime Home page click **Administer the server**.
   c. On the Server - Overview page, make sure all the Sametime services are running.
6. If some, but not all, processes are running, stop the running processes before restarting all the processes.
   a. On the application server, login as the `notes` user.
   b. Change to the `/local/notesdata` directory.
   c. Run the `"nohup /opt/IBM/lotus/bin/server -q >console.out 2>&1 &"` command to stop all running Sametime processes.
   d. Check that all processes have stopped by running the `ps -ef | grep notes` command.
   e. If any processes are still running, stop them by using the **`kill -9`** *pid* where *pid* is the process identifier of the Lotus Domino process.
7. If the Sametime processes are not running, start the Lotus Sametime Server components.
   a. On the application server, login as the `notes` user.
   b. Change to the `/local/notesdata` directory.
   c. Run the `"nohup /opt/IBM/lotus/bin/server > console.out 2>&1 &"` command to start all Lotus Sametime Server components.

What to do next

Resolve any issues or errors found and retry the test.

Collaboration (Lotus Sametime Proxy console) Test

The Collaboration (Lotus Sametime Proxy console) test determines if the Lotus Sametime Proxy Web Application can be accessed by the Lotus Sametime Proxy Web Application URL.

Resources

The Collaboration (Lotus Sametime Proxy console) test uses the following resource:

- Sametime Proxy (on the application server).

Problem determination

If the Collaboration (Lotus Sametime Proxy console) test fails, do the following to find and resolve the access problem.

Procedure

1. If running in the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use `stproxy` and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
      ```
      su - ibmadmin

      DOPControl -a status -c component -p topology_password
      ```
   b. To start the component run the following commands:
      ```
      su - ibmadmin

      DOPControl -a start -c component -p topology_password
      ```
   c. To stop the component run the following commands:
      ```
      su - ibmadmin

      DOPControl -a stop -c component -p topology_password
      ```
2. If running in the Command Center Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the server, specify `status` for *action* and `stproxy` for *component*.
   - To start the server, specify `start` for *action* and `stproxy` for *component*.
   - To stop the server, specify `stop` for *action* and `stproxy` for *component*.

   Specify your topology password for *topology_password*.
   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
   b. On the application server review the following Sametime Proxy Server logs:
      - `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/logs/STProxyServer1/SystemErr.log`
4. Verify that the file systems on the application server system have not reached capacity. This can be determined using the **`df -h`** command.
5. Verify that the Sametime Proxy Server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the application server system log on as `ibmadmin`.
   b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/serverStatus.sh -all -username waswebadmin -password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.`is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.

d. If message `ADMU0509I: The Application Server "STProxyServer1" cannot be reached. It appears to be stopped.` is displayed, start STProxyServer1 using the following command: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/startServer.sh STProxyServer1`. Skip this step if message `ADMU0508I: The Application Server "STProxyServer1" is STARTED.` is displayed. If you had to start STProxyServer1, a message similar to the following will be displayed: `ADMU3000I: Server STProxyServer1 open for e-business; process id is 26654`.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. STProxyServer1

Stop servers in this order:

a. STProxyServer1

b. nodeagent

The STProxyServer1 server is stopped by running the following command in a command window on the Application Server: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopServer.sh STProxyServer1 -username waswebadmin -password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_PWD* is the WebSphere administrator password.

The nodeagent is stopped by running the following command in a command window on the Application Server: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopNode.sh -username waswebadmin -password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_PWD* is the WebSphere administrator password.

6. Verify that the Sametime Proxy Server is are started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.

b. View the status of the STProxyServer1 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/STProxyServer1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. STProxyServer1

Stop servers in this order:

a. STProxyServer1

b. nodeagent

To stop the STProxyServer1 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the Application Server: `/opt/IBM/WebSphere/AppServer/profiles/STPAppProfile1/bin/stopNode.sh -username waswebadmin -password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_PWD* is the WebSphere administrator password.

7. Verify that the Sametime Proxy Console can be accessed from the WebSphere Portal system, on the application server, using following URL: `http://`*`APPLICATION_SERVER_HOST`*`:9083/stwebclient/popup.jsp`. Where the *APPLICATION_SERVER_HOST* is host name for the application server.

What to do next

Resolve any issues or errors found and retry the test.

Database (DB2 Instance - Applications) Test

The Database (DB2 Instance - Applications) tests the DB2 manager status of the DB2 instance on the data server.

Resources

The Database (DB2 Instance - Applications) test uses the following resource:

- The DB2 Applications instance (on the data server)

Problem determination

If the Database (DB2 Instance - Applications) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the component and to start and stop it as needed. For *component* use `db24app` and specify your topology password for *topology_password*.

   a. To check the status of the component run the following commands:

   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```

   b. To start the component run the following commands:

   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```

   c. To stop the component run the following commands:

   ```
   su - ibmadmin

   DOPControl -a stop -c component -p topology_password
   ```

2. Check that there is network connectivity between the application server where the test was initiated and the data server where the database resides. This can be done by sending **`ping`** commands with both the short and fully-qualified host name of the data server from the application server. The results of the **`ping`** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.

3. Review the log files for runtime exceptions.

   a. On the application server review the following WebSphere Portal logs:

   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`

   - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log
4. Verify that the file system on the data server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the database manager used by the data server is started.
   a. On the data server, run the following command from a command window as the Applications instance user.
   ```
   db2 get snapshot for dbm | grep "Database manager status"
   ```
   If the database manager is started for the Applications instance, the following message is displayed: `Database manager status = Active`.
6. If the DB2 processes are not running, start them by running **su - db2inst2** from the command window if running as the `root` user. Otherwise, run **db2start** to start the Database Manager.
7. Check the DB2 logs for errors related to the database instance used for this test. The logs are located on the data server in the `/datahome/db2inst2/sqllib/db2dump` directory. Check the `db2diag.log` in the `/datahome/db2inst2/sqllib/db2dump` directory for errors issued when starting the database used for this test.

What to do next

Resolve any issues or errors found and retry the test.

Database (DB2 Instance - Applications) [1] Test

The Database (DB2 Instance - Applications) [1] tests the DB2 manager status of the DB2 instance on data server 1.

Resources

The Database (DB2 Instance - Applications) [1] test uses the following resource:

- The DB2 Applications instance (on the data server)

Problem determination

If the Database (DB2 Instance - Applications) [1] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of the primary server, specify `status` for *action* and `db24apppri` for *component*.
   - To check the status of the standby server, specify `status` for *action* and `db24appsby` for *component*.
   - To start the primary server, specify `start` for *action* and `db24apppri` for *component*.
   - To start the standby server, specify `start` for *action* and `db24appsby` for *component*.
   - To stop the primary server, specify `stop` for *action* and `db24apppri` for *component*.
   - To stop the standby server, specify `stop` for *action* and `db24appsby` for *component*.

   Specify your topology password for *topology_password*.
   ```
   su - ibmadmin
   ```
   ```
   DOPControl -a action -c component -p topology_password
   ```
2. Check that there is network connectivity between the application server where the test was initiated and the data server where the database resides. This can be done by sending **ping** commands with

both the short and fully-qualified host name of the data server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or /etc/hosts file.

3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log
4. Verify that the file system on the data server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the database manager used by the data server is started.
   a. On the data server, run the following command from a command window as the Applications instance user.

      ```
      db2 get snapshot for dbm | grep "Database manager status"
      ```

      If the database manager is started for the Applications instance, the following message is displayed: Database manager status = Active.
6. If the DB2 processes are not running, start them by running **su - db2inst2** from the command window if running as the root user. Otherwise, run **db2start** to start the Database Manager.
7. Check the DB2 logs for errors related to the database instance used for this test. The logs are located on the data server in the /datahome/db2inst2/sqllib/db2dump directory. Check the db2diag.log in the /datahome/db2inst2/sqllib/db2dump directory for errors issued when starting the database used for this test.

What to do next

Resolve any issues or errors found and retry the test.

Database (DB2 Instance - Applications) [2] Test

The Database (DB2 Instance - Applications) [2] tests the DB2 manager status of the DB2 instance on data server 2.

Resources

The Database (DB2 Instance - Applications) [2] test uses the following resource:

- The DB2 Applications instance (on the data server)

Problem determination

If the Database (DB2 Instance - Applications) [2] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of the primary server, specify status for *action* and db24apppri for *component*.
   - To check the status of the standby server, specify status for *action* and db24appsby for *component*.

- To start the primary server, specify `start` for *action* and `db24apppri` for *component*.
- To start the standby server, specify `start` for *action* and `db24appsby` for *component*.
- To stop the primary server, specify `stop` for *action* and `db24apppri` for *component*.
- To stop the standby server, specify `stop` for *action* and `db24appsby` for *component*.

Specify your topology password for *topology_password*.

```
su - ibmadmin

DOPControl -a action -c component -p topology_password
```

2. Check that there is network connectivity between the application server where the test was initiated and the data server where the database resides. This can be done by sending **ping** commands with both the short and fully-qualified host name of the data server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
4. Verify that the file system on the data server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the database manager used by the data server is started.
   a. On the data server, run the following command from a command window as the Applications instance user.

      ```
      db2 get snapshot for dbm | grep "Database manager status"
      ```

      If the database manager is started for the Applications instance, the following message is displayed: `Database manager status = Active`.
6. If the DB2 processes are not running, start them by running **su - db2inst2** from the command window if running as the `root` user. Otherwise, run **db2start** to start the Database Manager.
7. Check the DB2 logs for errors related to the database instance used for this test. The logs are located on the data server in the `/datahome/db2inst2/sqllib/db2dump` directory. Check the `db2diag.log` in the `/datahome/db2inst2/sqllib/db2dump` directory for errors issued when starting the database used for this test.

What to do next

Resolve any issues or errors found and retry the test.

Database (DB2 Instance - Directory Server) Test

The Database (DB2 Instance - Directory Server) tests the DB2 manager status of the DB2 instance on the data server.

Resources

The Database (DB2 Instance - Directory Server) test uses the following resource:
- The DB2 Directory Server instance (on the data server)

Problem determination

If the Database (DB2 Instance - Directory Server) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the component and to start and stop it as needed. For *component* use db and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```
   b. To start the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```
   c. To stop the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a stop -c component -p topology_password
   ```
2. Check that there is network connectivity between the application server where the test was initiated and the data server where the database resides. This can be done by sending **ping** commands with both the short and fully-qualified host name of the data server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or /etc/hosts file.
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log
4. Verify that the file system on the data server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the database manager used by the data server is started.
   a. On the data server, run the following command from a command window as the Directory Server instance user.
   ```
   db2 get snapshot for dbm | grep "Database manager status"
   ```
   If the database manager is started for the Directory Server instance, the following message is displayed: Database manager status = Active.
6. If the DB2 processes are not running, start them by running **su - dsrdbm01** from the command window if running as the root user. Otherwise, run **db2start** to start the Database Manager.
7. Check the DB2 logs for errors related to the database instance used for this test. The logs are located on the data server in the /datahome/dsrdbm01/sqllib/db2dump directory.
8. Check the db2diag.log for errors issued when starting the database used for this test.

What to do next

Resolve any issues or errors found and retry the test.

Database (DB2 Instance - Directory Server) [1] Test

The Database (DB2 Instance - Directory Server) [1]tests the DB2 manager status of the DB2 instance on data server 1.

Resources

The Database (DB2 Instance - Directory Server) [1] test uses the following resource:

- The DB2 Directory Server instance (on the data server)

Problem determination

If the Database (DB2 Instance - Directory Server) [1] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of the primary server, specify `status` for *action* and `tdspri` for *component*.
   - To check the status of the standby server, specify `status` for *action* and `tdssby` for *component*.
   - To start the primary server, specify `start` for *action* and `tdspri` for *component*.
   - To start the standby server, specify `start` for *action* and `tdssby` for *component*.
   - To stop the primary server, specify `stop` for *action* and `tdspri` for *component*.
   - To stop the standby server, specify `stop` for *action* and `tdssby` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Check that there is network connectivity between the application server where the test was initiated and the data server where the database resides. This can be done by sending **ping** commands with both the short and fully-qualified host name of the data server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
4. Verify that the file system on the data server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the database manager used by the data server is started.
   a. On the data server, run the following command from a command window as the Directory Server instance user.

   ```
   db2 get snapshot for dbm | grep "Database manager status"
   ```

   If the database manager is started for the Directory Server instance, the following message is displayed: `Database manager status = Active`.
6. If the DB2 processes are not running, start them by running **su - dsrdbm01** from the command window if running as the `root` user. Otherwise, run **db2start** to start the Database Manager.
7. Check the DB2 logs for errors related to the database instance used for this test. The logs are located on the data server in the `/datahome/dsrdbm01/sqllib/db2dump` directory.

8. Check the `db2diag.log` for errors issued when starting the database used for this test.

What to do next

Resolve any issues or errors found and retry the test.

Database (DB2 Instance - Directory Server) [2] Test

The Database (DB2 Instance - Directory Server) [2] tests the DB2 manager status of the DB2 instance on data server 2.

Resources

The Database (DB2 Instance - Directory Server) [2] test uses the following resource:

- The DB2 Directory Server instance (on the data server)

Problem determination

If the Database (DB2 Instance - Directory Server) [2] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of the primary server, specify `dbpri` for *action* and `tdspri` for *component*.
   - To check the status of the standby server, specify `dbsby` for *action* and `tdspri` for *component*.
   - To start the primary server, specify `dbpri` for *action* and `tdspri` for *component*.
   - To start the standby server, specify `dbsby` for *action* and `tdspri` for *component*.
   - To stop the primary server, specify `dbpri` for *action* and `tdspri` for *component*.
   - To stop the standby server, specify `dbsby` for *action* and `tdspri` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Check that there is network connectivity between the application server where the test was initiated and the data server where the database resides. This can be done by sending **`ping`** commands with both the short and fully-qualified host name of the data server from the application server. The results of the **`ping`** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
4. Verify that the file system on the data server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the database manager used by the data server is started.

a. On the data server, run the following command from a command window as the Directory Server instance user.

```
db2 get snapshot for dbm | grep "Database manager status"
```

If the database manager is started for the Directory Server instance, the following message is displayed: `Database manager status = Active`.

6. If the DB2 processes are not running, start them by running **`su - dsrdbm01`** from the command window if running as the `root` user. Otherwise, run **`db2start`** to start the Database Manager.
7. Check the DB2 logs for errors related to the database instance used for this test. The logs are located on the data server in the `/datahome/dsrdbm01/sqllib/db2dump` directory.
8. Check the `db2diag.log` for errors issued when starting the database used for this test.

What to do next

Resolve any issues or errors found and retry the test.

Database (DB2 Instance - Middleware) Test

The Database (DB2 Instance - Middleware) tests the DB2 manager status of the DB2 instance on the data server.

Resources

The Database (DB2 Instance - Middleware) test uses the following resource:

- The DB2 Middleware instance (on the data server)

Problem determination

If the Database (DB2 Instance - Middleware) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the component and to start and stop it as needed. For *component* use `db24mid` and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:

   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```

   b. To start the component run the following commands:

   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```

   c. To stop the component run the following commands:

   ```
   su - ibmadmin

   DOPControl -a stop -c component -p topology_password
   ```

2. Check that there is network connectivity between the application server where the test was initiated and the data server where the database resides. This can be done by sending **`ping`** commands with both the short and fully-qualified host name of the data server from the application server. The results of the **`ping`** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`

- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log

4. Verify that the file system on the data server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the database manager used by the data server is started.
   a. On the data server, run the following command from a command window as the Middleware instance user.

   ```
   db2 get snapshot for dbm | grep "Database manager status"
   ```

   If the database manager is started for the Middleware instance, the following message is displayed: Database manager status = Active.
6. If the DB2 processes are not running, start them by running **su - db2inst1** from the command window if running as the root user. Otherwise, run **db2start** to start the Database Manager.
7. Check the DB2 logs for errors related to the database instance used for this test. The logs are located on the data server in the /datahome/db2inst1/sqllib/db2dump directory.
8. Check the db2diag.log for errors issued when starting the database used for this test.

What to do next

Resolve any issues or errors found and retry the test.

Database (DB2 Instance - Middleware) [1] Test

The Database (DB2 Instance - Middleware) [1] tests the DB2 manager status of the DB2 instance on data server 1.

Resources

The Database (DB2 Instance - Middleware) [1] test uses the following resource:

- The DB2 Middleware instance (on the data server)

Problem determination

If the Database (DB2 Instance - Middleware) [1] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of the primary server, specify status for *action* and db24midpri for *component*.
   - To check the status of the standby server, specify status for *action* and db24midsby for *component*.
   - To start the primary server, specify start for *action* and db24midpri for *component*.
   - To start the standby server, specify start for *action* and db24midsby for *component*.
   - To stop the primary server, specify stop for *action* and db24midpri for *component*.
   - To stop the standby server, specify stop for *action* and db24midsby for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Check that there is network connectivity between the application server where the test was initiated and the data server where the database resides. This can be done by sending **ping** commands with

both the short and fully-qualified host name of the data server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or /etc/hosts file.

3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log
4. Verify that the file system on the data server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the database manager used by the data server is started.
   a. On the data server, run the following command from a command window as the Middleware instance user.

      ```
      db2 get snapshot for dbm | grep "Database manager status"
      ```

      If the database manager is started for the Middleware instance, the following message is displayed: Database manager status = Active.
6. If the DB2 processes are not running, start them by running **su - db2inst1** from the command window if running as the root user. Otherwise, run **db2start** to start the Database Manager.
7. Check the DB2 logs for errors related to the database instance used for this test. The logs are located on the data server in the /datahome/db2inst1/sqllib/db2dump directory.
8. Check the db2diag.log for errors issued when starting the database used for this test.

What to do next

Resolve any issues or errors found and retry the test.

Database (DB2 Instance - Middleware) [2] Test

The Database (DB2 Instance - Middleware) [2]tests the DB2 manager status of the DB2 instance on data server 2.

Resources

The Database (DB2 Instance - Middleware) [2] test uses the following resource:

- The DB2 Middleware instance (on the data server)

Problem determination

If the Database (DB2 Instance - Middleware) [2] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of the primary server, specify status for *action* and db24midpri for *component*.
   - To check the status of the standby server, specify status for *action* and db24midsby for *component*.

- To start the primary server, specify `start` for *action* and `db24midpri` for *component*.
- To start the standby server, specify `start` for *action* and `db24midsby` for *component*.
- To stop the primary server, specify `stop` for *action* and `db24midpri` for *component*.
- To stop the standby server, specify `stop` for *action* and `db24midsby` for *component*.

Specify your topology password for *topology_password*.

