Application Note: Veritas High Availability Solution for DLP Enforce Server

Windows

7.0

Veritas InfoScale™ Availability Agents

Last updated: 2018-07-09

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

xyz@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Veritas High Availability solution for DLP Enforce Server

This document includes the following topics:

- Introduction
- Components of the High Availability solution for DLP Enforce Server
- About installing and configuring DLP Enforce Server for high availability
- Sample configurations
- Service group and resource dependencies
- Troubleshooting

Introduction

This application note describes the Veritas High Availability solution for Symantec Data Loss Prevention (DLP) Enforce Server. In this solution, DLP Enforce Server services are managed using the GenericService agent. The GenericService agent brings specific Enforce Server services online, monitors their state, detects failures, and takes the services offline.

About Data Loss Prevention

Symantec Data Loss Prevention (DLP) answers three fundamental questions:

- Where is your confidential data?

- How is it being used?
- How do you prevent data loss?

DLP delivers a unified solution to discover, monitor, and protect confidential data wherever it is stored or used. DLP Enforce Platform automatically enforces universal data loss prevention policies with a centralized platform for detection, incident remediation workflow and automation, reporting, system management, and security.

For details, refer to the DLP documentation.

Supported software

The Veritas High Availability solution for DLP Enforce Server supports the following software:

Cluster Server (VCS)	VCS 5.1 SP2 or later
Operating Systems	Microsoft Windows Server 2008 R2 (x64) or later
Symantec DLP	11.1
Component	Enforce Server

About DLP Enforce Server

Review the recommendations for the different installation tiers and the Enforce Server services that are supported:

DLP installation tiers

DLP supports the following installer types:

- **Single-tier**
  To implement the single-tier installation, you install the database, the Enforce Server, and a detection server, all on the same computer.
- **Two-tier**
  To implement the two-tier installation, you install the Oracle database and the Enforce Server on the same computer. You then install detection servers on separate computers.
- **Three-tier**
  To implement the three-tier installation, you install the Oracle database, the Enforce Server, and a detection server on separate computers.

Veritas recommends that you implement the three-tier installation architecture, as it enables your database administration team to control the database. In this way, you can use all of your standard corporate tools for database backup, recovery, monitoring, performance, and maintenance. Three-tier installations require that you install the Oracle Client (SQL*Plus and Database Utilities) on the Enforce Server to communicate with the Oracle server.

This document also provides details on the required VCS configuration based on the type of installation tier.

DLP Enforce Server services

Services for DLP 15.1 and later	Services for older DLP versions	Description
Symantec DLP Incident Persister	Vontu Incident Persister	Writes the incidents to the database.
Symantec DLP Manager	Vontu Manager	Provides the centralized reporting and management services for DLP.
Symantec DLP Detection Server Controller	Vontu Monitor Controller	Controls the detection servers (monitors).
Symantec DLP Notifier	Vontu Notifier	Provides the database notifications.
Symantec DLP Update	Vontu Update	Installs the DLP system updates. This service only runs during system updates and upgrades.

Components of the High Availability solution for DLP Enforce Server

Storage Foundation and High Availability Solutions for DLP Enforce Server on Windows contains the following components:

Storage Foundation

The Storage Foundation components brings advanced volume management technology, quick recovery, and fault tolerant capabilities to enterprise computing environments.

Cluster Server

The Cluster Server (VCS) component provides is a high availability solution that monitors system and application services, and restarts services when hardware or software fails. A VCS cluster connects multiple independent systems to provide failover capability, thus reducing application downtime. VCS supports local, metropolitan, and global clusters.

VCS agent for Oracle

DLP Enforce Server stores incident data in an Oracle database. The VCS database agent for Oracle provides high availability for Oracle in a VCS cluster. The VCS database agent for Oracle monitors the Oracle database and listener services, brings them online, and takes them offline. For details, see the to *Cluster Server Database Agent for Oracle Configuration Guide*.

VCS agent used to cluster DLP Enforce Server services

VCS uses the GenericService agent to provide high availability for DLP Enforce Server. The GenericService agent brings the DLP services online, takes them offline, and monitors their status. Note that a service is an application type that is supported by Windows and that conforms to the interface rules of the Service Control Manager (SCM).