```
su - ibmadmin

DOPControl -a action -c component -p topology_password
```

2. Check that there is network connectivity between the application server where the test was initiated and the data server where the database resides. This can be done by sending **ping** commands with both the short and fully-qualified host name of the data server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
4. Verify that the file system on the data server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the database manager used by the data server is started.
   a. On the data server, run the following command from a command window as the Middleware instance user.

      ```
      db2 get snapshot for dbm | grep "Database manager status"
      ```

      If the database manager is started for the Middleware instance, the following message is displayed: `Database manager status = Active`.
6. If the DB2 processes are not running, start them by running **su - db2inst1** from the command window if running as the `root` user. Otherwise, run **db2start** to start the Database Manager.
7. Check the DB2 logs for errors related to the database instance used for this test. The logs are located on the data server in the `/datahome/db2inst1/sqllib/db2dump` directory.
8. Check the `db2diag.log` for errors issued when starting the database used for this test.

What to do next

Resolve any issues or errors found and retry the test.

Database (System Verification Check Scheduler) Test

The Database (System Verification Check Scheduler) tests the DB2 manager status of the *database name* DB2 instance on the data server.

Resources

The Database (System Verification Check Scheduler) test uses the following resource:

- The Application DB2 instance (on the data server)

Problem determination

If the Database (System Verification Check Scheduler) test fails, do the following to find and resolve the access problem.

Procedure

1. If running in the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use `db24mid` and specify your topology password for *topology_password*.
   1. To check the status of the component run the following commands:

      ```
      su - ibmadmin

      DOPControl -a status -c component -p topology_password
      ```
   2. To start the component run the following commands:

      ```
      su - ibmadmin

      DOPControl -a start -c component -p topology_password
      ```
   3. To stop the component run the following commands:

      ```
      su - ibmadmin

      DOPControl -a stop -c component -p topology_password
      ```
2. If running in the Command Center Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the server, specify `status` for *action* and `db24apppri` for *component*.
   - To start the server, specify `start` for *action* and `db24apppri` for *component*.
   - To stop the server, specify `stop` for *action* and `db24apppri` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
3. Check that there is network connectivity between the application server where the test was initiated and the data server where the database resides. This can be done by sending **`ping`** commands with both the short and fully-qualified host name of the data server from the application server. The results of the **`ping`** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
4. Review the log files for runtime exceptions.
   1. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
5. Verify that the file system on the data server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
6. Verify that the database manager used by the data server is started.
   1. On the data server, run the following command from a command window as the Applications DB2 instance user (db2inst2).

      ```
      db2 get snapshot for dbm | grep "Database manager status"
      ```

      If the database manager is started for the *database name* instance, the following message is displayed: `Database manager status = Active`.

7. If the DB2 processes are not running, start them by running **su - db2inst2** from the command window if running as the root user. Otherwise, run **db2start** to start the Database Manager.
8. Check the DB2 logs for errors related to the database instance used for this test. The logs are located on the data server in the /datahome/db2inst2/sqllib/db2dump directory. Check the db2diag.log in the /datahome/db2inst2/sqllib/db2dump directory for errors issued when starting the database used for this test.

What to do next

Resolve any issues or errors found and retry the test.

Decision Management (WebSphere Operational Decision Management Decision Center console) Test

The Decision Management (WebSphere Operational Decision Management Decision Center console) test determines the status of the WebSphere Operational Decision Management Decision Center server.

Resources

The Decision Management (WebSphere Operational Decision Management Decision Center console) test uses the following resources:

- WebSphere Operational Decision Management on the process server.
- WebSphere Application Server server odmdc1

Problem determination

If the Decision Management (WebSphere Operational Decision Management Decision Center console) test fails, do the following to find and resolve the problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the WebSphere Operational Decision Management server, specify status for *action* and odm for *component*.
   - To start the WebSphere Operational Decision Management server, specify start for *action* and odm for *component*.
   - To stop the WebSphere Operational Decision Management server, specify stop for *action* and odm for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Check that there is network connectivity between the application server and the process server. This can be done by sending **ping** commands with both the short and fully-qualified host name of the process server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or /etc/hosts file.
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log

   - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log

   c. On the process server review the following WebSphere Application Server logs:
      - Error log: /opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/logs/odmdc1/SystemErr.log
      - Output log:/opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/logs/odmdc1/SystemOut.log
      - Start log: /opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/logs/odmdc1/startServer.log

4. Verify that the file system on the process server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the WebSphere Application Server server odmdc1 is running.
   a. Log on to a terminal session on the process server as the ibmadmin user.
   b. Run the **/opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1/bin/serverStatus.sh odmdc1** command.

Decision Management (WebSphere Operational Decision Management Rule Execution Server console) Test

The Decision Management (WebSphere Operational Decision Management Rule Execution Server console) test determines the status of the WebSphere Operational Decision Management Rule Execution server.

Resources

The Decision Management (WebSphere Operational Decision Management Rule Execution Server console) test uses the following resources:

- WebSphere Operational Decision Management on the process server.
- WebSphere Application Server server odmServer1

Problem determination

If the Decision Management (WebSphere Operational Decision Management Rule Execution Server console) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the WebSphere Operational Decision Management server, specify status for *action* and odm for *component*.
   - To start the WebSphere Operational Decision Management server, specify start for *action* and odm for *component*.
   - To stop the WebSphere Operational Decision Management server, specify stop for *action* and odm for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Check that there is network connectivity between the application server and the process server. This can be done by sending **ping** commands with both the short and fully-qualified host name of the process server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or /etc/hosts file.

3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
   c. On the process server review the following WebSphere Application Server logs:
      - Error log: `/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/logs/odmServer1/SystemErr.log`
      - Output log:`/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/logs/odmServer1/SystemOut.log`
      - Start log: `/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/logs/odmServer1/startServer.log`
4. Verify that the file system on the process server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the WebSphere Application Server server odmServer1 is running.
   a. Log on to a terminal session on the process server as the `ibmadmin` user.
   b. Run the **`/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1/bin/serverStatus.sh odmServer1`** command.

Directory (Tivoli Directory Server) Test

The Directory (Tivoli Directory Server) test determines if the Tivoli Directory Server is available by sending an HTTP request to the server.

Resources

The Directory (Tivoli Directory Server) test uses the following resource:

- Tivoli Directory Server (on the data server)

Problem determination

If the Directory (Tivoli Directory Server) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the component and to start and stop it as needed. For *component* use `tds` and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
      ```
      su - ibmadmin

      DOPControl -a status -c component -p topology_password
      ```
   b. To start the component run the following commands:
      ```
      su - ibmadmin

      DOPControl -a start -c component -p topology_password
      ```
   c. To stop the component run the following commands:

```
su - ibmadmin
```

```
DOPControl -a stop -c component -p topology_password
```

2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
3. Verify that the file system on the data server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the Tivoli Directory Server LDAP server is running.
   a. Log on to a terminal session on data server 1 data server as `root`.
   b. Run the **ps -ef | grep ibmslapd** command. The results will be similar to the following:

      ```
      dsrdbm01 13797     1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
      root     32080 19149  0 23:17 pts/1    00:00:00 grep ibmslapd
      ```

      This example shows that the Tivoli Directory Server daemon, ibmslapd, is running.
   c. Run the **ps -ef | grep ibmdiradm** command. The results will be similar to the following:

      ```
      root      4394 14038  0 14:17 pts/2    00:00:00 grep ibmdiradm
      dsrdbm01 11055     1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
      ```

      This example shows that the Tivoli Directory Server daemon, ibmdiradm, is running.
5. If the Tivoli Directory Server, ibmslapd, is not running, do the following.
   a. As a *root* Linux user, run **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01** to start the Directory Server
6. If the Tivoli Directory Administration Server, ibmdiradm, is not running, do the following.
   a. On a terminal session on the data server, run **su - dsrdbm01**.
   b. Run **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t** to start the application server.
7. If the Tivoli Directory Server, ibmslapd, is running, do the following.

   Note: Do this step even if the Tivoli Directory Server was started in the previous step.
   a. Log on to a terminal session on the data server as dsrdbm01.
   b. Run **idsldapsearch -h localhost -D "cn=root" -w "***ADMIN_PASSWORD***" -s sub uid=*** where *ADMIN_PASSWORD* is the LDAP Root Administrator account password. The existing LDAP user objects will be displayed.
8. Verify that the Tivoli Directory Server Web Administration Tool is running. The Tivoli Directory Server Web Administration Tool is used to stop and start the LDAP instance, add users or accounts, and view log files.
   a. Log on to a terminal session on the application server as `ibmadmin`.
   b. Run the **/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/serverStatus.sh -all -username waswebadmin -password** *WAS_ADMIN_PASSWORD* command on the application server where *WAS_ADMIN_PASSWORD* is the WebSphere Application Server administrator password. If the tool is running, a message similar to the following will be returned.

      ```
      ADMU0508I: The Application Server "tdsServer" is STARTED
      ```

      If the following message is returned, the tdsServer needs to be started.

      ```
      ADMU0509I: The Application Server "tdsServer" cannot be reached. It appears to be stopped.
      ```
   c. Start the tdsServer by running the **/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh tdsServer** command. The server, tdsServer, will start and a message similar to the following will be displayed.

      ```
      ADMU3000I: Server tdsServer open for e-business; process id is 26654
      ```

9. Access the Tivoli Directory Server Web Administration Tool at: `http://APPLICATION_SERVER_HOST:9081/IDSWebApp` where *APPLICATION_SERVER_HOST* is the host name of the application server.
10. Log on with the LDAP Root Administrator Account, cn=root, and the appropriate password. The LDAP Server name should be `DATABASE_DIRECTORY_SERVER_HOST:389` where *DATABASE_DIRECTORY_SERVER_HOST* is the host name of the data server.
11. Click **Server Administration** > **Start/stop/reset server**. The LDAP server status will be displayed. This page can also be used to start, stop, or reset the LDAP server.

What to do next

Resolve any issues or errors found and retry the test.

Directory (Tivoli Directory Server) [1] Test

The Directory (Tivoli Directory Server) [1] test determines if the Tivoli Directory Server is available by sending an HTTP request to the server.

Resources

The Directory (Tivoli Directory Server) [1] test uses the following resource:

- Tivoli Directory Server (on the data server)

Problem determination

If the Directory (Tivoli Directory Server) [1] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of the primary server, specify `status` for *action* and `tdspri` for *component*.
   - To check the status of the standby server, specify `status` for *action* and `tdssby` for *component*.
   - To start the primary server, specify `start` for *action* and `tdspri` for *component*.
   - To start the standby server, specify `start` for *action* and `tdssby` for *component*.
   - To stop the primary server, specify `stop` for *action* and `tdspri` for *component*.
   - To stop the standby server, specify `stop` for *action* and `tdssby` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. On the data server review the following Tivoli Directory Server log: `/datahome/dsrdbm01/idsslapd-dsrdbm01/logs/audit.log`
3. Verify that the file system on the data server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the Tivoli Directory Server LDAP server is running.

a. Log on to a terminal session on data server 1 data server as `root`.

b. Run the **`ps -ef | grep ibmslapd`** command. The results will be similar to the following:

```
dsrdbm01 13797     1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
root     32080 19149  0 23:17 pts/1    00:00:00 grep ibmslapd
```

This example shows that the Tivoli Directory Server daemon, ibmslapd, is running.

c. Run the **`ps -ef | grep ibmdiradm`** command. The results will be similar to the following:

```
root      4394 14038  0 14:17 pts/2    00:00:00 grep ibmdiradm
dsrdbm01 11055     1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
```

This example shows that the Tivoli Directory Server daemon, ibmdiradm, is running.

5. If the Tivoli Directory Server, ibmslapd, is not running, do the following.

   a. As a *root* Linux user, run **`/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01`** to start the Directory Server

6. If the Tivoli Directory Administration Server, ibmdiradm, is not running, do the following.

   a. On a terminal session on the data server, run **`su - dsrdbm01`**.

   b. Run **`/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t`** to start the application server.

7. If the Tivoli Directory Server, ibmslapd, is running, do the following.

   Note: Do this step even if the Tivoli Directory Server was started in the previous step.

   a. Log on to a terminal session on the data server as dsrdbm01.

   b. Run **`idsldapsearch -h localhost -D "cn=root" -w "`***ADMIN_PASSWORD***`" -s sub uid=*`** where *ADMIN_PASSWORD* is the LDAP Root Administrator account password. The existing LDAP user objects will be displayed.

8. Verify that the Tivoli Directory Server Web Administration Tool is running. The Tivoli Directory Server Web Administration Tool is used to stop and start the LDAP instance, add users or accounts, and view log files.

   a. Log on to a terminal session on the application server as `ibmadmin`.

   b. Run the **`/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/serverStatus.sh -all -username waswebadmin -password`** *WAS_ADMIN_PASSWORD* command on the application server where *WAS_ADMIN_PASSWORD* is the WebSphere Application Server administrator password. If the tool is running, a message similar to the following will be returned.

   ```
   ADMU0508I: The Application Server "tdsServer" is STARTED
   ```

   If the following message is returned, the tdsServer needs to be started.

   ```
   ADMU0509I: The Application Server "tdsServer" cannot be reached. It appears to be stopped.
   ```

   c. Start the tdsServer by running the **`/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh tdsServer`** command. The server, tdsServer, will start and a message similar to the following will be displayed.

   ```
   ADMU3000I: Server tdsServer open for e-business; process id is 26654
   ```

9. Access the Tivoli Directory Server Web Administration Tool at: `http://`*`APPLICATION_SERVER_HOST`*`:9081/IDSWebApp` where *APPLICATION_SERVER_HOST* is the host name of the application server.

10. Log on with the LDAP Root Administrator Account, cn=root, and the appropriate password. The LDAP Server name should be *`DATABASE_DIRECTORY_SERVER_HOST`*`:389` where *DATABASE_DIRECTORY_SERVER_HOST* is the host name of the data server.

11. Click **Server Administration** > **Start/stop/reset server**. The LDAP server status will be displayed. This page can also be used to start, stop, or reset the LDAP server.

What to do next

Resolve any issues or errors found and retry the test.

Directory (Tivoli Directory Server) [2] Test

The Directory (Tivoli Directory Server) [2] test determines if the Tivoli Directory Server is available by sending an HTTP request to the server.

Resources

The Directory (Tivoli Directory Server) [2] test uses the following resource:

- Tivoli Directory Server (on the backup data server)

Problem determination

If the Directory (Tivoli Directory Server) [2] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of the primary server, specify `status` for *action* and `tdspri` for *component*.
   - To check the status of the standby server, specify `status` for *action* and `tdssby` for *component*.
   - To start the primary server, specify `start` for *action* and `tdspri` for *component*.
   - To start the standby server, specify `start` for *action* and `tdssby` for *component*.
   - To stop the primary server, specify `stop` for *action* and `tdspri` for *component*.
   - To stop the standby server, specify `stop` for *action* and `tdssby` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the data server review the following Tivoli Directory Server log: `/datahome/dsrdbm01/idsslapd-dsrdbm01/logs/audit.log`
3. Verify that the file system on the data server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the Tivoli Directory Server LDAP server is running.
   a. Log on to a terminal session on data server 2 as `root`.

   b. Run the **`ps -ef | grep ibmslapd`** command. The results will be similar to the following:

      ```
      dsrdbm01 13797     1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
      root     32080 19149  0 23:17 pts/1    00:00:00 grep ibmslapd
      ```

      This example shows that the Tivoli Directory Server daemon, ibmslapd, is running.

   c. Run the **`ps -ef | grep ibmdiradm`** command. The results will be similar to the following:

      ```
      root      4394 14038  0 14:17 pts/2    00:00:00 grep ibmdiradm
      dsrdbm01 11055     1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
      ```

      This example shows that the Tivoli Directory Server daemon, ibmdiradm, is running.

5. If the Tivoli Directory Server, ibmslapd, is not running, do the following.
   a. As a *root* Linux user, run **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01** to start the Directory Server
6. If the Tivoli Directory Administration Server, ibmdiradm, is not running, do the following.
   a. On a terminal session on data server 2, run **su - dsrdbm01**.
   b. Run **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t** to start the application server.
7. If the Tivoli Directory Server, ibmslapd, is running, do the following.

   Note: Do this step even if the Tivoli Directory Server was started in the previous step.
   a. Log on to a terminal session on the data server as dsrdbm01.
   b. Run **idsldapsearch -h localhost -D "cn=root" -w "***ADMIN_PASSWORD***" -s sub uid=*** where *ADMIN_PASSWORD* is the LDAP Root Administrator account password. The existing LDAP user objects will be displayed.
8. Verify that the Tivoli Directory Server Web Administration Tool is running. The Tivoli Directory Server Web Administration Tool is used to stop and start the LDAP instance, add users or accounts, and view log files.
   a. Log on to a terminal session on application server 2 as `ibmadmin`.
   b. Run the **/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/serverStatus.sh -all -username waswebadmin -password** *WAS_ADMIN_PASSWORD* command on application server 2 where *WAS_ADMIN_PASSWORD* is the WebSphere Application Server administrator password. If the tool is running, a message similar to the following will be returned.

      ```
      ADMU0508I: The Application Server "tdsServer" is STARTED
      ```

      If the following message is returned, the tdsServer needs to be started.

      ```
      ADMU0509I: The Application Server "tdsServer" cannot be reached. It appears to be stopped.
      ```
   c. Start the tdsServer by running the **/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh tdsServer** command. The server, tdsServer, will start and a message similar to the following will be displayed.

      ```
      ADMU3000I: Server tdsServer open for e-business; process id is 26654
      ```
9. Access the Tivoli Directory Server Web Administration Tool at: `http://`*`APPLICATION_SERVER_HOST`*`:9081/IDSWebApp` where *APPLICATION_SERVER_HOST* is the host name of the application server.
10. Log on with the LDAP Root Administrator Account, cn=root, and the appropriate password. The LDAP Server name should be *`DATABASE_DIRECTORY_SERVER_HOST`*`:389` where *DATABASE_DIRECTORY_SERVER_HOST* is the host name of the backup data server.
11. Click **Server Administration** > **Start/stop/reset server**. The LDAP server status will be displayed. This page can also be used to start, stop, or reset the LDAP server.

What to do next

Resolve any issues or errors found and retry the test.

Directory (Tivoli Directory Server console) Test

The Directory (Tivoli Directory Server console) test determines if the Tivoli Directory Server is available by sending an HTTP request to the server.

Resources

The Directory (Tivoli Directory Server console) test uses the following resource:
- Tivoli Directory Server (on the data server)

Problem determination

If the Directory (Tivoli Directory Server console) test fails, do the following to find and resolve the access problem.

Procedure

1. If running in the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use `tds` and specify your topology password for *topology_password*.
   1. To check the status of the component run the following commands:
      ```
      su - ibmadmin

      DOPControl -a status -c component -p topology_password
      ```
   2. To start the component run the following commands:
      ```
      su - ibmadmin

      DOPControl -a start -c component -p topology_password
      ```
   3. To stop the component run the following commands:
      ```
      su - ibmadmin

      DOPControl -a stop -c component -p topology_password
      ```
2. If running in a high availability environment, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the server, specify `status` for *action* and `tds` for *component*.
   - To start the server, specify `start` for *action* and `tds` for *component*.
   - To stop the server, specify `stop` for *action* and `tds` for *component*.

   Specify your topology password for *topology_password*.
   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
3. Review the log files for runtime exceptions.
   1. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
4. Verify that the file system on the data server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the Tivoli Directory Server LDAP server is running.
   1. Log on to a terminal session on data server 1 data server as `root`.
   2. Run the **`ps -ef | grep ibmslapd`** command. The results will be similar to the following:
      ```
      dsrdbm01 13797     1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
      root     32080 19149  0 23:17 pts/1    00:00:00 grep ibmslapd
      ```
      This example shows that the Tivoli Directory Server daemon, ibmslapd, is running.
   3. Run the **`ps -ef | grep ibmdiradm`** command. The results will be similar to the following:
      ```
      root      4394 14038  0 14:17 pts/2    00:00:00 grep ibmdiradm
      dsrdbm01 11055     1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
      ```
      This example shows that the Tivoli Directory Server daemon, ibmdiradm, is running.
6. If the Tivoli Directory Server, ibmslapd, is not running, do the following.
   1. As a *root* Linux user, run **`/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01`** to start the Directory Server

7. If the Tivoli Directory Administration Server, ibmdiradm, is not running, do the following.
   a. On a terminal session on the data server, run **su - dsrdbm01**.
   b. Run **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t** to start the application server.
8. If the Tivoli Directory Server, ibmslapd, is running, do the following.

   Note: Do this step even if the Tivoli Directory Server was started in the previous step.
   a. Log on to a terminal session on the data server as dsrdbm01.
   b. Run `idsldapsearch -h localhost -D "cn=root" -w "ADMIN_PASSWORD" -s sub uid=*` where *ADMIN_PASSWORD* is the LDAP Root Administrator account password. The existing LDAP user objects will be displayed.
9. Verify that the Tivoli Directory Server Web Administration Tool is running. The Tivoli Directory Server Web Administration Tool is used to stop and start the LDAP instance, add users or accounts, and view log files.
   a. Log on to a terminal session on the application server as ibmadmin.
   b. Run the **/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/serverStatus.sh -all -username waswebadmin -password** *WAS_ADMIN_PASSWORD* command on the application server where *WAS_ADMIN_PASSWORD* is the WebSphere Application Server administrator password. If the tool is running, a message similar to the following will be returned.

      ```
      ADMU0508I: The Application Server "tdsServer" is STARTED
      ```

      If the following message is returned, the tdsServer needs to be started.

      ```
      ADMU0509I: The Application Server "tdsServer" cannot be reached. It appears to be stopped.
      ```

   c. Start the tdsServer by running the **/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh tdsServer** command. The server, tdsServer, will start and a message similar to the following will be displayed.

      ```
      ADMU3000I: Server tdsServer open for e-business; process id is 26654
      ```

10. Access the Tivoli Directory Server Web Administration Tool at: http://*APPLICATION_SERVER_HOST*:9081/IDSWebApp where *APPLICATION_SERVER_HOST* is the host name of the application server.
11. Log on with the LDAP Root Administrator Account, cn=root, and the appropriate password. The LDAP Server name should be *DATABASE_DIRECTORY_SERVER_HOST*:389 where *DATABASE_DIRECTORY_SERVER_HOST* is the host name of the data server.
12. Click **Server Administration** > **Start/stop/reset server**. The LDAP server status will be displayed. This page can also be used to start, stop, or reset the LDAP server.

What to do next

Resolve any issues or errors found and retry the test.

Directory (Tivoli Directory Server Proxy) Test

The Directory (Tivoli Directory Server Proxy) test determines if the Tivoli Directory Server is available by sending an HTTP request to the server.

Resources

The Directory (Tivoli Directory Server Proxy) test uses the following resource:
- Tivoli Directory Server (on the messaging server)

Problem determination

If the Directory (Tivoli Directory Server Proxy) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the server, specify `status` for *action* and `tdsproxy4app` for *component*.
   - To start the server, specify `start` for *action* and `tdsproxy4app` for *component*.
   - To stop the server, specify `stop` for *action* and `tdsproxy4app` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
3. Verify that the file system on the messaging server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the file system on the data server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the Tivoli Directory Server proxy server is running using the platform control tool (DOPControl) or by the following steps. Only application server 1 will have a Tivoli Directory Server proxy server running.
   a. On application server 1 start a terminal session and log on as the `root` user.
   b. Run the **ps -ef | grep tdsproxy** command. If the Tivoli Directory Server proxy server is running, output similar to the following will be returned.
      ```
      tdsproxy 10046 1 0 Oct24 ? 00:00:18 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I tdsproxy
      tdsproxy 13920 1 0 22:55 ? 00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I tdsproxy -f /datahome/proxy/idsslapd-tdsproxy/etc/ibmslapd.conf
      ```
   c. Run the following to determine if Tivoli Directory Server is running.
      ```
      /opt/ibm/ldap/V6.3/bin/64/ibmdirctl -D cn=root -w password status
      ```
      where *password* is the password defined in the `LDAP.ADMIN.DN` property in the topology properties file.
6. If the Tivoli Directory Server proxy server is not running on application server 1, start the Tivoli Directory Server proxy server using the platform control tool (DOPControl) or by the following steps.
   a. On application server 1 start a terminal session and log on as the `tdsproxy` user. If running as the `root` user, change to the `tdsproxy` user by running the **su - tdsproxy** command.
   b. Run the **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I tdsproxy** command. Messages similar to the following should be returned.
      ```
      Server starting
      ...
      Non-SSL port initialized to 3358.
      GLPADM056I Admin server starting.
      GLPCOM003I Non-SSL port initialized to 3538.
      ```
   c. On application server 1 start a terminal session and log on as the `root` user.
   d. Run the **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I tdsproxy** command. Messages similar to the following should be returned.

```
Server starting
...
Non-SSL port initialized to 389.
GLPSRV041I Server starting.
GLPCOM003I Non-SSL port initialized to 389.
```

7. Verify that the Tivoli Directory Server LDAP server is running.
   a. Log on to a terminal session on data server 1 data server as `root`.
   b. Run the **`ps -ef | grep ibmslapd`** command. The results will be similar to the following:
   ```
   dsrdbm01 13797     1  0 Apr26 pts/1    00:00:09 /opt/ibm/ldap/V6.3/sbin/64/ibmslapd -I dsrdbm01 -t -n
   root     32080 19149  0 23:17 pts/1    00:00:00 grep ibmslapd
   ```
   This example shows that the Tivoli Directory Server daemon, ibmslapd, is running.
   c. Run the **`ps -ef | grep ibmdiradm`** command. The results will be similar to the following:
   ```
   root      4394 14038  0 14:17 pts/2    00:00:00 grep ibmdiradm
   dsrdbm01 11055     1  0 Apr26 pts/1    00:00:00 /opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t
   ```
   This example shows that the Tivoli Directory Server daemon, ibmdiradm, is running.
8. If the Tivoli Directory Server, ibmslapd, is not running, do the following.
   a. As a *root* Linux user, run **`/opt/ibm/ldap/V6.3/sbin/ibmslapd -I dsrdbm01`** to start the Directory Server
9. If the Tivoli Directory Administration Server, ibmdiradm, is not running, do the following.
   a. On a terminal session on the messaging server, run **`su - dsrdbm01`**.
   b. Run **`/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I dsrdbm01 -t`** to start the application server.
10. If the Tivoli Directory Server, ibmslapd, is running, do the following.

    Note: Do this step even if the Tivoli Directory Server was started in the previous step.
    a. Log on to a terminal session on the data server as dsrdbm01.
    b. Run **`idsldapsearch -h localhost -D "cn=root" -w "`***ADMIN_PASSWORD***`" -s sub uid=*`** where *ADMIN_PASSWORD* is the LDAP Root Administrator account password. The existing LDAP user objects will be displayed.
11. Verify that the Tivoli Directory Server Web Administration Tool is running. The Tivoli Directory Server Web Administration Tool is used to stop and start the LDAP instance, add users or accounts, and view log files.
    a. Log on to a terminal session on the application server as `ibmadmin`.
    b. Run the **`/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/serverStatus.sh -all -username waswebadmin -password`** *WAS_ADMIN_PASSWORD* command on the application server where *WAS_ADMIN_PASSWORD* is the WebSphere Application Server administrator password (usually `admin`). If the tool is running, a message similar to the following will be returned.
    ```
    ADMU0508I: The Application Server "server1" is STARTED
    ```
    If the following message is returned, the server1 needs to be started.
    ```
    ADMU0509I: The Application Server "server1" cannot be reached. It appears to be stopped.
    ```
    c. Start the server1 by running the **`/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh server1`** command. The server, server1, will start and a message similar to the following will be displayed.
    ```
    ADMU3000I: Server server1 open for e-business; process id is 26654
    ```
12. Access the Tivoli Directory Server Web Administration Tool at: `http://`*`APPLICATION_SERVER_HOST`*`:9081/IDSWebApp` where *APPLICATION_SERVER_HOST* is the host name of application server 1.
13. Log on with the LDAP Root Administrator Account, cn=root, and the appropriate password. The LDAP Server name should be *`DATABASE_DIRECTORY_SERVER_HOST`*`:389` where *DATABASE_DIRECTORY_SERVER_HOST* is the host name of the messaging server.
14. Click **Server Administration** > **Start/stop/reset server**. The LDAP server status will be displayed. This page can also be used to start, stop, or reset the LDAP server.

15. The Tivoli Directory Server proxy server can be stopped using the platform control tool (DOPControl) or by the following steps.
    a. On application server 1 start a terminal session and log on as the `tdsproxy` user. If running as the `root` user, change to the `tdsproxy` user by running the **su - tdsproxy** command.
    b. Run the **/opt/ibm/ldap/V6.3/sbin/64/ibmdiradm -I tdsproxy -k** command. Messages similar to the following should be returned.

       ```
       GLPADM034I Stopped Admin server instance: 'tdsproxy'.
       ```

    c. On application server 1 start a terminal session and log on as the `root` user.
    d. Run the **/opt/ibm/ldap/V6.3/sbin/ibmslapd -I tdsproxy -k** command. Messages similar to the following should be returned.

       ```
       GLPSRV176I Terminated directory server instance 'tdsproxy' normally.
       ```

What to do next

Resolve any issues or errors found and retry the test.

Directory (WebSphere Service Registry and Repository) Test

The Directory (WebSphere Service Registry and Repository) test determines the status of the WebSphere Service Registry and Repository server.

Resources

The Directory (WebSphere Service Registry and Repository) test uses the following resources:
- WebSphere Service Registry and Repository on the process server.
- WebSphere Application Server server WSRRServer1 (cluster WSRRCluster)

Problem determination

If the Directory (WebSphere Service Registry and Repository) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the server, specify `status` for *action* and `wsrr` for *component*.
   - To start the server, specify `start` for *action* and `wsrr` for *component*.
   - To stop the server, specify `stop` for *action* and `wsrr` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```

2. Check that there is network connectivity between the application server and the process server. This can be done by sending **ping** commands with both the short and fully-qualified host name of the process server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:

        - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
        - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
    c. On the process server review the following WebSphere Application Server logs:
        - Error log: `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/logs/WSRRServer1/SystemErr.log`
        - Output log: `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/logs/WSRRServer1/SystemOut.log`
        - Start log: `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/logs/WSRRServer1/startServer.log`

4. Verify that the file system on the process server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the WSRRServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
    a. On the process server system log on as `ibmadmin`.
    b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/serverStatus.sh -all -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.
    c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654.`
    a. If message `ADMU0509I: The Application Server "WSRRServer1" cannot be reached. It appears to be stopped.` is displayed, start the server using the following command: `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/startServer.sh WSRRServer1`. Skip this step if message `ADMU0508I: The Application Server "WSRRServer1" is STARTED.` is displayed. If you had to start the server, a message similar to the following will be displayed: `ADMU3000I: Server WSRRServer1 open for e-business; process id is 26654.`

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent
b. WSRRServer1

Stop servers in this order:

a. WSRRServer1
b. nodeagent

The WSRRServer1 server is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/stopServer.sh -all -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

The nodeagent is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/stopNode.sh -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

6. Verify that the WSRRServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
   a. Log on to the WebSphere Application Server V8 Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server 1.
   b. View the status of the WSRRServer1 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/startNode.sh` command in a command window.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:
   a. nodeagent
   b. WSRRServer1

   Stop servers in this order:
   a. WSRRServer1
   b. nodeagent

   To stop the WSRRServer1 server, select the server and click **Stop**.

   The nodeagent is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Messaging (Message Broker install check) Test

The Messaging (Message Broker install check) test determines if the message broker and queue manager can be accessed.

Resources

The Messaging (Message Broker install check) uses the following resource:
- WebSphere Portal Server (on the application server).

Problem determination

If the Messaging (Message Broker install check) test fails, do the following to find and resolve the problem.

Procedure

1. Use the platform control tool to check the status of the component and to start and stop it as needed. For *component* use `msg` and specify your topology password for *topology_password*.

a. To check the status of the component run the following commands:

```
su - ibmadmin

DOPControl -a status -c component -p topology_password
```

b. To start the component run the following commands:

```
su - ibmadmin

DOPControl -a start -c component -p topology_password
```

c. To stop the component run the following commands:

```
su - ibmadmin

DOPControl -a stop -c component -p topology_password
```

Alternately, the following commands can be run from the messaging server to check the status of WebSphere Message Broker:

```
su - mqm

dspmq
```

If WebSphere Message Broker is running, `QMNAME(DFT.MB.QM) STATUS(Running)` will be returned. If WebSphere Message Broker is not running, `QMNAME(DFT.MB.QM) STATUS(Ended normally)` will be returned.

2. Check that there is network connectivity between the application server) and the messaging server. This can be done by sending **ping** commands with both the short and fully-qualified host name of the messaging server from the application server and vice versa. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or /etc/hosts file.
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
   - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
   - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log
4. Verify that the file system on the application server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Check the logs for errors. The logs are located on the messaging server in the /var/log/messages directory. Look for messages with the prefix 'BIP'. Also look for queue names and timestamps when the test was run.
6. If WebSphere Message Broker is not running, start it using the platform control tool or by the following steps.
   a. Run the following commands.

```
su - mqmconn
source /opt/IBM/mqsi/8.0.0.1/bin/mqsiprofile
```

The following should be returned.

```
MQSI 8.0.0.1
/opt/IBM/mqsi/8.0.0.1
```

b. Run the following command.

```
strmqm -x DFT.MB.QM
```

The following should be returned.

```
WebSphere MQ queue manager 'DFT.MB.QM' starting.
The queue manager is associated with installation 'Installation1'.
5 log records accessed on queue manager 'DFT.MB.QM' during the log replay phase.
```

```
Log replay for queue manager 'DFT.MB.QM' complete.
Transaction manager state recovered for queue manager 'DFT.MB.QM'.
WebSphere MQ queue manager 'DFT.MB.QM' started using V7.5.0.0.
```

c. Run the following command:

```
mqsistart DFT_BROKER
```

The following should be returned.

```
BIP8096I: Successful command initiation, check the system log to
ensure that the component started without problem and that it
continues to run without problem.
```

What to do next

Resolve any issues or errors found and retry the test.

Messaging (Message Broker install check) [1] Test

The Messaging (Message Broker install check) [1] test determines if the message broker and queue manager can be accessed on the primary server in a high availability environment.

Resources

The Messaging (Message Broker install check) [1] test uses the following resource:

- WebSphere Portal Server (on the application server).

Problem determination

If the Messaging (Message Broker install check) [1] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of the primary server, specify `status` for *action* and `msgpri` for *component*.
   - To check the status of the standby server, specify `status` for *action* and `msgsby` for *component*.
   - To start the primary server, specify `start` for *action* and `msgpri` for *component*.
   - To start the standby server, specify `start` for *action* and `msgsby` for *component*.
   - To stop the primary server, specify `stop` for *action* and `msgpri` for *component*.
   - To stop the standby server, specify `stop` for *action* and `msgsby` for *component*.

   Specify your topology password for *topology_password*. The *component* `msg` can also be used to start, stop, or obtain the status of both messaging server 1 and messaging server 2.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```

   Alternately, the following commands can be run from the messaging server to check the status of WebSphere Message Broker:

   ```
   su - mqm

   dspmq
   ```

   If WebSphere Message Broker is running on messaging server 1, `QMNAME(DFT.MB.QM) STATUS(Running)` will be returned. If WebSphere Message Broker is running on messaging server 2, `QMNAME(DFT.MB.QM) STATUS(Running as standby)` will be returned. If WebSphere Message Broker is not running, `QMNAME(DFT.MB.QM) STATUS(Ended normally)` will be returned.

2. Check that there is network connectivity between the application server) and the messaging server. This can be done by sending **ping** commands with both the short and fully-qualified host name of the messaging server from the application server and vice versa. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or /etc/hosts file.
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log
4. Verify that the file system on the application server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Check the logs for errors. The logs are located on the messaging server in the /var/log/messages directory. Look for messages with the prefix 'BIP'. Also look for queue names and timestamps when the test was run.
6. If WebSphere Message Broker is not running, start it using the platform control tool or by the following steps.
   a. Run the following commands.

   ```
   su - mqmconn
   source /opt/IBM/mqsi/8.0.0.1/bin/mqsiprofile
   ```

   The following should be returned.

   ```
   MQSI 8.0.0.1
   /opt/IBM/mqsi/8.0.0.1
   ```

   b. Run the following command.

   ```
   strmqm -x DFT.MB.QM
   ```

   The following should be returned.

   ```
   WebSphere MQ queue manager 'DFT.MB.QM' starting.
   The queue manager is associated with installation 'Installation1'.
   5 log records accessed on queue manager 'DFT.MB.QM' during the log replay phase.
   Log replay for queue manager 'DFT.MB.QM' complete.
   Transaction manager state recovered for queue manager 'DFT.MB.QM'.
   WebSphere MQ queue manager 'DFT.MB.QM' started using V7.5.0.0.
   ```

   c. Run the following command:

   ```
   mqsistart DFT_BROKER
   ```

   The following should be returned.

   ```
   BIP8096I: Successful command initiation, check the system log to
   ensure that the component started without problem and that it
   continues to run without problem.
   ```

What to do next

Resolve any issues or errors found and retry the test.

Messaging (Message Broker install check) [2] Test

The Messaging (Message Broker install check) [2] test determines if the message broker and queue manager can be accessed on the backup server in a high availability environment.

Resources

The Messaging (Message Broker install check) [2] test uses the following resourc:

- WebSphere Portal Server (on the application server).

Problem determination

If the Messaging (Message Broker install check) [2] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of the primary server, specify `status` for *action* and `msgpri` for *component*.
   - To check the status of the standby server, specify `status` for *action* and `msgsby` for *component*.
   - To start the primary server, specify `start` for *action* and `msgpri` for *component*.
   - To start the standby server, specify `start` for *action* and `msgsby` for *component*.
   - To stop the primary server, specify `stop` for *action* and `msgpri` for *component*.
   - To stop the standby server, specify `stop` for *action* and `msgsby` for *component*.

   Specify your topology password for *topology_password*. The *component* `msg` can also be used to start, stop, or obtain the status of both messaging server 1 and messaging server 2.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```

   Alternately, the following commands can be run from the messaging server to check the status of WebSphere Message Broker:

   ```
   su - mqm

   dspmq
   ```

   If WebSphere Message Broker is running on messaging server 1, `QMNAME(DFT.MB.QM) STATUS(Running)` will be returned. If WebSphere Message Broker is running on messaging server 2, `QMNAME(DFT.MB.QM) STATUS(Running as standby)` will be returned. If WebSphere Message Broker is not running, `QMNAME(DFT.MB.QM) STATUS(Ended normally)` will be returned.
2. Check that there is network connectivity between the application server) and the messaging server. This can be done by sending **`ping`** commands with both the short and fully-qualified host name of the messaging server from the application server and vice versa. The results of the **`ping`** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
4. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.

5. Check the logs for errors. The logs are located on the messaging server in the `/var/log/messages` directory. Look for messages with the prefix 'BIP'. Also look for queue names and timestamps when the test was run.
6. If WebSphere Message Broker is not running, start it using the platform control tool or by the following steps.
   a. Run the following commands.

   ```
   su - mqmconn
   source /opt/IBM/mqsi/8.0.0.1/bin/mqsiprofile
   ```

   The following should be returned.

   ```
   MQSI 8.0.0.1
   /opt/IBM/mqsi/8.0.0.1
   ```

   b. Run the following command.

   ```
   strmqm -x DFT.MB.QM
   ```

   The following should be returned.

   ```
   WebSphere MQ queue manager 'DFT.MB.QM' starting.
   The queue manager is associated with installation 'Installation1'.
   5 log records accessed on queue manager 'DFT.MB.QM' during the log replay phase.
   Log replay for queue manager 'DFT.MB.QM' complete.
   Transaction manager state recovered for queue manager 'DFT.MB.QM'.
   WebSphere MQ queue manager 'DFT.MB.QM' started using V7.5.0.0.
   ```

   c. Run the following command:

   ```
   mqsistart DFT_BROKER
   ```

   The following should be returned.

   ```
   BIP8096I: Successful command initiation, check the system log to
   ensure that the component started without problem and that it
   continues to run without problem.
   ```

What to do next

Resolve any issues or errors found and retry the test.

Mobile (IBM Worklight console) Test

The Mobile (IBM Worklight console) test determines if the IBM Worklight server is running and the administration console is available.

Note: IBM Worklight is only available for installation through an IBM Services engagement.

Resources

The Mobile (IBM Worklight console) test uses the following resource:

- WebSphere Application Server named WorklightServer1

Problem determination

If the Mobile (IBM Worklight console) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the component and to start and stop it as needed. For *component* use `wrklt` and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:

```
su - ibmadmin
```

```
DOPControl -a status -c component -p topology_password
```

b. To start the component run the following commands:

```
su - ibmadmin
```

```
DOPControl -a start -c component -p topology_password
```

c. To stop the component run the following commands:

```
su - ibmadmin
```

```
DOPControl -a stop -c component -p topology_password
```

2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the aplication server review the following WebSphere Application Server logs:
   - `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/logs/WorklightServer1/SystemOut.log`
   - `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/logs/WorklightServer1/SystemErr.log`
3. Verify that the file system on the application server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the WorklightServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:

   a. On the application server system log on as `ibmadmin`.

   b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/serverStatus.sh -all -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.

   a. If message `ADMU0509I: The Application Server "WorklightServer1" cannot be reached. It appears to be stopped.` is displayed, start the WorklightServer1 server using the following command: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startServer.sh WorklightServer1`. Skip this step if message `ADMU0508I: The Application Server "WorklightServer1" is STARTED.` is displayed. If you had to start WorklightServer1, a message similar to the following will be displayed: `ADMU3000I: Server WorklightServer1 open for e-business; process id is 26654`.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

   a. nodeagent
   b. WorklightServer1

   Stop servers in this order:

   a. WorklightServer1
   b. nodeagent

   The WorklightServer1 server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopServer.sh -all -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopNode.sh -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the WorklightServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.

   b. View the status of the WorklightServer1 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startNode.sh` command in a command window.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:

   a. nodeagent
   b. WorklightServer1

   Stop servers in this order:

   a. WorklightServer1
   b. nodeagent

   To stop the WorklightServer1 server, select the server and click **Stop**.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopNode.sh -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

Mobile (IBM Worklight console) [1] Test

The Mobile (IBM Worklight console) [1] test determines if the primary IBM Worklight server in a high availability environment is running and the administration console is available.

Note: IBM Worklight is only available for installation through an IBM Services engagement.

Resources

The Mobile (IBM Worklight console) [1] test uses the following resource:

- WebSphere Application Server named WorklightServer1

Problem determination

If the Mobile (IBM Worklight console) [1] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of IBM Worklight, specify `status` for *action* and `wrklt` for *component*.
   - To start IBM Worklight, specify `start` for *action* and `wrklt` for *component*.
   - To stop IBM Worklight, specify `stop` for *action* and `wrklt` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the aplication server review the following WebSphere Application Server logs:
      - `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/logs/WorklightServer1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/logs/WorklightServer1/SystemErr.log`
3. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the WorklightServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the application server system log on as `ibmadmin`.

   b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654.`

a. If message `ADMU0509I: The Application Server "WorklightServer1" cannot be reached. It appears to be stopped.` is displayed, start the WorklightServer1 server using the following command: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startServer.sh WorklightServer1`. Skip this step if message `ADMU0508I: The Application Server "WorklightServer1" is STARTED.` is displayed. If you had to start WorklightServer1, a message similar to the following will be displayed: `ADMU3000I: Server WorklightServer1 open for e-business; process id is 26654`.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. WorklightServer1

Stop servers in this order:

a. WorklightServer1

b. nodeagent

The WorklightServer1 server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the WorklightServer1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.

   b. View the status of the WorklightServer1 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➔ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. WorklightServer1

Stop servers in this order:

a. WorklightServer1

b. nodeagent

To stop the WorklightServer1 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

Mobile (IBM Worklight console) [2] Test

The Mobile (IBM Worklight console) [2] test determines if the backup IBM Worklight server in a high availability environment is running and the administration console is available.

Note: IBM Worklight is only available for installation through an IBM Services engagement.

Resources

The Mobile (IBM Worklight console) [2] test uses the following resource:

- WebSphere Application Server named WorklightServer2

Problem determination

If the Mobile (IBM Worklight console) [2] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of IBM Worklight, specify `status` for *action* and `wrklt` for *component*.
   - To start IBM Worklight, specify `start` for *action* and `wrklt` for *component*.
   - To stop IBM Worklight, specify `stop` for *action* and `wrklt` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On application server 2 review the following WebSphere Application Server logs:
      - `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/logs/WorklightServer2/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/logs/WorklightServer2/SystemErr.log`
3. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the WorklightServer2 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:

a. On the application server 2 system log on as `ibmadmin`.

b. In a command window, run: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.

a. If message `ADMU0509I: The Application Server "WorklightServer2" cannot be reached. It appears to be stopped.` is displayed, start the WorklightServer2 server using the following command: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/startServer.sh WorklightServer2`. Skip this step if message `ADMU0508I: The Application Server "WorklightServer2" is STARTED.` is displayed. If you had to start WorklightServer2, a message similar to the following will be displayed: `ADMU3000I: Server WorklightServer2 open for e-business; process id is 26654`.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. WorklightServer2

Stop servers in this order:

a. WorklightServer2

b. nodeagent

The WorklightServer2 server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the WorklightServer2 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.

   b. View the status of the WorklightServer2 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➔ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent
b. WorklightServer2

Stop servers in this order:

a. WorklightServer2
b. nodeagent

To stop the WorklightServer2 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServer/profiles/WorklightProfile2/bin/stopNode.sh -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Monitoring (Netcool Omnibus) Test

The Monitoring (Netcool Omnibus) test determines if the Tivoli Netcool/OMNIbus server can be accessed.

Resources

The Monitoring (Netcool Omnibus) test uses the following resource:

- Tivoli Netcool/OMNIbus server on the monitoring server.

Problem determination

If the Monitoring (Netcool Omnibus) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the server, specify `status` for *action* and `ncobus` for *component*.
   - To start the server, specify `start` for *action* and `ncobus` for *component*.
   - To stop the server, specify `stop` for *action* and `ncobus` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Check that the process control server services and agent are running.

   a. On the monitoring server, run the **`/opt/IBM/netcool/omnibus/bin/nco_pa_status -server NCO_PA -user netcool -password`** *netcool_password* command where *netcool_password* is the password defined in the `OMNIBUS.OWNER.ACCOUNT.PWD` property in the topology properties file. Output similar the following will be returned. The `Status` column should be `RUNNING`.

   ```
   ------------------------------------------------------------------------------
   Service Name        Process Name        Hostname   User      Status      PID
   ------------------------------------------------------------------------------
   Core                MasterObjectServer  dopmon     netcool   RUNNING    3595
   ------------------------------------------------------------------------------
   ```

   b. If the services are not started or running, run the **/etc/init.d/nco start** command on the monitoring server as the `netcool` user to start the server.
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the monitoring server review all logs beginning with the letters NCO in the following directories.
      - `/opt/IBM/netcool/log`
      - `/opt/IBM/netcool/omnibus/log`
4. Verify that the file system on the monitoring server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the Tivoli Netcool/OMNIbus portlet can be accessed from the application server by accessing `http://`*`monitor_server_host`*`:16310/ibm/console` where *monitor_server_host* is the host name of the application server.

What to do next

Resolve any issues or errors found and retry the test.

Monitoring (Tivoli Enterprise Monitoring Server) Test

The Monitoring (Tivoli Enterprise Monitoring Server) test determines the status of the Tivoli Enterprise Monitoring server.

Resources

The Monitoring (Tivoli Enterprise Monitoring Server) test uses the following resources:
- Tivoli Enterprise Monitoring web services SOAP server on the monitoring server.
- Tivoli Enterprise Portal server on the monitoring server.
- Tivoli Enterprise Portal DB2 database on the monitoring server.

Problem determination

If the Monitoring (Tivoli Enterprise Monitoring Server) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the server, specify `status` for *action* and `tems` for *component*.
   - To start the server, specify `start` for *action* and `tems` for *component*.
   - To stop the server, specify `stop` for *action* and `tems` for *component*.

   Specify your topology password for *topology_password*.

```
su - ibmadmin

DOPControl -a action -c component -p topology_password
```

2. Check that there is network connectivity between the application server and the monitoring server. This can be done by sending **ping** commands with both the short and fully-qualified host name of the monitoring server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or /etc/hosts file.
3. Review the log files for runtime exceptions.
   a. On the monitoring server review the following monitoring server logs:
      - Tivoli Enterprise Monitoring server: /opt/IBM/ITM/logs/*monitoring_server_host*_ms_*.log
      - Tivoli Enterprise Portal server: /opt/IBM/ITM/logs/*monitoring_server_host*_cq_*.log
      - Embedded WebSphere Application Server:
        – Error log: /opt/IBM/ITM/lx8266/iw/profiles/ITMProfile/logs/ITMServer/SystemErr.log
        – Output log: /opt/IBM/ITM/lx8266/iw/profiles/ITMProfile/logs/ITMServer/SystemOut.log
        – Start log: /opt/IBM/ITM/lx8266/iw/profiles/ITMProfile/logs/ITMServer/startServer.log

   Where *monitoring_server_host* is the hostname of the monitoring server.
4. Verify that the file system on the monitoring server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the Tivoli Enterprise Monitoring components are running on the monitoring server server.
   a. Log on to a terminal session on the monitoring server as a root user.
   b. Run the **/opt/IBM/ITM/bin/cinfo -r** command.
6. Verify the Tivoli component databases are operational.
   a. Log on to a terminal session on the monitoring server as the db2inst1 user.
   b. Run the **ps -ef | grep db2inst1** command.
   c. Verify the following DB2 process are running: db2sync, db2vend, and db2acd.
   d. If the DB2 process are not running, run the **db2start** command.
   e. Check the DB2 logs on the data server for any database errors related starting databases used by Tivoli components. The log files can be found in the /datahome/db2inst1/sqllib/db2dump directory on the data server.
7. Verify that the Tivoli Enterprise Monitoring server is running by looking for an entry for ms. If the entry is not listed, the Tivoli Enterprise Monitoring server is not running.
8. If the Tivoli Enterprise Monitoring server is not running, start the server.
   a. Log on to a terminal session on the monitoring server as a root user.
   b. Run the **/opt/IBM/ITM/bin/itmcmd server start HUB_MWOS** command.
9. Verify that the Tivoli Enterprise Portal server is running by looking for an entry for cq in the results of the **/opt/IBM/ITM/bin/cinfo -r** command. If the entry is not listed, the Tivoli Enterprise Portal server is not running.
10. If the Tivoli Enterprise Portal server is not running, start the server.
    a. Log on to a terminal session on the monitoring server as a root user.
    b. Run the **/opt/IBM/ITM/bin/itmcmd agent start cq** command.
11. Verify that the following other subcomponents are running in the results of the **/opt/IBM/ITM/bin/cinfo -r** command.

    kf Eclipse Help Server

    lz Monitoring Agent for Linux OS

12. If the subcomponents are not running, start the IBM Defense Operations Platform agents by running the **DOPControl -a start -c agents -p** *topology_password* command where *topology_password* is the topology password.

What to do next

Resolve any issues or errors found and retry the test.

Monitoring (Tivoli Enterprise Portal Server) Test

The Monitoring (Tivoli Enterprise Portal Server) test determines the status of the Tivoli Enterprise Portal server.

Resources

The Monitoring (Tivoli Enterprise Portal Server) test uses the following resources:

- Tivoli Enterprise Monitoring web services SOAP server on the monitoring server.
- Tivoli Enterprise Portal server on the monitoring server.
- Tivoli Enterprise Portal DB2 database on the monitoring server.

Problem determination

If the Monitoring (Tivoli Enterprise Portal Server) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the server, specify `status` for *action* and `teps` for *component*.
   - To start the server, specify `start` for *action* and `teps` for *component*.
   - To stop the server, specify `stop` for *action* and `teps` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Check that there is network connectivity between the application server and the monitoring server. This can be done by sending **ping** commands with both the short and fully-qualified host name of the monitoring server from the application server. The results of the **ping** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
3. Review the log files for runtime exceptions.
   a. On the monitoring server review the following monitoring server logs:
      - Tivoli Enterprise Monitoring server: `/opt/IBM/ITM/logs/`*monitoring_server_host*`_ms_*.log`
      - Tivoli Enterprise Portal server: `/opt/IBM/ITM/logs/`*monitoring_server_host*`_cq_*.log`
      - Embedded WebSphere Application Server:
        – Error log: `/opt/IBM/ITM/lx8266/iw/profiles/ITMProfile/logs/ITMServer/SystemErr.log`
        – Output log: `/opt/IBM/ITM/lx8266/iw/profiles/ITMProfile/logs/ITMServer/SystemOut.log`
        – Start log: `/opt/IBM/ITM/lx8266/iw/profiles/ITMProfile/logs/ITMServer/startServer.log`

      Where *monitoring_server_host* is the hostname of the monitoring server.
4. Verify that the file system on the monitoring server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.

5. Verify that the Tivoli Enterprise Monitoring components are running on the monitoring server server.
   a. Log on to a terminal session on the monitoring server as a root user.
   b. Run the **/opt/IBM/ITM/bin/cinfo -r** command.
6. Verify the Tivoli component databases are operational.
   a. Log on to a terminal session on the monitoring server as the db2inst1 user.
   b. Run the **ps -ef | grep db2inst1** command.
   c. Verify the following DB2 process are running: db2sync, db2vend, and db2acd.
   d. If the DB2 process are not running, run the **db2start** command.
   e. Check the DB2 logs on the data server for any database errors related starting databases used by Tivoli components. The log files can be found in the `/datahome/db2inst1/sqllib/db2dump` directory on the data server.
7. Verify that the Tivoli Enterprise Monitoring server is running by looking for an entry for `ms`. If the entry is not listed, the Tivoli Enterprise Monitoring server is not running.
8. If the Tivoli Enterprise Monitoring server is not running, start the server.
   a. Log on to a terminal session on the monitoring server as a root user.
   b. Run the **/opt/IBM/ITM/bin/itmcmd server start HUB_MWOS** command.
9. Verify that the Tivoli Enterprise Portal server is running by looking for an entry for `cq` in the results of the **/opt/IBM/ITM/bin/cinfo -r** command. If the entry is not listed, the Tivoli Enterprise Portal server is not running.
10. If the Tivoli Enterprise Portal server is not running, start the server.
    a. Log on to a terminal session on the monitoring server as a root user.
    b. Run the **/opt/IBM/ITM/bin/itmcmd agent start cq** command.
11. Verify that the following other subcomponents are running in the results of the **/opt/IBM/ITM/bin/cinfo -r** command.

    kf Eclipse Help Server

    lz Monitoring Agent for Linux OS
12. If the subcomponents are not running, start the IBM Defense Operations Platform agents by running the **DOPControl -a start -c agents -p** *topology_password* command where *topology_password* is the topology password.

Monitoring (Tivoli Integrated Portal/Netcool) Test

The Monitoring (Tivoli Integrated Portal/Netcool) test determines the status of the Tivoli Integrated Portal server.

Resources

The Monitoring (Tivoli Integrated Portal/Netcool) test uses the following resource:

- Tivoli Integrated Portal server on the monitoring server

Problem determination

If the Monitoring (Tivoli Integrated Portal/Netcool) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the server, specify `status` for *action* and `ncobus` for *component*.
   - To start the server, specify `start` for *action* and `ncobus` for *component*.

- To stop the server, specify `stop` for *action* and `ncobus` for *component*.

Specify your topology password for *topology_password*.