Table 1-1 Agent functions

Fucntion	Description
online	Starts the configured service.
offline	Stops the configured service.
monitor	Verifies the user context of the configured service, if applicable, and retrieves its current state.

Note: To configure a service for high availability by using the GenericService agent, the Startup Type of the service must be Manual and its Status must be Stopped.

For earlier versions of DLP, the following services can be clustered by using the GenericService agent:

- Vontu Incident Persister
- Vontu Manager
- Vontu Monitor Controller
- Vontu Notifier
- Vontu Update

For DLP 15.1 or later, the following services can be clustered by using the GenericService agent:

- Symantec DLP Incident Persister
- Symantec DLP Manager
- Symantec DLP Detection Server Controller
- Symantec DLP Notifier
- Symantec DLP Update

Note: On Windows platforms, all the DLP services run under the System Account user name (by default, `protect`), except for the Symantec DLP Update service or the Vontu Update service, which runs under *`username`*`_update` (by default, `protect_update`).

For details on the GenericService agent, see the *Cluster Server Bundled Agents Reference Guide* for Windows.

VCS storage agents

The VCS agents for storage management (storage agents) make shared storage highly available. The Volume Manager Diskgroup (VMDg) and the MountV agents provide high availability for shared disks and volumes that are managed using the Storage Foundation components.

For details on the storage agents, see the *Cluster Server Bundled Agents Reference Guide* for Windows.

VCS network agents

The VCS agents for network management (network agents) make IP addresses and computer names highly available. The NIC and the IP agents work together to make a virtual IP address highly available. The Lanman agent makes a virtual computer name highly available, and it requires the IP agent to perform its operations.

For details on the network agents, see the *Cluster Server Bundled Agents Reference Guide* for Windows.

About installing and configuring DLP Enforce Server for high availability

This section includes the installation and configuration requirements for the various components that are involved in making DLP Enforce Server highly available. References to product documentation are provided based on the component of the solution that is involved.

Installation of Veritas products

Install InfoScale Enterprise or Storage Foundation and High Availability Solutions for Windows (SFW HA) on all the systems on which you plan to host DLP Enforce Server or its Oracle database. For details on the installation and upgrade procedures, see the *Veritas InfoScale Installation and Upgrade Guide* or the *Veritas Storage Foundation and High Availability Solutions Installation and Upgrade Guide* for Windows. These documents also list the services and ports that are required for installing and using the products.

Administration of VCS service groups

The *Cluster Server Administrator's Guide* explains clustering concepts and terminology. It provides information on how to administer VCS resources and service groups using the Java console as well as using the command line. Troubleshooting information is also included.

Configuration of Oracle for high availability

The *Symantec Data Loss Prevention Oracle 11g Installation and Upgrade Guide* provides Oracle installation and upgrade steps. It also provides the steps to create the DLP database and the required Oracle accounts.

- For single-tier and two-tier DLP installations, Oracle is installed on the server where Enforce Server is installed.
- For a three-tier installation, Oracle is installed on a separate server. The Oracle Client (SQL*Plus and Database Utilities) must be installed on the server where Enforce Server is installed, so that they can communicate with the Oracle server.

The strategy for installing Oracle in a VCS cluster is aimed at ensuring that the Oracle installation on all the nodes in the cluster is uniform. This involves installing the Oracle binaries locally on each system. You can perform this installation simultaneously on multiple cluster nodes. The installer screens and options may vary for different versions of Oracle. The *Cluster Server Database Agent for Oracle Configuration Guide* lists the VCS requirements for Oracle installation and how to configure the corresponding VCS resources for that Oracle installation.

By switching the Oracle service group between the VCS cluster nodes you can verify whether Oracle is correctly set up for high availability.