```
su - ibmadmin

DOPControl -a action -c component -p topology_password
```

2. Check that the process control server services and agent are running.
   a. On the monitoring server, run the **/opt/IBM/netcool/omnibus/bin/nco_pa_status -server NCO_PA -user netcool -password** *netcool_password* command where *netcool_password* is the password defined in the `OMNIBUS.OWNER.ACCOUNT.PWD` property in the topology properties file. Output similar the following will be returned. The `Status` column should be `RUNNING`.

   ```
   -------------------------------------------------------------------------------
   Service Name         Process Name        Hostname   User      Status      PID
   -------------------------------------------------------------------------------
   Core                 MasterObjectServer  dopmon     netcool   RUNNING    3595
   -------------------------------------------------------------------------------
   ```

   b. If the services are not started or running, run the **/etc/init.d/nco start** command on the monitoring server as the `netcool` user to start the server.
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the monitoring server review all logs beginning with the letters NCO in the following directories.
      - `/opt/IBM/netcool/log`
      - `/opt/IBM/netcool/omnibus/log`
      - `/opt/IBM/netcool/tipv2/profiles/TIPProfile/logs/server1/SystemOut.log`
      - `/opt/IBM/netcool/tipv2/profiles/TIPProfile/logs/server1/SystemErr.log`
4. Verify that the file system on the monitoring server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the Tivoli Netcool/OMNIbus portlet can be accessed from the application server by accessing `http://`*`monitor_server_host`*`:16310/ibm/console` where *monitor_server_host* is the host name of the application server.
6. Manage Tivoli Integrated Portal server using the following commands on the monitoring server.
   - Check the status of the Tivoli Integrated Portal server by running the following command.

     ```
     /opt/IBM/netcool/tipv2/profiles/TIPProfile/bin/serverStatus.sh  server1 -user user -password password
     ```

     where *user* is the value of the `OMNIBUS.ADMIN.ACCOUNT` property in the topology properties file and *password* is the value of the `OMNIBUS.ADMIN.ACCOUNT.PWD` property in the topology properties file.
   - Stop Tivoli Integrated Portal server by running the following command.

     ```
     /opt/IBM/netcool/tipv2/profiles/TIPProfile/bin/stopServer.sh  server1 -user user -password password
     ```

     where *user* is the value of the `OMNIBUS.ADMIN.ACCOUNT` property in the topology properties file and *password* is the value of the `OMNIBUS.ADMIN.ACCOUNT.PWD` property in the topology properties file.
   - Start Tivoli Integrated Portal server by running the following command.

     ```
     /opt/IBM/netcool/tipv2/profiles/TIPProfile/bin/startServer.sh  server1
     ```

What to do next

Resolve any issues or errors found and retry the test.

Password Management (Tivoli Directory Integrator) Test

The Password Management (Tivoli Directory Integrator) tests access to Tivoli Directory Integrator.

Resources

The Password Management (Tivoli Directory Integrator) test uses the following resource:

- Tivoli Directory Server (on the data server)
- Tivoli Directory Integrator (on the data server)

Problem determination

If the Password Management (Tivoli Directory Integrator) test fails, do the following to find and resolve the access problem.

Procedure

1. If running in the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use `tdi` and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```
   b. To start the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```
   c. To stop the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a stop -c component -p topology_password
   ```
2. If running in a high availability environment, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To start the server, specify `start` for *action* and `tdi` for *component*.
   - To stop the server, specify `stop` for *action* and `tdi` for *component*.

   Specify your topology password for *topology_password*.
   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the data server review all the Tivoli Directory Server logs in the following directory:

   - /opt/IBM/TDI/V7.1/timsol/logs
   d. On the data server review all the Tivoli Directory Server logs:
      - /opt/IBM/TDI/V7.1/pwd_plugins/tds/plugin.log
      - /opt/IBM/TDI/V7.1/pwd_plugins/tds/proxy.log
4. Verify that the file system on the application server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the Tivoli Directory Integrator server is started.
   a. Log on to the data server as the ibmadmin user.
   b. Start or restart the server.
      - To start the server, run the **/opt/IBM/TDI/V7.1/timsol/ITIMAd start** command.
      - To restart the server, run the **/opt/IBM/TDI/V7.1/timsol/ITIMAd restart** command.

What to do next

Resolve any issues or errors found and retry the test.

Portal (WebSphere Portal console via Web Server) Test

The Portal (WebSphere Portal console via Web Server) test tests web server access to the WebSphere Portal console.

Resources

The Portal (WebSphere Portal console via Web Server) test uses the following resource:
- WebSphere Application Server on the application server.

Problem determination

If the Portal (WebSphere Portal console via Web Server) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the component and to start and stop it as needed. For *component* use wpe and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```
   b. To start the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```
   c. To stop the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a stop -c component -p topology_password
   ```
2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log
   b. On the application server review the following WebSphere Application Server logs:

- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
- /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log

3. Verify that the file system on the application server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the WebSphere_Portal server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the application server system log on as `ibmadmin`.
   b. In a command window, run: `/opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.
   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654.`
   a. If message `ADMU0509I: The Application Server "WebSphere_Portal" cannot be reached. It appears to be stopped.` is displayed, start the WebSphere_Portal server using the following command: `/opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_Portal`. Skip this step if message `ADMU0508I: The Application Server "WebSphere_Portal" is STARTED.` is displayed. If you had to start WebSphere_Portal, a message similar to the following will be displayed: `ADMU3000I: Server WebSphere_Portal open for e-business; process id is 26654.`

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:
   a. nodeagent
   b. WebSphere_Portal

   Stop servers in this order:
   a. WebSphere_Portal
   b. nodeagent

   The WebSphere_Portal server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopServer.sh -all -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.
5. Verify that the WebSphere_Portal server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
   a. Log on to the WebSphere Application Server Administrative Console at `http://`*APPLICATION_SERVER_HOST*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.

b. View the status of the WebSphere_Portal server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

   The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

   The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

   The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. WebSphere_Portal

Stop servers in this order:

a. WebSphere_Portal

b. nodeagent

To stop the WebSphere_Portal server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Portal (WebSphere Portal console via Web Server) [1] Test

The Portal (WebSphere Portal console via Web Server) [1] test tests web server access to the WebSphere Portal console on the primary server in a high availability environment.

Resources

The Portal (WebSphere Portal console via Web Server) [1] test uses the following resource:

- WebSphere Application Server on the application server.

Problem determination

If the Portal (WebSphere Portal console via Web Server) [1] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To start the server, specify `start` for *action* and `wpe` for *component*.
   - To stop the server, specify `stop` for *action* and `wpe` for *component*.
   - To check the status of the server, specify `status` for *action* and `wpe` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin
   ```

   ```
   DOPControl -a action -c component -p topology_password
   ```

2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
   b. On the application server review the following WebSphere Application Server logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
3. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the WebSphere_Portal server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the application server system log on as `ibmadmin`.
   b. In a command window, run: `/opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.
   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.
   a. If message `ADMU0509I: The Application Server "WebSphere_Portal" cannot be reached. It appears to be stopped.` is displayed, start the WebSphere_Portal server using the following command: `/opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_Portal`. Skip this step if message `ADMU0508I: The Application Server "WebSphere_Portal" is STARTED.` is displayed. If you had to start WebSphere_Portal, a message similar to the following will be displayed: `ADMU3000I: Server WebSphere_Portal open for e-business; process id is 26654`.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:
   a. nodeagent
   b. WebSphere_Portal

   Stop servers in this order:
   a. WebSphere_Portal
   b. nodeagent

   The WebSphere_Portal server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the WebSphere_Portal server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.
   b. View the status of the WebSphere_Portal server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➔ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` command in a command window.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:
   a. nodeagent
   b. WebSphere_Portal

   Stop servers in this order:
   a. WebSphere_Portal
   b. nodeagent

   To stop the WebSphere_Portal server, select the server and click **Stop**.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Portal (WebSphere Portal console via Web Server) [2] Test

The Portal (WebSphere Portal console via Web Server) [2] test tests web server access to the WebSphere Portal console on the backup server in a high availability environment.

Resources

The Portal (WebSphere Portal console via Web Server) [2] test uses the following resource:
- WebSphere Application Server on application server 2.

Problem determination

If the Portal (WebSphere Portal console via Web Server) [2] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.

- To start the server, specify `start` for *action* and `wpe` for *component*.
- To stop the server, specify `stop` for *action* and `wpe` for *component*.
- To check the status of the server, specify `status` for *action* and `wpe` for *component*.

Specify your topology password for *topology_password*.

```
su - ibmadmin

DOPControl -a action -c component -p topology_password
```

2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
   c. On application server 2 review the following WebSphere Application Server logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
3. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the WebSphere_Portal_PortalNode2 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the application server system log on as `ibmadmin`.
   b. In a command window, run: `/opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.
   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654.`
   a. If message `ADMU0509I: The Application Server "WebSphere_Portal_PortalNode2" cannot be reached. It appears to be stopped.` is displayed, start the WebSphere_Portal_PortalNode2 server using the following command: `/opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_Portal_PortalNode2`. Skip this step if message `ADMU0508I: The Application Server "WebSphere_Portal_PortalNode2" is STARTED.` is displayed. If you had to start WebSphere_Portal_PortalNode2, a message similar to the following will be displayed: `ADMU3000I: Server WebSphere_Portal_PortalNode2 open for e-business; process id is 26654.`

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:
   a. nodeagent
   b. WebSphere_Portal_PortalNode2

   Stop servers in this order:

   a. WebSphere_Portal_PortalNode2
   b. nodeagent

   The WebSphere_Portal_PortalNode2 server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopServer.sh -all -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the WebSphere_Portal_PortalNode2 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
   a. Log on to the WebSphere Application Server Administrative Console at `http://`*APPLICATION_SERVER_HOST*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.
   b. View the status of the WebSphere_Portal_PortalNode2 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➔ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` command in a command window.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:
   a. nodeagent
   b. WebSphere_Portal_PortalNode2

   Stop servers in this order:
   a. WebSphere_Portal_PortalNode2
   b. nodeagent

   To stop the WebSphere_Portal_PortalNode2 server, select the server and click **Stop**.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Portal (WebSphere Portal console) Test

The Portal (WebSphere Portal console) test tests access to the WebSphere Portal console.

Resources

The Portal (WebSphere Portal console) test uses the following resource:

- WebSphere Application Server on the application server.

Problem determination

If the Portal (WebSphere Portal console) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the component and to start and stop it as needed. For *component* use `wpe` and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
      ```
      su - ibmadmin

      DOPControl -a status -c component -p topology_password
      ```
   b. To start the component run the following commands:
      ```
      su - ibmadmin

      DOPControl -a start -c component -p topology_password
      ```
   c. To stop the component run the following commands:
      ```
      su - ibmadmin

      DOPControl -a stop -c component -p topology_password
      ```
2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
   b. On the application server review the following WebSphere Application Server logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
3. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the WebSphere_Portal server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the application server system log on as `ibmadmin`.
   b. In a command window, run: `/opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.
   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654.`
   a. If message `ADMU0509I: The Application Server "WebSphere_Portal" cannot be reached. It appears to be stopped.` is displayed, start the WebSphere_Portal server using the following command: `/opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_Portal`. Skip this step

if message `ADMU0508I: The Application Server "WebSphere_Portal" is STARTED.` is displayed. If you had to start WebSphere_Portal, a message similar to the following will be displayed: `ADMU3000I: Server WebSphere_Portal open for e-business; process id is 26654.`

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. WebSphere_Portal

Stop servers in this order:

a. WebSphere_Portal

b. nodeagent

The WebSphere_Portal server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the WebSphere_Portal server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.

   b. View the status of the WebSphere_Portal server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➜ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ❓ icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. WebSphere_Portal

Stop servers in this order:

a. WebSphere_Portal

b. nodeagent

To stop the WebSphere_Portal server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *`WAS_ADMIN_USER`*

`-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Portal (WebSphere Portal console) [1] Test

The Portal (WebSphere Portal console) [1] test tests access to the WebSphere Portal console on the primary server in a high availability environment.

Resources

The Portal (WebSphere Portal console) [1] test uses the following resource:

- WebSphere Application Server on the application server.

Problem determination

If the Portal (WebSphere Portal console) [1] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of the server, specify `status` for *action* and `wpe` for *component*.
   - To start the server, specify `start` for *action* and `wpe` for *component*.
   - To stop the server, specify `stop` for *action* and `wpe` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. On the application server review the following WebSphere Application Server logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`
3. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
4. Verify that the WebSphere_Portal server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the application server system log on as `ibmadmin`.

   b. In a command window, run: `/opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/`

`wp_profile/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.

a. If message `ADMU0509I: The Application Server "WebSphere_Portal" cannot be reached. It appears to be stopped.` is displayed, start the WebSphere_Portal server using the following command: `/opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_Portal`. Skip this step if message `ADMU0508I: The Application Server "WebSphere_Portal" is STARTED.` is displayed. If you had to start WebSphere_Portal, a message similar to the following will be displayed: `ADMU3000I: Server WebSphere_Portal open for e-business; process id is 26654`.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. WebSphere_Portal

Stop servers in this order:

a. WebSphere_Portal

b. nodeagent

The WebSphere_Portal server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the WebSphere_Portal server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.

   b. View the status of the WebSphere_Portal server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➔ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. WebSphere_Portal

Stop servers in this order:

a. WebSphere_Portal

b. nodeagent

To stop the WebSphere_Portal server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Portal (WebSphere Portal console) [2] Test

The Portal (WebSphere Portal console) [2] test tests access to the WebSphere Portal console on the backup server in a high availability environment.

Resources

The Portal (WebSphere Portal console) [2] test uses the following resource:

- WebSphere Application Server on application server 2.

Problem determination

If the Portal (WebSphere Portal console) [2] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the servers and to start and stop them as needed. Run the following commands with the desired options.
   - To check the status of the server, specify `status` for *action* and `wpe` for *component*.
   - To start the server, specify `start` for *action* and `wpe` for *component*.
   - To stop the server, specify `stop` for *action* and `wpe` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On application server 2 review the following WebSphere Application Server logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`
3. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.

4. Verify that the WebSphere_Portal_PortalNode2 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:

   a. On the application server system log on as `ibmadmin`.

   b. In a command window, run: `/opt/IBM/WebSphere/wp_profile/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.

   a. If message `ADMU0509I: The Application Server "WebSphere_Portal_PortalNode2" cannot be reached. It appears to be stopped.` is displayed, start the WebSphere_Portal_PortalNode2 server using the following command: `/opt/IBM/WebSphere/wp_profile/bin/startServer.sh WebSphere_Portal_PortalNode2`. Skip this step if message `ADMU0508I: The Application Server "WebSphere_Portal_PortalNode2" is STARTED.` is displayed. If you had to start WebSphere_Portal_PortalNode2, a message similar to the following will be displayed: `ADMU3000I: Server WebSphere_Portal_PortalNode2 open for e-business; process id is 26654`.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:

   a. nodeagent

   b. WebSphere_Portal_PortalNode2

   Stop servers in this order:

   a. WebSphere_Portal_PortalNode2

   b. nodeagent

   The WebSphere_Portal_PortalNode2 server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the WebSphere_Portal_PortalNode2 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.

   b. View the status of the WebSphere_Portal_PortalNode2 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

The ❓ icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/wp_profile/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent
b. WebSphere_Portal_PortalNode2

Stop servers in this order:

a. WebSphere_Portal_PortalNode2
b. nodeagent

To stop the WebSphere_Portal_PortalNode2 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/wp_profile/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Process Management (Business Process Manager Business Space console) Test

The Process Management (Business Process Manager Business Space console) test determines if the IBM Business Process Manager server is running.