Configuration of DLP Enforce Server for high availability

Take the following considerations into account before you deploy and configure DLP for high availability:

- The Oracle software and the DLP database must be installed on the cluster nodes that can host the Oracle database.
- DLP Enforce Server must be installed on all the cluster nodes so that the DLP Enforce Server services get created on all the possible failover nodes.
- The DLP installation directory must be present on the shared storage. The VCS storage agents make the shared storage highly available.
  The default installation directory is: `C:\Vontu`.
  Veritas recommends that you use the default installation directory.
- The `protect` user must have the correct permissions to access and modify the contents of the DLP installation directory on all the cluster nodes.
- The `jdbc.properties` file must be updated with the Oracle virtual IP information to ensure that the Oracle instance failover works correctly.
  The VCS network agents make IP addresses and computer names highly available.

Creation of VCS service groups for DLP Enforce Server

Configuring the high availability solution for DLP Enforce Server involves creating the following service groups:

- DLP Enforce service group
  This service group is used for clustering the DLP Enforce Server services. In a DLP Enforce service group, each DLP Enforce Server service is clustered by using a resource of the GenericService type. The Symantec DLP Notifier or the Vontu Notifier service must be started before any other DLP services are started. To address this requirement, make the VCS resources that correspond to other DLP services dependent on the VCS resource for the Symantec DLP Notifier or the Vontu Notifier service. VCS resources are also created for the storage and the network components that are required by DLP.
- Oracle service group
  This service group is used for clustering the database and the listener services. In an Oracle service group, the database and the listener services are clustered by using the Oracle and the Netlistener resources respectively. VCS resources are also created for the storage and the network components that are required by Oracle.

Effect of DLP installation tiers on VCS service group configuration

Veritas recommends that the Oracle resources and the Enforce Server resources should be part of different service groups.

- For single-tier and two-tier DLP installations: Veritas recommends that the DLP Enforce Server service group should have the Online Local Firm dependency on the Oracle service group. This service group-level dependency ensures that both the service groups are online on the same node in the cluster.
- For three-tier installations: Veritas recommends that DLP Enforce Server service group should have the Online Global Firm dependency on the Oracle service group. With this configuration, the Oracle service group and the DLP Enforce Server service group can be brought online on any node in the cluster independent of each other.

For details on service group dependencies, see the *Cluster Server Administrator's Guide* for Windows.

Sample configurations

The sample configurations graphically depict the resource types, resources, and resource dependencies within the service group. Review these dependencies carefully before configuring the DLP Enforce Server services for high availability by using the GenericService agent.

For details on these resource types, see the `Cluster Server Bundled Agents Reference Guide` for Windows.

Sample GenericService agent resource type definition

```
type GenericService (
  static i18nstr ArgList[] = { ServiceName, DelayAfterOnline,
    DelayAfterOffline, UserAccount, Password, Domain,
    service_arg, UseVirtualName, "LanmanResName:VirtualName" }
  i18nstr ServiceName
  int DelayAfterOnline = 10
  int DelayAfterOffline = 10
  i18nstr UserAccount
  str Password
  i18nstr Domain
  str service_arg[]
  boolean UseVirtualName = 0
  str LanmanResName
)
```

Sample configuration in a VCS environment

The following sample `main.cf` file includes the GenericService agent resources that are used to cluster the DLP Enforce Server services and the Oracle agent resource that is used to cluster the Oracle database.

This sample configuration is for a three-tier installation of DLP. The service group-level dependency must be changed based on the DLP installation tiers.