Resources

The Process Management (Business Process Manager Business Space console) test uses the following resource:

- WebSphere Application Server named WBM_DE.AppTarget.WBMNode1.0

Problem determination

If the Process Management (Business Process Manager Business Space console) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the component and to start and stop it as needed. For *component* use `bpm` and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```
   b. To start the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```
   c. To stop the component run the following commands:

```
su - ibmadmin
```

```
DOPControl -a stop -c component -p topology_password
```

2. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log
      - /opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log

   c. On the process server review the following WebSphere Application Server logs:
      - /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/logs/BPM_DE.AppTarget.BPMNode1.0/SystemOut.log
      - /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/logs/BPM_DE.AppTarget.BPMNode1.0/SystemErr.log

3. Verify that the file system on the application server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.

4. Verify that the BPM_DE.AppTarget.BPMNode1.0 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the process server system log on as ibmadmin.

   b. In a command window, run: /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/serverStatus.sh -all -username *WAS_ADMIN_USER* -password *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally admin) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   c. If message ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped. is displayed, start the nodeagent using the following command: /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/startNode.sh . Skip this step if message ADMU0508I: The Application Server "nodeagent" is STARTED. is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: ADMU3000I: Server nodeagent open for e-business; process id is 26654.

   a. If message ADMU0509I: The Application Server "BPM_DE.AppTarget.BPMNode1.0" cannot be reached. It appears to be stopped. is displayed, start the server using the following command: /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/startServer.sh BPM_DE.AppTarget.BPMNode1.0. Skip this step if message ADMU0508I: The Application Server "BPM_DE.AppTarget.BPMNode1.0" is STARTED. is displayed. If you had to start the server, a message similar to the following will be displayed: ADMU3000I: Server BPM_DE.AppTarget.BPMNode1.0 open for e-business; process id is 26654.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:

   a. nodeagent
   b. BPM_DE.AppTarget.BPMNode1.0

   Stop servers in this order:

   a. BPM_DE.AppTarget.BPMNode1.0
   b. nodeagent

The BPM_DE.AppTarget.BPMNode1.0 server is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

The nodeagent is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

5. Verify that the BPM_DE.AppTarget.BPMNode1.0 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9062/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.
   b. View the status of the BPM_DE.AppTarget.BPMNode1.0 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

      The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent
b. BPM_DE.AppTarget.BPMNode1.0

Stop servers in this order:

a. BPM_DE.AppTarget.BPMNode1.0
b. nodeagent

To stop the BPM_DE.AppTarget.BPMNode1.0 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the process server: `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

Process Management (Business Process Manager console) Test

The Process Management (Business Process Manager console) test determines if WebSphere Business Process Management can be accessed.

Resources

The Process Management (Business Process Manager console) test uses the following resource:

- WebSphere Business Process Management on the process server.
- WebSphere Application Server server BPM_DE.AppTarget.BPMNode1.0.

Problem determination

If the Process Management (Business Process Manager console) test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the server, specify `status` for *action* and `bpm` for *component*.
   - To start the server, specify `start` for *action* and `bpm` for *component*.
   - To stop the server, specify `stop` for *action* and `bpm` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Check that there is network connectivity between the application server and the process server. This can be done by sending **`ping`** commands with both the short and fully-qualified host name of the process server from the application server. The results of the **`ping`** commands will show if the host name is being correctly resolved by the DNS or `/etc/hosts` file.
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the process server review the following WebSphere Application Server logs:
      - Error log: `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/logs/BPM_DE.AppTarget.BPMNode1.0/SystemErr.log`
      - Output log: `/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/logs/BPM_DE.AppTarget.BPMNode1.0/SystemOut.log`
      - Start log: `Not /opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/logs/BPM_DE.AppTarget.BPMNode1.0/startServer.log`
4. Verify that the file system on the process server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the WebSphere Application Server is running.
   a. On the process server system log on as `ibmadmin`.

   b. Run the **`/opt/IBM/WebSphere/AppServer/profiles/bpmProfile1/bin/serverStatus.sh BPM_DE.AppTarget.BPMNode1.0`** command.

What to do next

Resolve any issues or errors found and retry the test.

Security (IBM Security Identity Manager administration console) Test

The Security (IBM Security Identity Manager administration console) test determines if the IBM Security Identity Manager server is running and the administration console is available.

Resources

The Security (IBM Security Identity Manager administration console) test uses the following resource:

- WebSphere Application Server named isim1.

Problem determination

If the Security (IBM Security Identity Manager administration console) test fails, do the following to find and resolve the access problem.

Procedure

1. If running in the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use `isim` and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```
   b. To start the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```
   c. To stop the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a stop -c component -p topology_password
   ```
2. If running in the Command Center Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of IBM Security Identity Manager, specify `status` for *action* and `isim` for *component*.
   - To stop IBM Security Identity Manager, specify `stop` for *action* and `isim` for *component*.
   - To start IBM Security Identity Manager, specify `start` for *action* and `isim` for *component*.

   Specify your topology password for *topology_password*.
   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the application server review the following WebSphere Application Server logs:
   - `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/isim1/SystemOut.log`
   - `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/isim1/SystemErr.log`
4. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.

5. Verify that the isim1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:

   a. On the application server system log on as `ibmadmin`.

   b. In a command window, run: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.

   a. If message `ADMU0509I: The Application Server "isim1" cannot be reached. It appears to be stopped.` is displayed, start the isim1 server using the following command: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh isim1`. Skip this step if message `ADMU0508I: The Application Server "isim1" is STARTED.` is displayed. If you had to start isim1, a message similar to the following will be displayed: `ADMU3000I: Server isim1 open for e-business; process id is 26654`.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:

   a. nodeagent

   b. isim1

   Stop servers in this order:

   a. isim1

   b. nodeagent

   The isim1 server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

6. Verify that the isim1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:

   a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9061/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.

   b. View the status of the isim1 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

      The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

      The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent

b. isim1

Stop servers in this order:

a. isim1

b. nodeagent

To stop the isim1 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopNode.sh -username` *WAS_ADMIN_USER* `-password` *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Security (IBM Security Identity Manager console) Test

The Security (IBM Security Identity Manager console) test determines if the IBM Security Identity Manager server is running and the console is available.

Resources

The Security (IBM Security Identity Manager console) test uses the following resource:

- WebSphere Application Server named isim1.

Problem determination

If the Security (IBM Security Identity Manager console) test fails, do the following to find and resolve the access problem.

Procedure

1. If running in the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use `isim` and specify your topology password for *topology_password*.

   a. To check the status of the component run the following commands:

   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```

   b. To start the component run the following commands:

   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```

   c. To stop the component run the following commands:

   ```
   su - ibmadmin

   DOPControl -a stop -c component -p topology_password
   ```

2. If running in the Command Center Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of IBM Security Identity Manager, specify `status` for *action* and `isim` for *component*.
   - To stop IBM Security Identity Manager, specify `stop` for *action* and `isim` for *component*.
   - To start IBM Security Identity Manager, specify `start` for *action* and `isim` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
      - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the application server review the following WebSphere Application Server logs:
      - `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/isim1/SystemOut.log`
      - `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/isim1/SystemErr.log`
4. Verify that the file system on the application server has not reached capacity. This can be determined by running the **`df -h`** command. The file system can be considered full even if it less than 100% used. For this reason if the **`df -h`** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the isim1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the application server system log on as `ibmadmin`.

   b. In a command window, run: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/serverStatus.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   c. If message `ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped.` is displayed, start the nodeagent using the following command: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startNode.sh` . Skip this step if message `ADMU0508I: The Application Server "nodeagent" is STARTED.` is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: `ADMU3000I: Server nodeagent open for e-business; process id is 26654`.

   a. If message `ADMU0509I: The Application Server "isim1" cannot be reached. It appears to be stopped.` is displayed, start the isim1 server using the following command: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh isim1`. Skip this step if message `ADMU0508I: The Application Server "isim1" is STARTED.` is displayed. If you had to start isim1, a message similar to the following will be displayed: `ADMU3000I: Server isim1 open for e-business; process id is 26654`.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:

   a. nodeagent

    b. isim1

    Stop servers in this order:

    a. isim1
    b. nodeagent

    The isim1 server is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopServer.sh -all -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

    The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

6. Verify that the isim1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
    a. Log on to the WebSphere Application Server Administrative Console at `http://`*`APPLICATION_SERVER_HOST`*`:9061/ibm/console` using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.
    b. View the status of the isim1 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

        The ➔ icon means the server is started. If required, select the server and click **Restart** to restart the server.

        The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

        The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startNode.sh` command in a command window.

    Important: Servers must be started and stopped in a specific order.

    Start servers in this order:

    a. nodeagent
    b. isim1

    Stop servers in this order:

    a. isim1
    b. nodeagent

    To stop the isim1 server, select the server and click **Stop**.

    The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Security (IBM Security Identity Manager self console) Test

The Security (IBM Security Identity Manager self console) test determines if the IBM Security Identity Manager server is running and the self console is available.

Resources

The Security (IBM Security Identity Manager self console) test uses the following resource:

- WebSphere Application Server named isim1.

Problem determination

If the Security (IBM Security Identity Manager self console) test fails, do the following to find and resolve the access problem.

Procedure

1. If running in the Field Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options. For *component* use `isim` and specify your topology password for *topology_password*.
   a. To check the status of the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a status -c component -p topology_password
   ```
   b. To start the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a start -c component -p topology_password
   ```
   c. To stop the component run the following commands:
   ```
   su - ibmadmin

   DOPControl -a stop -c component -p topology_password
   ```
2. If running in the Command Center Edition, use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of IBM Security Identity Manager, specify `status` for *action* and `isim` for *component*.
   - To stop IBM Security Identity Manager, specify `stop` for *action* and `isim` for *component*.
   - To start IBM Security Identity Manager, specify `start` for *action* and `isim` for *component*.

   Specify your topology password for *topology_password*.
   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
3. Review the log files for runtime exceptions.
   a. On the application server review the following WebSphere Portal logs:
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemOut.log`
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal/SystemErr.log`

   b. In the Command Center Edition, on application server 2 review the following WebSphere Portal logs:
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemOut.log`
   - `/opt/IBM/WebSphere/wp_profile/logs/WebSphere_Portal_PortalNode2/SystemErr.log`

   c. On the application server review the following WebSphere Application Server logs:
   - `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/isim1/SystemOut.log`

   - /opt/IBM/WebSphere/AppServerv7/profiles/isim1/logs/isim1/SystemErr.log
4. Verify that the file system on the application server has not reached capacity. This can be determined by running the **df -h** command. The file system can be considered full even if it less than 100% used. For this reason if the **df -h** command returns that the file system is 90% or more full, you should consider that the file system has reached capacity.
5. Verify that the isim1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the manual steps:
   a. On the application server system log on as ibmadmin.
   b. In a command window, run: /opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/serverStatus.sh -all -username *WAS_ADMIN_USER* -password *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally admin) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.
   c. If message ADMU0509I: The Application Server "nodeagent" cannot be reached. It appears to be stopped. is displayed, start the nodeagent using the following command: /opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startNode.sh . Skip this step if message ADMU0508I: The Application Server "nodeagent" is STARTED. is displayed. If you had to start the nodeagent, a message similar to the following will be displayed: ADMU3000I: Server nodeagent open for e-business; process id is 26654.
   a. If message ADMU0509I: The Application Server "isim1" cannot be reached. It appears to be stopped. is displayed, start the isim1 server using the following command: /opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startServer.sh isim1. Skip this step if message ADMU0508I: The Application Server "isim1" is STARTED. is displayed. If you had to start isim1, a message similar to the following will be displayed: ADMU3000I: Server isim1 open for e-business; process id is 26654.

   Important: Servers must be started and stopped in a specific order.

   Start servers in this order:
   a. nodeagent
   b. isim1

   Stop servers in this order:
   a. isim1
   b. nodeagent

   The isim1 server is stopped by running the following command in a command window on the application server: /opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopServer.sh -all -username *WAS_ADMIN_USER* -password *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally admin) and *WAS_ADMIN_PWD* is the WebSphere Application Server administrator password.

   The nodeagent is stopped by running the following command in a command window on the application server: /opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopNode.sh -username *WAS_ADMIN_USER* -password *WAS_ADMIN_PWD* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally admin) and *WAS_ADMIN_PWD* is the WebSphere administrator password.
6. Verify that the isim1 server is started. Verification can be done using the WebSphere Application Server Administrative Console or by manual steps. The following are the steps using the WebSphere Application Server Administrative Console:
   a. Log on to the WebSphere Application Server Administrative Console at http://*APPLICATION_SERVER_HOST*:9061/ibm/console using the WebSphere Application Server Administrative ID admin and password. *APPLICATION_SERVER_HOST* is the host name for the application server.
   b. View the status of the isim1 server by clicking **Servers** > **Server Types** > **WebSphere application servers**.

The ➡ icon means the server is started. If required, select the server and click **Restart** to restart the server.

The ✖ icon means the server is stopped. Select the server and click **Start** to start the server.

The ? icon means the server status is unavailable. The Node Agent might not be running. To start the Node Agent run the `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/startNode.sh` command in a command window.

Important: Servers must be started and stopped in a specific order.

Start servers in this order:

a. nodeagent
b. isim1

Stop servers in this order:

a. isim1
b. nodeagent

To stop the isim1 server, select the server and click **Stop**.

The nodeagent is stopped by running the following command in a command window on the application server: `/opt/IBM/WebSphere/AppServerv7/profiles/isim1/bin/stopNode.sh -username` *`WAS_ADMIN_USER`* `-password` *`WAS_ADMIN_PWD`* where *WAS_ADMIN_USER* is the WebSphere administrator ID (normally `admin`) and *WAS_ADMIN_PWD* is the WebSphere administrator password.

What to do next

Resolve any issues or errors found and retry the test.

Security (WebSEAL) [1] Test

The Security (WebSEAL) [1] test determines the status of the IBM Security Access Manager WebSEAL server.

Resources

The Security (WebSEAL) [1] test uses the following resources:

- IBM Security Access Manager on the policy enforcement server.
- IBM Security Access Manager WebSEAL on the policy enforcement server.

Problem determination

If the Security (WebSEAL) [1] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the primary server, specify `status` for *action* and `websealpri` for *component*.
   - To check the status of the standby server, specify `status` for *action* and `websealsby` for *component*.
   - To start the primary server, specify `start` for *action* and `websealpri` for *component*.
   - To start the standby server, specify `start` for *action* and `websealsby` for *component*.
   - To stop the primary server, specify `stop` for *action* and `websealpri` for *component*.
   - To stop the standby server, specify `stop` for *action* and `websealsby` for *component*.

   Specify your topology password for *topology_password*.

```
su - ibmadmin

DOPControl -a action -c component -p topology_password
```

2. Review the log files for runtime exceptions.
   a. On the policy enforcement server review the following IBM Security Access Manager logs:
      - /var/PolicyDirector/log/msg__pdmgrd_utf8.log
      - /var/PolicyDirector/log/msg__pdacld_utf8.log
   b. On the policy enforcement server, review the following IBM Security Access Manager logs:
      - /var/ibm/tivoli/common/DPW/logs/msg__webseald-default.log
      - /var/ibm/tivoli/common/DPW/logs/www-default/log/*.log
3. Verify that the required IBM Security Access Manager WebSEAL components are running.
   a. Log on to a terminal session on the monitoring server as root.
   b. Run the **pd_start status** command. The results will be similar to the following:

```
Security Access Manager servers

Server         Enabled   Running
----------------------------------
pdmgrd           yes       yes
pdacld           yes       yes
pdmgrproxyd      no        no
```

   c. If the pdmgrd or pdacld servers are not running, start them by running the **pd_start start** command.

      Note: Only the pdmgrd and pdacld servers are enable on the monitoring server. Both are started with the **pd_start start** command and both can be stopped with the **pd_start stop** command.
4. Verify that the required IBM Security Access Manager WebSEAL components are running.
   a. Log on to a terminal session on the policy enforcement server 1 as root.
   b. Run the **pd_start status** command. The results will be similar to the following:

```
Security Access Manager servers

Server         Enabled   Running
----------------------------------
pdmgrd           no         no
pdacld           no         no
pdmgrproxyd      no         no
webseald-default yes        yes
```

   c. If the webseald-default server is not running, start it by running the **pd_start start** command.

      Note: Only the webseald-default server is enabled on the policy enforcement server 1. It is started with the **pd_start start** command and can be stopped with the **pd_start stop** command. The servers are: pdmgrd is the policy server, pdacld is the authorization server, pdmgrproxyd is the policy proxy server, and webseald-default is the WebSEAL server. The IBM Security Access Manager WebSEAL server is on both policy enforcement server servers and the IBM Security Access Manager authorization and policy servers is on the monitoring server.

What to do next

Resolve any issues or errors found and retry the test.

Security (WebSEAL) [2] Test

The Security (WebSEAL) [2] test determines the status of the IBM Security Access Manager WebSEAL server.

Resources

The Security (WebSEAL) [2] test uses the following resources:

- IBM Security Access Manager on the policy enforcement server.
- IBM Security Access Manager WebSEAL on the policy enforcement server.

Problem determination

If the Security (WebSEAL) [2] test fails, do the following to find and resolve the access problem.

Procedure

1. Use the platform control tool to check the status of the components and to start and stop them as needed. Run the following command with the desired options.
   - To check the status of the primary server, specify `status` for *action* and `websealpri` for *component*.
   - To check the status of the standby server, specify `status` for *action* and `websealsby` for *component*.
   - To start the primary server, specify `start` for *action* and `websealpri` for *component*.
   - To start the standby server, specify `start` for *action* and `websealsby` for *component*.
   - To stop the primary server, specify `stop` for *action* and `websealpri` for *component*.
   - To stop the standby server, specify `stop` for *action* and `websealsby` for *component*.

   Specify your topology password for *topology_password*.

   ```
   su - ibmadmin