Sample service group configuration for earlier versions of DLP:

```
include "types.cf"
cluster DLPClus (
 UserNames = { admin = GnoGniNkoJooMwoInl, a = dqqK }
 Administrators = { admin, a }
 )

system NODE1 (
 )

system NODE2 (
 )

group DLPSG (
 SystemList = { NODE1 = 0, NODE2 = 1 }
 )

 GenericService VontuNotifier_res (
  ServiceName = VontuNotifier
  )

 GenericService VontuIncidentPersister_res (
  ServiceName = VontuIncidentPersister
  )

 GenericService VontuMonitorController_res (
  ServiceName = VontuMonitorController
  )

 GenericService VontuUpdate_res (
  ServiceName = VontuUpdate
  )

 GenericService VontuManager_res (
  ServiceName = VontuManager
  )

 IP dlp_ip_res (
  Address = "10.209.68.246"
  SubNetMask = "255.255.252.0"
  MACAddress @NODE1 = 00-1D-09-65-E9-3B
  MACAddress @NODE2 = 00-1D-09-65-D5-8C
  )

 Lanman EnforceHost_lanman_res (
  VirtualName = enforcehost
  IPResName = dlp_ip_res
  )

 MountV dlp_mount_res (
  MountPath = "C:\\Vontu"
  VolumeName = DlpSofvol
  VMDGResName = dlp_dg_res
  )

 NIC dlp_nic_res (
  Enabled = 0
  MACAddress @NODE1 = 00-1D-09-65-E9-3B
  MACAddress @NODE2 = 00-1D-09-65-D5-8C
  )

 VMDg dlp_dg_res (
  DiskGroupName = DlpSofdg
  )

 requires group OraSG online global firm
 VontuNotifier_res requires dlp_mount_res
 VontuNotifier_res requires EnforceHost_lanman_res
 VontuIncidentPersister_res requires VontuNotifier_res
 VontuMonitorController_res requires VontuNotifier_res
 VontuUpdate_res requires dlp_mount_res
 VontuManager_res requires VontuNotifier_res
 dlp_ip_res requires dlp_nic_res
 EnforceHost_lanman_res requires dlp_ip_res
 dlp_mount_res requires dlp_dg_res

 // resource dependency tree
 //
```

```
// group DLPSG
// {
// GenericService VontuIncidentPersister_res
//     {
//     GenericService VontuNotifier_res
//         {
//         MountV dlp_mount_res
//             {
//             VMDg dlp_dg_res
//             }
//         Lanman EnforceHost_lanman_res
//             {
//             IP dlp_ip_res
//                 {
//                 NIC dlp_nic_res
//                 }
//             }
//         }
//     }
// GenericService VontuMonitorController_res
//     {
//     GenericService VontuNotifier_res
//         {
//         MountV dlp_mount_res
//             {
//             VMDg dlp_dg_res
//             }
//         Lanman EnforceHost_lanman_res
//             {
//             IP dlp_ip_res
//                 {
//                 NIC dlp_nic_res
//                 }
//             }
//         }
//     }
// GenericService VontuUpdate_res
//     {
//     MountV dlp_mount_res
//         {
//         VMDg dlp_dg_res
//         }
//     }
```

```
 // GenericService VontuManager_res
 //     {
 //     GenericService VontuNotifier_res
 //         {
 //         MountV dlp_mount_res
 //             {
 //             VMDg dlp_dg_res
 //             }
 //         Lanman EnforceHost_lanman_res
 //             {
 //             IP dlp_ip_res
 //                 {
 //                 NIC dlp_nic_res
 //                 }
 //             }
 //         }
 //     }
 // }

group OraSG (
 SystemList = { NODE1 = 0, NODE2 = 1 }
 )

 IP ora_ip_res (
  Address = "10.209.68.244"
  SubNetMask = "255.255.252.0"
  MACAddress @NODE1 = 00-1D-09-65-E9-3B
  MACAddress @NODE2 = 00-1D-09-65-D5-8C
  )

 MountV ora_mount_res (
  MountPath = "C:\\oracle\\db"
  VolumeName = DbVol
  VMDGResName = ora_dg_res
  )

 NIC ora_nic_res (
  MACAddress @NODE1 = 00-1D-09-65-E9-3B
  MACAddress @NODE2 = 00-1D-09-65-D5-8C
  )

 Netlsnr netlsnr_res (
  ServiceName = OracleOraDb11g_home1TNSListener
  )

 Oracle oradb_protect_res (
  ServiceName = OracleServicePROTECT
  Domain = isv
  SID = protect
  UserName = administrator
  EncryptedPasswd = JXPvMXm
  SQLFile = "C:\\Program Files\\Veritas\\cluster server\\
    bin\\Oracle\\check.SQL"
  )

 VMDg ora_dg_res (
  DiskGroupName = DlpDBdg
  )

 netlsnr_res requires oradb_protect_res
 oradb_protect_res requires ora_mount_res
 oradb_protect_res requires ora_ip_res
 ora_mount_res requires ora_dg_res
 ora_ip_res requires ora_nic_res

 // resource dependency tree
 //
 // group OraSG
 // {
 // Netlsnr netlsnr_res
 //     {
 //     Oracle oradb_protect_res
 //         {
 //         MountV ora_mount_res
 //             {
 //             VMDg ora_dg_res
 //             }
 //         IP ora_ip_res
 //             {
 //             NIC ora_nic_res
 //             }
 //         }
 //     }
 // }
```

Sample service group configuration for DLP 15.1 and later:

```
include "types.cf"

cluster DLPCLUS (
 SecureClus = 1
 )

system DLPHOST1 (
 )

system DLPHOST2 (
 )

group SymcDLP_SG (
 SystemList = { DLPHOST1 = 0 }
 )

 GenericService SymcDLP_DT_Res (
  Critical = 0
  ServiceName @DLPHOST1 = SymantecDLPDetectionServer
  Password = E
  Domain = peregrine
  )

 GenericService DLPDetectionServer_Controller_Res (
  ServiceName = SymantecDLPdetectionServerController
  )

 GenericService DLPIncisdentPersister_Res (
  ServiceName = SymantecDLPIncidentPersister
  )

 GenericService SymantecDLPManager_Res (
  ServiceName = SymantecDLPManager
  )

 GenericService DLPNotifier_Res (
  ServiceName = SymantecDLPNotifier
  )

 SymcDLP_DT_Res requires DLPNotifier_Res
 DLPDetectionServer_Controller_Res requires DLPNotifier_Res
 DLPIncisdentPersister_Res requires DLPNotifier_Res
 SymantecDLPManager_Res requires DLPNotifier_Res
```

```
// resource dependency tree
//
// group SymcDLP_SG
// {
// GenericService SymcDLP_DT_Res
//     {
//     GenericService DLPNotifier_Res
//     }
// GenericService DLPDetectionServer_Controller_Res
//     {
//     GenericService DLPNotifier_Res
//     }
// GenericService DLPIncisdentPersister_Res
//     {
//     GenericService DLPNotifier_Res
//     }
// GenericService SymantecDLPManager_Res
//     {
//     GenericService DLPNotifier_Res
//     }
// }
```

Service group and resource dependencies

This section depicts sample service group and resource dependencies for the DLP Enforce Server and the Oracle service groups and resources.

Service group dependency (Java console view)

The following figures illustrate a sample VCS configuration with different service group dependencies based on the DLP installation tiers.

Figure 1-1 Service group dependency view for a three-tier installation of DLP

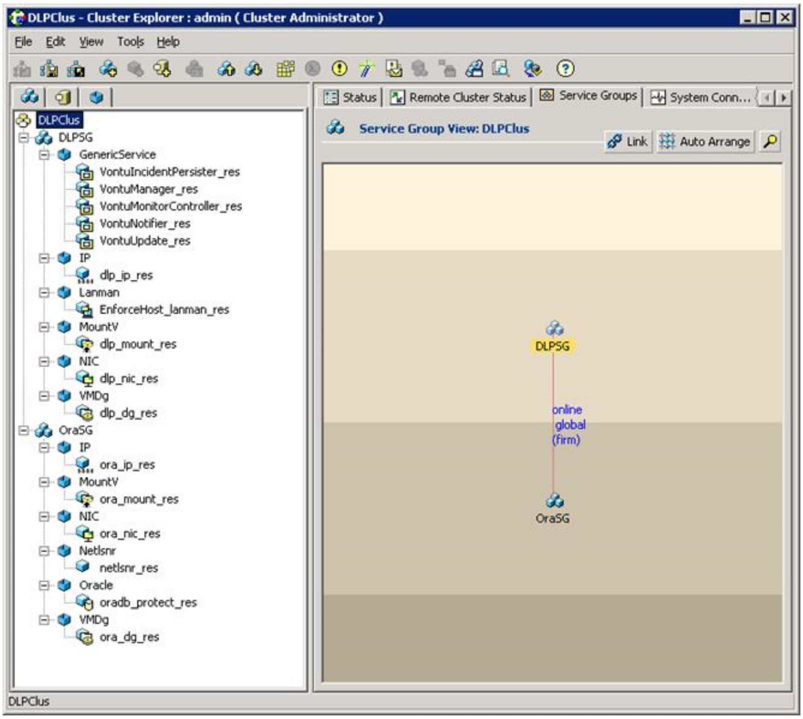


Figure 1-1 shows the service group dependency graph for a three-tier installation of DLP; the DLP Enforce Server service group has an Online Global Firm dependency on the Oracle service group.