   DOPControl -a action -c component -p topology_password
   ```
2. Review the log files for runtime exceptions.
   a. On the policy enforcement server review the following IBM Security Access Manager logs:
      - `/var/PolicyDirector/log/msg__pdmgrd_utf8.log`
      - `/var/PolicyDirector/log/msg__pdacld_utf8.log`

   b. On the policy enforcement server, review the following IBM Security Access Manager logs:
      - `/var/ibm/tivoli/common/DPW/logs/msg__webseald-default.log`
      - `/var/ibm/tivoli/common/DPW/logs/www-default/log/*.log`
3. Verify that the required IBM Security Access Manager WebSEAL components are running.
   a. Log on to a terminal session on the monitoring server as `root`.

   b. Run the **`pd_start status`** command. The results will be similar to the following:

   ```
   Security Access Manager servers

   Server         Enabled   Running
   -----------------------------------
   pdmgrd           yes       yes
   pdacld           yes       yes
   pdmgrproxyd      no        no
   ```

   c. If the pdmgrd or pdacld servers are not running, start them by running the **`pd_start start`** command.

   Note: Only the pdmgrd and pdacld servers are enable on the monitoring server. Both are started with the **`pd_start start`** command and both can be stopped with the **`pd_start stop`** command.
4. Verify that the required IBM Security Access Manager WebSEAL components are running.
   a. Log on to a terminal session on the policy enforcement server 2 as root.

   b. Run the **`pd_start status`** command. The results will be similar to the following:

   ```
   Security Access Manager servers

   Server         Enabled   Running
   -----------------------------------
   ```

```
pdmgrd           no         no
pdacld           no         no
pdmgrproxyd      no         no
webseald-default yes        yes
```

c. If the webseald-default server is not running, start it by running the **`pd_start start`** command.

   Note: Only the webseald-default server is enabled on the policy enforcement server 2. It is started with the **`pd_start start`** command and can be stopped with the **`pd_start stop`** command. The servers are: `pdmgrd` is the policy server, `pdacld` is the authorization server, `pdmgrproxyd` is the policy proxy server, and `webseald-default` is the WebSEAL server. The IBM Security Access Manager WebSEAL server is on both policy enforcement server servers and the IBM Security Access Manager authorization and policy servers is on the monitoring server.

What to do next

Resolve any issues or errors found and retry the test.

Logging and analyzing usage data

IBM Defense Operations Platform logs usage data that can them be processed using a usage analysis application.

These logs provide information on session activities such as login, logout, time out, and login failures. The log entries comply with the NCSA combined industry standard.

By analyzing the log entries you can monitor the usage of IBM Defense Operations Platform.

Usage analysis logs

IBM Defense Operations Platform usage records are written to dedicated log files. WebSphere Portal is configured to rotate the logs every six hours. The rotation interval can be customized.

The usage analysis logs can be found on the application server in the Field Edition and on application server 1 and application server 2 in the Command Center Edition.The logs are in the following directory:

```
wp_root/logs/wp_server_name/SiteAnalyzerLogs
```

where *wp_root* is the WebSphere Portal home directory and *wp_server_name* is the WebSphere Portal server name.

Log files are named in the following format: sa_*CREATE_TIME_CLOSE_TIME*.log where *CREATE_TIME* is the timestamp when the log was created and *CLOSE_TIME* is the timestamp when the log was closed. The *CREATE_TIME* and *CLOSE_TIME* timestamps are in *YYYY.MM.DD-hh.mm.ss* format; where *YYYY* is year, *MM* is month, *DD* is day, *hh* is hour, *mm* is minutes and *ss* is seconds.

Logging must be enabled to capture usage analysis data. Logging is enabled by default.

Related information:

Enabling site analysis logging in WebSphere Portal

Running the usage analysis tool

The usage analysis tool processes the usage analytics logs and saves the data for realtime and historical reporting purposes.

About this task

The tool stores the following analysis information in the USAGEAN database in the SCHUSAG.USAGEDATA table. The processed logs are stored in the /opt/IBM/WebSphere/usageAnalysis/Archive_*date_time* directory where *date_time* is the timestamp when the tool was run.

- src_ip - the source IP address where the WebSphere Portal URL (req_url) request originated.
- req_user - the user who requested the WebSphere Portal URL (req_url).
- req_datetime - the date and time when the WebSphere Portal URL (req_url) was requested.
- req_url - the WebSphere Portal URL that was requested by the user (req_user).
- cookies - the cookies that were passed with the WebSphere Portal URL (req_url) request.
- sa_filename - the name of the processed usage analytics log file.
- p_server - the WebSphere Portal server where the usage analytics log file (sa_filename) originated. This information is useful for installations with more than one WebSphere Portal node.
- created - the date and time when the entry was created in the database.

The Usage Analysis tool can be configured by changing the following properties in the /opt/IBM/WebSphere/usageAnalysis/runAnalysisTool.sh file.

- IS_DEBUG can be set to yes or no indicating whether debug statements are displayed when the Usage Analysis tool is run. The default is no indicating that debug statements are not displayed.
- IS_FORCE can be set to yes or no indicating if a previously processed usage analysis file should be reprocessed. When set to yes existing entries in the database are deleted and the log is reprocessed.

To run the usage analytics tool, do the following.

Procedure

1. In the Field Edition, sign on to the application server server as the ibmadmin user. In the Command Center Edition, sign on to application server 1 and application server 2 in turn and run the following steps.
2. Change to the *was_root*/usageAnalysis directory where *was_root* is the WebSphere Application Server home directory. For example, /opt/IBM/WebSphere/usageAnalysis.
3. Run **./runAnalysisTool.sh -h** *database_server_hostname* **-p** *db2inst1_password*

   Where *database_server_hostname* is the host name of the data server or data server 1 and *db2inst1_password* is the password defined by the DEFAULT.PWD.DB2 in the topology properties file.

Results

The analysis results are written to the USAGEAN database.

Modifying the installation password

The installation password is used during the installation process to encrypt and access the file defining the solution topology. The password is created during the installation process when a keystore is created. If required, the password can be changed by deleting the keystore and specifying a new installation password.

About this task

On the installation server, go to the directory where the IBM Defense Operations Platform installation package was copied. In these steps, this directory is referred to as *install_home*.

Procedure

1. Log on as `root` or switch to the root account by running the **`su -`** command.
2. Change to the *`install_home`*`/dop16` directory.
3. Delete the *`install_home`*`/dop16/resource/ioc.keystore` file.
4. Run the **`./dop.d2.install.sh 3 -p`** *installation_password* command for the Field Edition or the **`./dop.d1.install.sh 3 -p`** *installation_password* command for the Command Center Edition where *installation_password* is the password to be created for the installation.
5. Make a note of the password for future use.

   Important: The installation password is needed when running or rerunning the command line installer. The initial installation password is also used as the topology password. However, changing the installation password using this process does not change the topology password. The topology password is changed using a different procedure.

Related tasks:

"Modifying the topology password"
The topology password is used to protect password information required for IBM Defense Operations Platform operation and maintenance. This password can be changed to meet organizational requirements.

Modifying the topology password

The topology password is used to protect password information required for IBM Defense Operations Platform operation and maintenance. This password can be changed to meet organizational requirements.

About this task

The platform control tool uses passwords to run software components across the topology. These passwords are protected by IBM Defense Operations Platform using encryption based on the topology password. The topology password is used to encrypt and decrypt the password information.

The initial topology password is the installation password defined when IBM Defense Operations Platform is installed. The topology password can be changed and the appropriate file encrypted using the new password.

Procedure

1. Log on to the messaging server (Field Edition) or messaging server 1 (Command Center Edition) as the `ibmadmin` user.
2. Run the following command to encrypt the protected passwords using a new topology password.

   ```
   iopmgmt-updatePCTpw.sh -p old_topology_password -n new_topology_password
   ```

   Where, *old_topology_password* is the current topology password, and *new_topology_password*is the new topology password. If the password values contain any special characters, the password must be enclosed in single quotes (for example: `'pass_word'`).

Results

The topology properties file containing passwords used by IBM Defense Operations Platform is encrypted using the new topology password.

What to do next

Use the new topology password when running the platform control tool (DOPControl).

Related tasks:

"Modifying the installation password" on page 176
The installation password is used during the installation process to encrypt and access the file defining the solution topology. The password is created during the installation process when a keystore is created. If required, the password can be changed by deleting the keystore and specifying a new installation password.

Updating the LTPA token for single sign-on

IBM Defense Operations Platform uses a Lightweight Third-Party Authentication (LTPA) token to enable single sign-on across many services. The token and keys generated during installation do not expire. It is a good security practice to periodically regenerate the LTPA token and update the services using it.

Before you begin

The IBM Defense Operations Platform product must be installed and all services started before updating the LTPA token.

This procedure requires that all services are stopped and started, so the update should not be done while the system is in production. Any users logged into the system will experience a service disruption and can lose data.

Procedure

Generate a new LTPA token for the application server

1. If running the Field Edition, on the application server open a web browser and go to `http://`*`application_host`*`:9062/ibm/console` where *application_host* is the host name of the application server.
2. If running the Command Center Edition, on the application server 1 open a web browser and go to `http://`*`application_host`*`:9062/ibm/console` where *application_host* is the host name of the application server 1.
3. Log on as the `admin` user with the password specified in the topology properties file `WAS.ADMIN.ACCOUNT.PWD` parameter.
4. Click **Security** > **Global Security** > **LTPA**.
5. Enter a password twice for the new LTPA token. The password is used to encrypt the LTPA token. This password will be used when importing the LTPA token. Record the password as the `WAS.LTPA.PWD` parameter in the topology properties file.
6. Enter the path and filename where the LTPA token will be saved, for example, `/tmp/newapp.ltpa`. If you specify a different path or file name, substitute your path and filename for `/tmp/newapp.ltpa` in the rest of these steps.
7. Click **Export Keys**. The new LTPA token is saved as `/tmp/newapp.ltpa`.
8. Click **Messages** > **Save**. Updates will be saved. Ignore any warnings about the single sign-on domain not being defined.
9. On the application server, log on as the `root` user and open a terminal window.
10. Run the **`cp /tmp/newapp.ltpa /opt/IBM/ISP/stproxy.ltpa`** command. This replaces the file that was created when IBM Defense Operations Platform was installed.

Update single sign-on for the collaboration service.

11. Follow the steps in "Configuring single sign-on for collaboration services" on page 44 to update single sign-on for the collaboration service.

Stop and restart all services.

12. Using the platform control tool stop all services.
13. Using the platform control tool start all services. LTPA tokens will be propagated between WebSphere Application Server and the Lotus Domino server.

Setting the session timeout

The session timeout determines the time a user can remain idle before the session is terminated and the user must log in again. The session time out includes administrators logged in through the portal service.

About this task

When IBM Defense Operations Platform is installed, no session time out is defined. Users will stay logged in until they log out even if the session is idle.

If your organization has security policies requiring that sessions log out after a period of inactivity, use the following steps to define a session timeout for your IBM Defense Operations Platform system.

Procedure

Configure server timeouts.

1. In the Field Edition, using a web browser go to `http://`*`application_server`*`:9062/ibm/console` where *application_server* is the host name of the application server.
2. In the Command Center Edition, using a web browser go to `http://`*`application_server`*`:9062/ibm/console` where *application_server* is the host name of application server 1.
3. Log on as the `admin` user with the password defined for `PORTAL.ADMIN.ACCOUNT.PWD` in the topology properties file.
4. Click **Servers** > **Server Type** > **WebSphere Application Servers** > **WebSphere Portal**.
5. Click **Container Settings** > **Session management** > **Set Timeout**.
6. Enter the desired timeout value in minutes.
7. Click **OK**.
8. Click **Save**.
9. Click **Servers** > **Server Type** > **WebSphere Application Servers** > **STProxyServer1**.
10. Click **Container Settings** > **Session management** > **Set Timeout**.
11. Enter the desired timeout value in minutes.
12. Click **OK**.
13. Click **Save**.

If running the Command Center Edition, configure the following additional servers.

14. Click **Servers** > **Server Type** > **WebSphere Application Servers** > **WebSphere_Portal_PortalNode2**.
15. Click **Container Settings** > **Session management** > **Set Timeout**.
16. Enter the desired timeout value in minutes.
17. Click **OK**.
18. Click **Save**.

Restart the server.

19. Stop and restart the application server in the Field Edition or application server 1 in the Command Center Edition using the platform control tool.

Setting the LTPA timeout

The Lightweight Third-Party Authentication (LTPA) timeout determines the time a user can remain logged on before the session is terminated and the user must log in again. The LTPA time out includes administrators logged in through the portal service.

About this task

When IBM Defense Operations Platform is installed, an LTPA timeout of 150 minutes is configured. Users will stay logged in until they log out after 150 minutes have elapsed.

If your organization has security policies requiring that sessions log out after a different period of time, use the following steps to define the LTPA timeout for your IBM Defense Operations Platform system.

Procedure

1. In the Field Edition, using a web browser go to `http://`*`application_server`*`:9062/ibm/console` where *application_server* is the host name of the application server.
2. In the Command Center Edition, using a web browser go to `http://`*`application_server`*`:9062/ibm/console` where *application_server* is the host name of application server 1.
3. Log on as the `admin` user with the password defined for `PORTAL.ADMIN.ACCOUNT.PWD` in the topology properties file.
4. Click **Security** > **Global security** > **LTPA**.
5. Enter the desired **LPTA timeout** value in minutes.
6. Click **Apply**.
7. Click **Save**.
8. Stop and restart all IBM Defense Operations Platform components using the platform control tool. If IBM Defense Operations Platform is still being installed, the servers will be restarted during installation full verification.

Chapter 4. Troubleshooting and support

To isolate and resolve problems with your IBM software, you can use the troubleshooting and support information, which contains instructions for using the problem-determination resources that are provided with your IBM products.

IBM Installation Manager fails to launch

The installer fails to launch and returns messages including a floating point exception and a core dump.

Symptoms

Messages similar to the following are returned when running the installer.

```
(Launcher:2554): GLib-GObject-WARNING **: invalid (NULL) pointer instance
(Launcher:2554): GLib-GObject-CRITICAL **: g_signal_connect_data: assertion `G_TYPE_CHECK_INSTANCE (instance)' failed
(Launcher:2554): Pango-CRITICAL **: pango_layout_get_line_count: assertion `layout != NULL' failed
Floating point exception (core dumped)
```

Resolving the problem

WebSphere Application Server and WebSphere Portal updates installed by IBM Installation Manager must be run as the ibmadmin user. Installation launch errors might be because IBM Installation Manager was previously run as the root user. Required files are locked and owned by the root user and cannot be access by the ibmadmin user. To resolve the problem, do the following:

1. On the application server where WebSphere Application Server or WebSphere Portal require updates, start a terminal session and log on as the root user.
2. Run the following commands:
   ```
   chown -R ibmadmin:ibmadmins /opt/IBM/InstallationManager
   su - ibmadmin
   cd /opt/IBM/InstallationManager/eclipse
   ./launcher
   ```
3. IBM Installation Manager should now run successfully.

WebSphere components fail to start

The platform control tool (DOPControl) cannot start WebSphere Application Server Network Deployment, the WebSphere Node Agent, or WebSphere Application Server components.

Symptoms

The platform control tool (DOPControl) indicates that one or more of the WebSphere components are not started and the WebSphere startServer.log file contains a message similar to the following:

```
[MM/DD/YY HH:MM:SS:nnn XXX] 00000000 AdminTool A ADMU3011E: Server launched but failed
initialization. Server logs, startServer.log, and other log files under
/opt/IBM/...../logs/...... should contain failure information.
```

Resolving the problem

WebSphere Application Server components must be started using the platform control tool (DOPControl) run as the ibmadmin user. Component start errors might be because start commands were previously run as the root user. In this case required files are locked and owned by the root user and cannot be access by the ibmadmin user. To resolve the problem, do the following:

1. On the server where the WebSphere Application Server component failed to start, start a terminal session and log on as the `root` user.
2. Run the following command:

   ```
   chown -R ibmadmin:ibmadmins websphere_profile_directory
   ```

   Where Table 22 shows the value for *websphere_profile_directory* depending on the failing DOPControl component.

Table 22. Value for websphere_profile_directory based on failing DOPControl component

websphere_profile_directory **value**	**DOPControl Command Center Edition components**	**DOPControl Field Edition components**
`/opt/IBM/WebSphere/AppServer/profiles/dmgr`	`appdmgrpri`	`appdmgr`
`/opt/IBM/WebSphere/AppServer/profiles/IopProfile1`	`ioppri`	`iop`
`/opt/IBM/WebSphere/AppServer/profiles/IopProfile2`	`iopsby`	Not applicable
`/opt/IBM/WebSphere/wp_profile`	`wpepri`, `wpesby`	`wpe`
`/opt/IBM/WebSphere/AppServer7/profiles/isim1`	`isimpri`	`isim`
`/opt/IBM/WebSphere/AppServer7/profiles/STPAppProfile1`	`stproxypri`	`stproxy`
`/opt/IBM/WebSphere/AppServer/profiles/bpmpProfile1`	`bpmpri`	Not applicable
`/opt/IBM/WebSphere/AppServer/profiles/wsrrProfile1`	`wsrrpri`	Not applicable
`/opt/IBM/WebSphere/AppServer85/profiles/dmgr`	`prodmgrpri`	Not applicable
`/opt/IBM/WebSphere/AppServer85/profiles/odmdcProfile1`	`odmdcpri`	Not applicable
`/opt/IBM/WebSphere/AppServer85/profiles/odmProfile1`	`odmpri`	Not applicable

3. Run the platform control tool (DOPControl) as the `ibmadmin` user to start the failing component.

Unable to start the LDAP server using the Tivoli Directory Server Web Administration Tool

When trying to start the LDAP server using the Tivoli Directory Server Web Administration Tool, an HTTP 500 error is returned and the LDAP server will not start.

Resolving the problem

Start Tivoli Directory Server using the platform control tool.

Related concepts:

"Starting, stopping, and querying status in the Field Edition" on page 53
The platform control tool allows a user to stop, start, and query IBM Defense Operations Platform components running in the Field Edition. A platform control tool tool is also available for IBM Defense Operations Platform running in the Command Center Edition.

"Starting, stopping, managing and querying status in the Command Center Edition" on page 57
The platform control tool allows a user to stop, start, and query IBM Defense Operations Platform services running in the Command Center Edition. A platform control tool tool is also available for IBM Defense Operations Platform running in the Field Edition.

Chapter 5. Reference

It is important to understand the configuration of the installed IBM Defense Operations Platform system. These references help you understand the installed products, ports used, processes requiring root access, and accessibility features. Additional legal references are also included.

Products and components installed with IBM Defense Operations Platform Field Edition

The IBM Defense Operations Platform solution installs a number of software products and components for the Field Edition.

The software products and components and the servers they are installed on are shown in Table 23.

Table 23. Products installed with IBM Defense Operations Platform

Product	Application server	Messaging server	Data server
Tivoli Directory Server 6.3.0.18	not installed	not installed	installed
Tivoli Directory Server Web Application 6.3.0.18	installed	not installed	not installed
DB2 Enterprise Server Edition 10.1.0.1	not installed	not installed	installed
DB2 10.1.0.1 Client	installed	not installed	not installed
Tivoli Directory Integrator 7.1.1.2	plug-in features installed	plug-in features installed	installed
Tivoli Directory Integrator Dispatcher 6.0.6	not installed	not installed	installed
Tivoli Directory Integrator POSIX adapter 6.0.24	not installed	not installed	installed
IBM Installation Manager 1.6.0	installed	not installed	installed (optional)
WebSphere Application Server Network Deployment v7.0.0 Fix Pack 29 (7.0.0.29)	installed	not installed	not installed
WebSphere Application Server Network Deployment v8.0.0 Fix Pack 7 (8.0.0.7)	installed	not installed	not installed
WebSphere Application Server 1.1.0.3 Feature Pack for Web 2.0 and Mobile	installed	not installed	not installed
WebSphere Portal Enable v8.0.0 Fix Pack 1 Cumulative Fix 5 (8.0.0.1 CF05)	installed	not installed	not installed
WebSphere HTTP Server v8.0.0 Fix Pack 7 (8.0.0.7)	installed	not installed	not installed
WebSphere MQ 7.5.0	not installed	installed	not installed
WebSphere Message Broker 8.0.0 Fix Pack 1 (8.0.0.1)	not installed	installed	not installed
IBM Java 1.7.0 SR5	not installed	installed	not installed
Lotus Domino 8.5.3 upgrade pack 1	installed	not installed	not installed
IBM Sametime Standard 8.5.2 Interim Feature Release 1 (8.5.2.1)	installed	not installed	not installed
IBM Worklight Consumer Edition 6.0.0 (optionally available through IBM Industry Solutions services)	installed	not installed	not installed
Lotus Sametime Proxy 8.5.2	installed	not installed	not installed
IBM Security Identity Manager 6.0	installed	not installed	not installed
Data Studio 3.2.0 (Optional component)	not installed	not installed	**Note:** IBM Installation Manager 1.6.0 will also be installed on this server if Data Studio is installed.

Products and components installed with IBM Defense Operations Platform Command Center Edition

The IBM Defense Operations Platform solution installs a number of software products and components for the Command Center Edition.

The software products and components and the servers they are installed on are shown in Table 24.

Table 24. Products installed with IBM Defense Operations Platform

Product	Application server 1	Application server 2	Messaging server 1	Messaging server 2	Data server 1	Data server 2	Policy enforcement server 1	Policy enforcement server 2	Monitoring server	Process server
Tivoli Directory Server 6.3.0.18	not installed	not installed	not installed	not installed	installed	installed	not installed	not installed	not installed	not installed
Tivoli Directory Server Proxy 6.3.0.18	installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed

Table 24. Products installed with IBM Defense Operations Platform (continued)

Product	Application server 1	Application server 2	Messaging server 1	Messaging server 2	Data server 1	Data server 2	Policy enforcement server 1	Policy enforcement server 2	Monitoring server	Process server
Tivoli Directory Server Web Application 6.3.0.18	installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed
DB2 Enterprise Server Edition 10.1.0.1	not installed	not installed	not installed	not installed	installed	installed	not installed	not installed	installed	not installed
DB2 10.1.0.1 Client	installed	installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed
Tivoli Directory Integrator 7.1.1.2	plug-in features installed	plug-in features installed	plug-in features installed	plug-in features installed	all features installed	plug-in features installed	plug-in features installed	plug-in features installed	plug-in features installed	plug-in features installed
Tivoli Directory Integrator Dispatcher 6.0.6	not installed	not installed	not installed	not installed	installed	not installed	not installed	not installed	not installed	not installed
Tivoli Directory Integrator POSIX adapter 6.0.24	not installed	not installed	not installed	not installed	installed	not installed	not installed	not installed	not installed	not installed
IBM Installation Manager 1.6.0	installed	installed	not installed	not installed	installed (optional)	installed (optional)	not installed	not installed	not installed	installed
WebSphere Application Server Network Deployment v7.0.0 Fix Pack 29 (7.0.0.29)	installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed
WebSphere Application Server Network Deployment 8.5.5	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	installed
WebSphere Application Server Network Deployment 8.0.0.7	installed	installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	installed
WebSphere Application Server 1.1.0.3 Feature Pack for Web 2.0 and Mobile	installed	installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	installed
WebSphere Portal 8.0.0.1.CF05	installed	installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed
IBM Security Access Manager Web Portal Manager 7.0.0.1	installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed
IBM HTTP Server 8.0.0.7	installed	installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	installed
IBM HTTP Server 8.5.5	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	installed
WebSphere MQ 7.5.0	not installed	not installed	installed	installed	not installed	not installed	not installed	not installed	not installed	not installed
WebSphere MQ Explorer 7.5.0	not installed	not installed	installed	installed	not installed	not installed	not installed	not installed	not installed	not installed
WebSphere Message Broker 8.0.0 Fix Pack 1 (8.0.0.1)	not installed	not installed	installed	installed	not installed	not installed	not installed	not installed	not installed	not installed
IBM Java 1.7.0 SR5	not installed	not installed	installed	installed	not installed	not installed	not installed	not installed	not installed	not installed
Lotus Domino 8.5.3 upgrade pack 1 (8.5.3 Upgrade Pack 1)	installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed
IBM Sametime Standard 8.5.2 Interim Feature Release 1 (8.5.2.1)	installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed
IBM Worklight Consumer Edition 6.0.0 (optionally available through IBM Industry Solutions services)	installed	installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed
Lotus Sametime Proxy 8.5.2	installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed
IBM Security Identity Manager 6.0	installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed

Table 24. Products installed with IBM Defense Operations Platform (continued)

Product	Application server 1	Application server 2	Messaging server 1	Messaging server 2	Data server 1	Data server 2	Policy enforcement server 1	Policy enforcement server 2	Monitoring server	Process server
Data Studio 3.2.0 (Optional component)	not installed	not installed	not installed	not installed	**Note:** IBM Installation Manager 1.6.0 will also be installed on this server if Data Studio is installed.	**Note:** IBM Installation Manager 1.6.0 will also be installed on this server if Data Studio is installed.	not installed	not installed	not installed	not installed
IBM Security Access Manager WebSEAL 7.0.0 Fix Pack 1 (7.0.0.1)	not installed	not installed	not installed	not installed	not installed	not installed	installed	installed	not installed	not installed
Tivoli Netcool/ OMNIbus 7.4.0.2	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	installed	not installed
IBM Security Access Manager 7.0.0.1	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	installed	not installed
Tivoli Application Performance Manager 7.6.0.1	agents only	agents only	agents only	agents only	agents only	agents only	agents only	agents only	installed	agents only
WebSphere Service Registry and Repository 8.0.0 Fix Pack 2 (8.0.0.2)	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	installed
WebSphere Operational Decision Management 8.5	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	installed
Business Process Manager Advanced 8.0.1 Fix Pack 1 (8.0.1.1)	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	not installed	installed

Ports used by Command Center Edition servers

IBM Defense Operations Platform Command Center Edition uses specific ports.

The ports used by the Command Center Edition are shown in Table 25.

Table 25. Ports used by the Command Center Edition

Server	Ports required for product use
Application server 1	80, 84, 389, 443, 1352, 1516, 1533, 1920, 1976, 2810, 2811, 2812, 2813, 2814, 3538, 3661, 5000, 5001, 5002, 5003, 5004, 5005, 6014, 7272, 7273, 7274, 7756, 7278, 7287, 8008, 8082, 8878, 8879, 8881, 8883, 8884, 8885, 8886, 9044, 9045, 9047, 9061, 9062, 9064, 9081, 9082, 9083, 9092, 9094, 9101, 9102, 9104, 9105, 9201, 9202, 9203, 9204, 9205, 9206, 9352, 9355, 9356, 9357, 9358, 9359, 9404, 9405, 9407, 9409, 9414, 9415, 9416, 9417, 9444, 9445, 9446, 9629, 9630, 9631, 9632, 9634, 9636, 9637, 9809, 9811, 9900, 9902, 9904, 10025, 10029, 10030, 10033, 10034, 10035, 10036, 10037, 10039, 10110, 14206, 18302, 20831, 20832, 60148
Application server 2	80, 443, 1920, 2809, 2810, 3661, 5000, 5001, 5002, 5003, 6014, 7272, 8008, 8878, 8879, 8885, 9048, 9083, 9105, 9201, 9202, 9203, 9204, 9353, 9354, 9359, 9446, 9629, 9630, 9637, 9812, 9900. 9902, 10043, 10044, 10045, 10047, 10048, 10050, 10051, 10053, 10056, 10110, 14206
Data server 1	389, 523, 1098, 1099, 1920, 3538, 3661, 3766, 6014, 7756, 10110, 11852, 14206,15948, 18001, 50001, 50002, 55002, 55003, 55044, 55005, 55006, 55007,55013, 55014, 55015, 55016, 55017, 55018, 55019, 55020, 55021, 55022, 55023, 55024, 55025
Data server 2	389, 523, 1098, 1099, 1920, 3538, 3661, 3766, 6014, 7756, 10110, 11852, 14206, 15948,18001, 50001, 50002, 55002, 55003, 55044, 55005, 55006, 55007,55013, 55014, 55015, 55016, 55017, 55018, 55019, 55020, 55021, 55022, 55023, 55024, 55025
Messaging server 1	1920, 3661, 4414, 6014, 10110, 14206
Messaging server 2	1920, 3661, 4414, 6014, 10110, 14206

Table 25. Ports used by the Command Center Edition (continued)

Server	Ports required for product use
Policy enforcement server 1	80, 443, 1920, 3661, 6014, 7234, 7756
Policy enforcement server 2	80, 443, 1920, 3661, 6014, 7234, 7756
Monitoring server	523, 1918, 1920, 3660, 3661, 4100, 4200, 6014, 7135, 7136, 7137, 7756, 9998, 9999, 10110, 11852, 14206, 15001, 15200, 15201, 15202, 15203, 15204, 15205, 15206, 15207, 15208, 15210, 15211, 15214, 15948, 20044, 50001
Process server	80, 443, 1920, 2809, 2810, 2811, 2812, 2815, 3661, 5000, 5001, 5002, 5003, 5004, 5005, 5006, 5007, 6014, 7060, 7062, 7063, 7272, 7273, 7274, 7275, 7277, 7756, 7282, 7283, 7290, 7291, 8008, 8878, 8879, 8880, 8881, 8882, 8883, 8884, 8887, 8888, 9043, 9044, 9045, 9049, 9050, 9060, 9061, 9062, 9066, 9067, 9080, 9081, 9084, 9085, 9100, 9101, 9102, 9106, 9107, 9201, 9202, 9203, 9204, 9205, 9206, 9207, 9208, 9352, 9353, 9354, 9355, 9356, 9357, 9358, 9361, 9362, 9402, 9403, 9405, 9406, 9408, 9409, 9420, 9421, 9423, 9424, 9425, 9443, 9444, 9447, 9448, 9629, 9630, 9631, 9632, 9633, 9634, 9635, 9638, 9639, 9809, 9810, 9811, 9812, 9900, 9902, 9904, 9906, 10110, 11003, 11004, 11005, 11006, 11007, 11008, 11009, 11010, 11011, 11012, 11852, 14206, 15948

Ports used by Field Edition servers

IBM Defense Operations Platform Field Edition uses specific ports.

The ports used by the Field Edition are shown in Table 26.

Table 26. Ports used by the Field Edition

Server	Ports required for product use
Application server	80, 84, 443, 1352, 1516, 1533, 2810, 2811, 2812, 2813, 2814, 5000, 5001, 5002, 5003, 5004, 5005, 7272, 7273, 7274, 7278, 7287, 8082, 8878, 8879, 8881, 8883, 8884, 8885, 8886, 9044, 9045, 9047, 9061, 9062, 9064, 9081, 9082, 9083, 9092, 9094, 9100, 9101, 9102, 9104, 9105, 9201, 9202, 9203, 9204, 9205, 9206, 9352, 9355, 9356, 9357, 9358, 9359, 9404, 9407,9409, 9414, 9415, 9416, 9417, 9444, 9445, 9446, 9629, 9630, 9631, 9632, 9634, 9636, 9637, 9809, 9811, 9900, 9902, 9904, 10025, 10029, 10030, 10033, 10034, 10035, 10036, 10037, 10039, 10788, 20831, 20832, 60148
Data server	389, 523, 3538, 3766, 18001, 50001, 50002
Messaging server	4414

Processes running under the `root` account

After cyber hygiene completes, some processes must still run under the `root` account.

Processes running under the `root` account can be vulnerable if a user or process can obtain `root` privileges through privilege escalation. Normally this is only a problem for services processing requests originated by a user. User-originated requests can contain maliciously configured input that can compromise the server. Services processing user requests are systems providing user interfaces or accessible application programming interfaces (APIs).

Linux daemons are not normally at risk since they usually only start, stop, or respond to well-defined system events. In many cases these daemons must run as the `root` account so they can control other processes or respond to critical system events. As long as a user-accessible server itself is not running as `root`, daemons running under the `root` account do not present as serious an exposure.

Accessibility

Accessibility features help users with physical disabilities, such as restricted mobility or limited vision, to use software products successfully.

The major accessibility features in this product enable users to do the following:

- Use assistive technologies, such as screen-reader software and digital speech synthesizer, to hear what is displayed on the screen. Consult the product documentation of the assistive technology for details on using those technologies with this product.
- Operate specific or equivalent features using only the keyboard.
- Magnify what is displayed on the screen.

In addition, the documentation was modified to include the following features to aid accessibility:

- All documentation is available in XHTML formats to give the maximum opportunity for users to apply screen-reader software technology.
- All images in the documentation are provided with alternative text so that users with vision impairments can understand the contents of the images.

Copyright notice and trademarks

Copyright notice

© Copyright IBM Corporation 2011, 2013. All rights reserved. May only be used pursuant to an IBM software license agreement. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without prior written permission of IBM Corporation. IBM Corporation grants you limited permission to make hardcopy or other reproductions of any machine-readable documentation for your own use, provided that each such reproduction shall carry the IBM Corporation copyright notice. No other rights under copyright are granted without prior written permission of IBM Corporation. The document is not intended for production and is furnished "as is" without warranty of any kind. **All warranties on this document are hereby disclaimed, including the warranty of non-infringement and the implied warranties of merchantability and fitness for a particular purpose.**

U.S. Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corporation.

Trademarks

Cognos®, CPLEX®, IBM, ibm.com®, DB2, Domino, GDDM®, ILOG®, Lotus, Notes, Passport Advantage, Rational®, Sametime, Tivoli, Service Request Manager®, Smarter Cities®, SPSS®, Redbooks®, WebSphere, and Worklight, are trademarks of the IBM Corporation in the United States, other countries, or both.

Microsoft, Internet Explorer, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Adobe, Acrobat, Portable Document Format (PDF), and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Oracle, Javascript, JavaBeans, and Java are registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other names may be trademarks of their respective owners. Other company, product, and service names may be trademarks or service marks of others.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

This Software Offering uses cookies for session management and single sign-on configuration. If you disable cookies, you will not be able to access the system.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

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:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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
Department T81B F6/Building 503
4205 S. Miami Boulevard
Durham NC 27709-9990
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 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. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

Cognos, CPLEX, IBM, ibm.com, DB2, Domino, GDDM, ILOG, Lotus, Notes, Passport Advantage, Rational, Sametime, Tivoli, Service Request Manager, Smarter Cities, SPSS, Redbooks, WebSphere, and Worklight, are trademarks of the IBM Corporation in the United States, other countries, or both.

Microsoft, Internet Explorer, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Adobe, Acrobat, Portable Document Format (PDF), and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Oracle, Javascript, JavaBeans, and Java are registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other names may be trademarks of their respective owners. Other company, product, and service names may be trademarks or service marks of others.

Index

Readers’ Comments — We'd Like to Hear from You

IBM Defense Operations Platform
IBM Defense Operations Platform
Product Documentation
Version 1 Release 6

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:
- Send your comments to the address on the reverse side of this form.
- Send a fax to the following number: 1-800-227-5088 (US and Canada)

If you would like a response from IBM, please fill in the following information:

Name	Address
Company or Organization	
Phone No.	Email address

Readers' Comments — We'd Like to Hear from You

IBM®

Cut or Fold
Along Line

Fold and Tape Please do not staple Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM
Information Development Department DLUA
P.O. Box 12195
Research Triangle Park, NC
USA 27709-9990

Fold and Tape Please do not staple Fold and Tape

Cut or Fold
Along Line

Printed in USA