Figure 1-2 Service group dependency view for a 2-tier installation of DLP

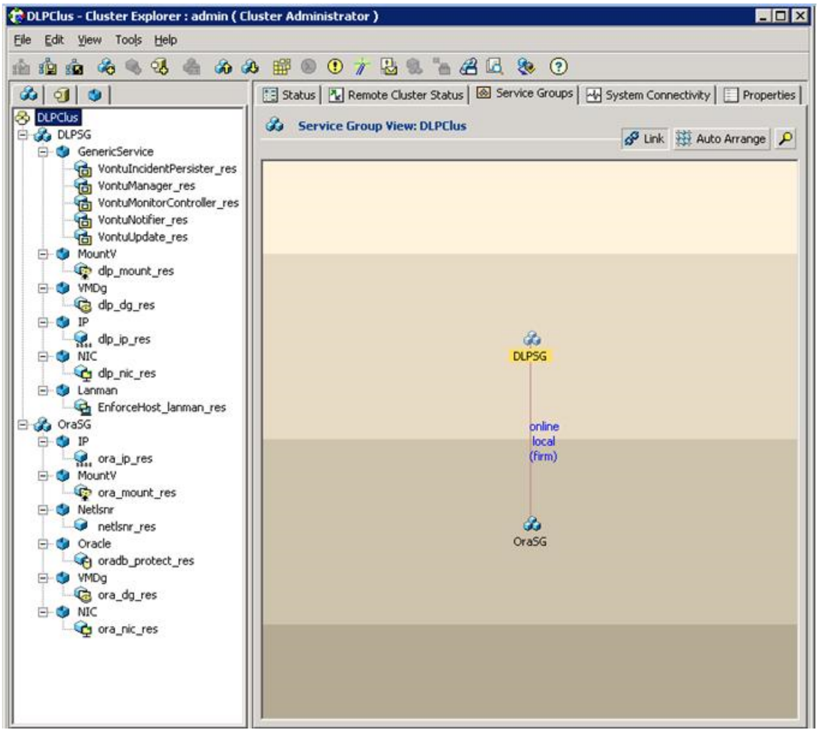


Figure 1-2 shows a service group dependency graph for a two-tier installation of DLP; the DLP Enforce Server service group has an Online Local Firm dependency on the Oracle service group.

Resource dependency (Java console view)

The following figures illustrate a sample VCS configuration with the resource dependencies for the DLP Enforce Server service group and the Oracle service group.

Figure 1-3 Resource dependency view for the DLP Enforce service group

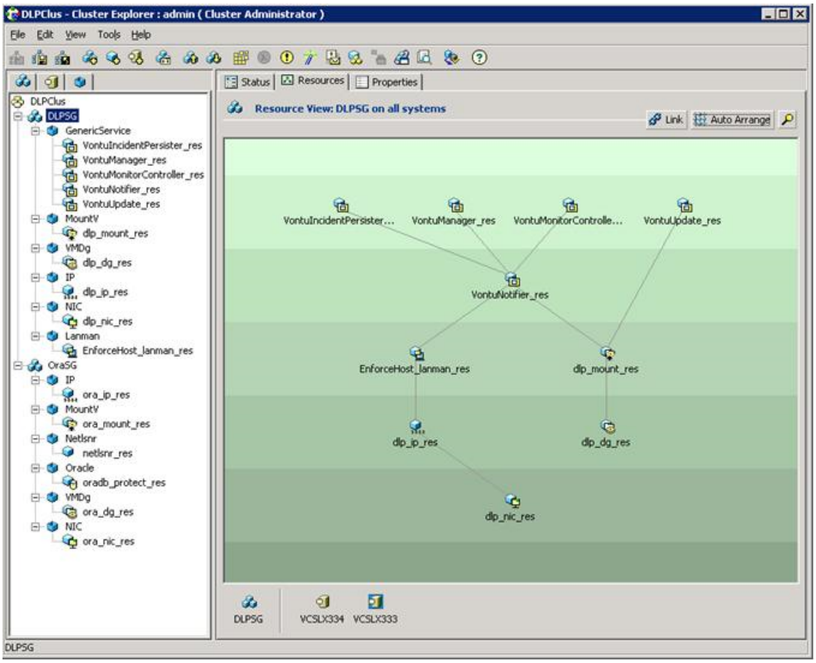


Figure 1-3 shows a resource dependency graph for the DLP Enforce Server service group. In this graph, the resources that correspond to the Vontu Incident Persister, the Vontu Manager, and the Vontu Monitor Controller services depend on the resource that corresponds to the Vontu Notifier service. The storage and the network resources provide the infrastructure that is necessary for the Vontu services to function.

Figure 1-4 Resource dependency view for the Oracle service group

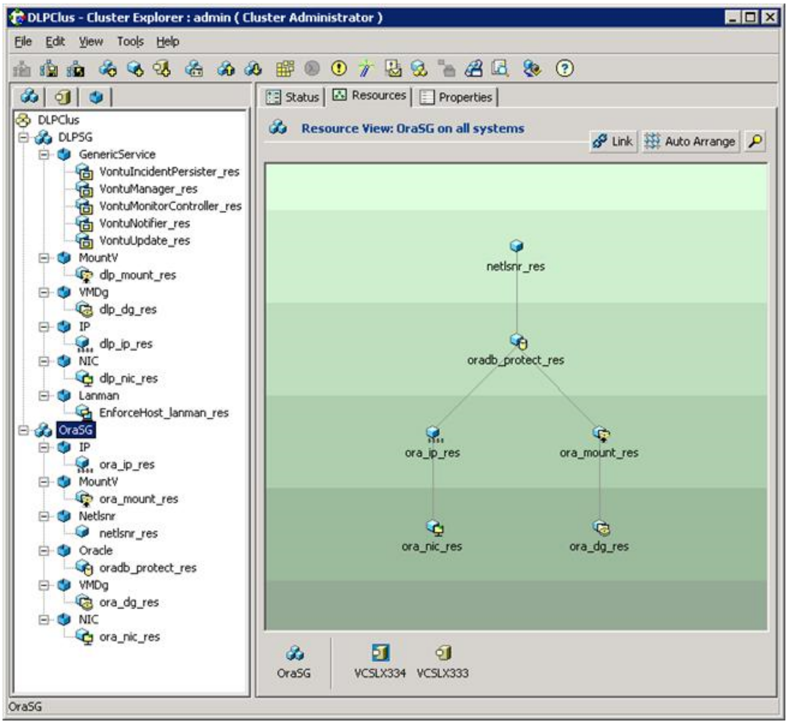
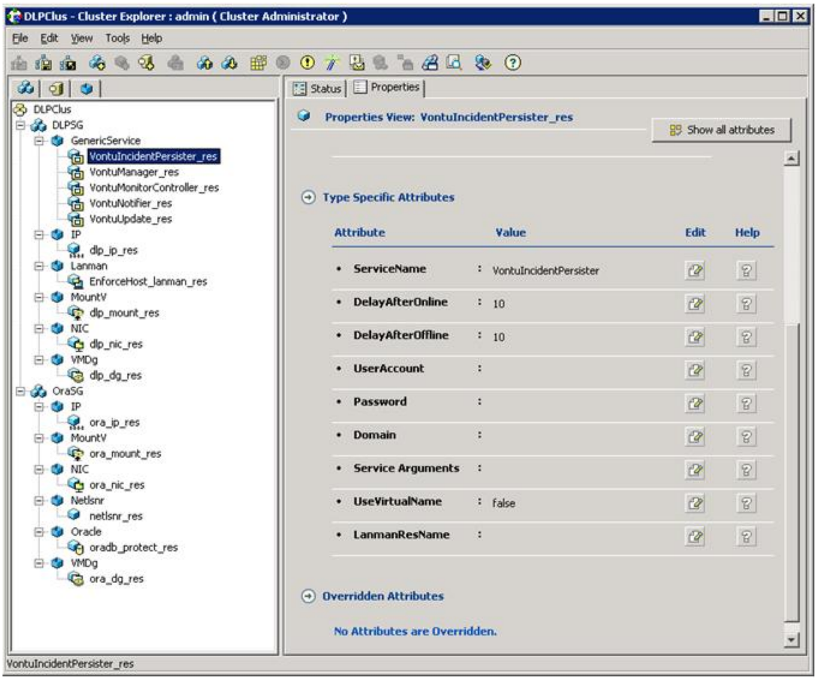


Figure 1-4 shows a resource dependency graph for the Oracle service group. In this graph, the Netlsnr resource depends on the Oracle resource, which in turn depends on the storage and the network resources.

Properties for GenericService resource (Java console view)

The following figure illustrates a sample VCS configuration with properties set for the GenericService resource that corresponds to the Vontu Incident Persister service. The properties for the other Vontu services must be set in a similar manner.

Figure 1-5 Properties of GenericService resource for Vontu Incident Persister



Attribute	Value
ServiceName	VontuIncidentPersister
DelayAfterOnline	10
DelayAfterOffline	10
UserAccount	
Password	
Domain	
Service Arguments	
UseVirtualName	false
LanmanResName	

No Attributes are Overridden.

In Figure 1-5, for the previously mentioned GenericService resource that corresponds to the Vontu Incident Persister service, the ServiceName attribute is set to VontuIncidentPersister.

Troubleshooting

This section describes how to troubleshoot common problems in the VCS configuration for DLP. References are provided to the appropriate product documentation.

VCS logging

VCS generates two error message logs, the engine log and the agent log:

- The engine log is located at `%VCS_HOME%\log\engine_A.txt`.
- The agent log is located at `%VCS_HOME%\log\agent_A.txt`.

Log file names are appended by letters; the letter A indicates the first log file, B the second, C the third, and so on.

GenericService agent error messages

For a list of the GenericService agent error message descriptions and recommended actions, see the *Cluster Server Bundled Agent Reference Guide* on Windows.

Troubleshooting details for VCS agent for Oracle

For a list of some commonly encountered problems with the VCS database agent for (Oracle agent) and some possible solutions, see the *Cluster Server Database Agent for Oracle Configuration Guide* on Windows. This document also lists the error messages that are associated with the agent.

DLP log locations

If the DLP services do not start, check the log files for possible issues. For example, you may encounter issues with connectivity, passwords, or database access.

The DLP installation log is located at `C:\Vontu\.install4j\installation.log`.

The DLP operational logs are located at `C:\Vontu\Protect\logs`.

Starting an Enforce Server on Windows outside VCS control

Perform the following tasks to start the DLP services on a Windows Enforce Server:

1. On the computer that hosts the Enforce Server, open the Services window.
2. Start the Symantec DLP Notifier or the Vontu Notifier service.
3. Start the remaining DLP services, including the following:
   - Symantec DLP Incident Persister or Vontu Incident Persister
   - Symantec DLP Manager or Vontu Manager
   - Symantec DLP Detection Server Controller or Vontu Monitor Controller
   - Symantec DLP Update or Vontu Update

Stopping an Enforce Server on Windows outside VCS control

Perform the following tasks to stop the DLP services on a Windows Enforce Server:

1. On the computer that hosts the Enforce Server, open the Services window.
2. Stop all the DLP services that are running, which may include:
   - Symantec DLP Incident Persister or Vontu Incident Persister
   - Symantec DLP Manager or Vontu Manager

- Symantec DLP Detection Server Controller or Vontu Monitor Controller
- Symantec DLP Update or Vontu Update
- Symantec DLP Notifier or the Vontu Notifier

Recursive permissions for `protect` user on DLP installation directory

Ensure that the `protect` user has the permissions that are required to access and to modify the contents of the DLP Enforce Server installation directory on each of the cluster nodes. The default DLP installation location is `C:\Vontu`.