Symantec Data Center Security: Server Advanced Overview Guide

Documentation version: 1.1

Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.
Technical Support

Symantec Technical Support maintains support centers globally. Technical Support’s primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec’s support offerings include the following:

■ A range of support options that give you the flexibility to select the right amount of service for any size organization
■ Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
■ Upgrade assurance that delivers software upgrades
■ Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
■ Premium service offerings that include Account Management Services

For information about Symantec’s support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

■ Product release level
■ Hardware information
Available memory, disk space, and NIC information
Operating system
Version and patch level
Network topology
Router, gateway, and IP address information
Problem description:
  Error messages and log files
  Troubleshooting that was performed before contacting Symantec
  Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:
www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:
www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:
  Questions regarding product licensing or serialization
  Product registration updates, such as address or name changes
  General product information (features, language availability, local dealers)
  Latest information about product updates and upgrades
  Information about upgrade assurance and support contracts
  Information about the Symantec Buying Programs
  Advice about Symantec's technical support options
  Nontechnical presales questions
  Issues that are related to CD-ROMs, DVDs, or manuals
Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan                     customercare_apj@symantec.com
Europe, Middle-East, and Africa            semea@symantec.com
North America and Latin America           supportsolutions@symantec.com
Symantec Data Center Security: Server Advanced Overview

This document includes the following topics:

- About Symantec Data Center Security: Server Advanced
- About DCS:S and DCS:SA
- About Unified Management Console
- About Operations Director
- About the DCS:SA components
- How do I achieve my objectives with DCS:SA
- How DCS:S works
- Where to get more information

About Symantec Data Center Security: Server Advanced

Symantec Data Center Security: Server Advanced (DCS:SA) provides a policy-based approach to endpoint security and compliance. The intrusion prevention and detection features of DCS:SA operate across a broad range of platforms and applications. It provides:

- A policy-based host security agent for monitoring and protection.
- Proactive attack prevention using the least privilege containment approach.
- A centralized management environment for enterprise systems that contain Windows, UNIX, and Linux computers.

### Table 1-1  DCS:SA capabilities

<table>
<thead>
<tr>
<th>Security and protection</th>
<th>Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time proactive enforcement</td>
<td>Real-time monitoring and auditing</td>
</tr>
<tr>
<td>Intrusion and malware prevention</td>
<td>Host intrusion detection</td>
</tr>
<tr>
<td>System hardening</td>
<td>File integrity monitoring</td>
</tr>
<tr>
<td>Application control</td>
<td>Configuration monitoring</td>
</tr>
<tr>
<td>Privileged user access control</td>
<td>Tracking and monitoring of user access</td>
</tr>
<tr>
<td>Vulnerability and patch mitigation</td>
<td>Logging and event reporting</td>
</tr>
<tr>
<td>Does not use signatures or require continual updates to content</td>
<td></td>
</tr>
</tbody>
</table>

The major features of DCS:SA are as follows:

- Intrusion detection facility for compliance auditing
  - Real-time file integrity monitoring
  - Granular change detection of registry values, file contents, and attributes
  - Operating system and application log monitoring
  - Local event correlation and smart response actions
- Intrusion Prevention facility for malware prevention and system lockdown
  - Sandbox containment of operating system and application processes by an in-kernel reference monitor
  - Granular access control of network, file systems, registry, process-to-process memory access, system calls, and application and child process launches
  - Privileged user and program behavior
- Anti-malware security
  DCS:SA Security Virtual Appliance (SVA) provides agentless anti-malware security services for the virtualized network through integration with the VMware Network and Security Virtualization (NSX) platform. SVA provides two types of policies: Antivirus policies, and configuration policies.
- Comprehensive out-of-the-box policies for complete system monitoring and protection of physical and virtual systems
- Security orchestration using Operations Director. Operations Director is intended to:
Automate security provisioning workflow.

Provide application-centric security service.

Seamlessly integrate with VMware NSX.

Provide out-of-box security product integration.

Centralized management environment for administering agents, policies, and events.

Integration with Security Information and Event Management (SIEM) and other security tools, as well as enterprise infrastructure components such as Active Directory, SMTP, and SNMP.

Broad platform support across Windows, Linux, UNIX and virtual environments for critical servers, workstations, laptops, and standalone systems.

The major benefits of DCS:SA are as follows:

- Reduces emergency patching and minimizes patch-related downtime and IT expenses through proactive protection that does not require continuous updates.

- Reduces incidents and remediation costs with continuous security. Once the agent has a policy, it enforces the policy even when the computer is not connected to the corporate network. And even if a computer is unable to obtain the latest patches in a timely fashion, DCS:SA continues to block attacks so that the computer is always protected.

- Provides visibility and control over the security posture of business-critical enterprise assets.

- Uses predefined compliance and hardening policies to provide efficient security management, reporting, alerting, and auditing of activities. Also provides compensating controls for compliance failures.

**About DCS:S and DCS:SA**

This document describes the features of Symantec Data Center Security: Server Advanced (DCS:SA). If you have purchased Symantec Data Center Security: Server (DCS:S), you are only entitled to a subset of these features. The features and components included in each product are described below:

- DCS:S entitles you to agentless anti-malware protection for your VMware guest VMs, via integration with the VMware NSX platform, as well as monitoring and hardening your VMware infrastructure.

In addition, DCS:S lets you orchestrate security using Operations Director. By using the intelligence of Operations Director, you can provision a vApp/VM with the right security policies.
DCS:SA extends DCS:S and allows you to monitor and protect physical and virtual data centers using a combination of host-based intrusion detection (HIDS), intrusion prevention (HIPS), and least privilege access control. Fully instrumented REST API provides corresponding API for all console actions to enable full internal and external Cloud automation.

About Unified Management Console

The Unified Management Console (UMC) is a console appliance that provides a web-based console for NSX virtual data center protection and orchestration. The console is used to register and configure various features and products in Symantec Data Center Security: Server Advanced (DCS:SA).

UMC provides unification of the common tasks across DCS:S, DCS:SA, and Operations Director.

A UMC administrator has the required rights and permissions to configure and set up the DCS:SA products.

About Operations Director

Operations Director is a security orchestration feature of Data Center Security: Server. Operations Director automates and simplifies security provisioning for virtual applications by assessing the security requirements for applications and applying the appropriate security policies. Operations Director automates policy provisioning through orchestration with security point products and the VMware NSX, an industry leading software-defined data center (SDDC) network virtualization and security platform. Operations Director is the software-defined security service for the NSX SDDC platform.

Operations Director delivers automated security management for software-defined data centers. A SDDC extends the virtualization concepts such as abstraction, pooling, and automation — to all data center resources and services. In a SDDC, new applications are provisioned on-demand and are ready for business consumption almost instantaneously. However, with traditional security processes and workflows, identification of the right security controls and the provisioning of the security policies by using various security point products can take days or weeks. Operations Director integrates into the SDDC automation framework to ensure that security provisioning is completed in the order of minutes.

The security orchestration feature powered by Symantec Operations Director is the latest addition to the Symantec Data Center Security portfolio and is intended to:

- Automate security provisioning workflow.
Provide application-centric security service.
Seamlessly integrate with VMware NSX.
Provide out-of-box security product integration.

All you have to do is:
- Configure Symantec Data Center Security plug-in in vSphere Web client.
- Deploy the Symantec Data Center Security Unified Management Console (UMC) appliance in vCenter.
- Deploy Operations Director appliance in vCenter.
- Register the Operations Director appliance with UMC.

To know more about configuration and product deployment, refer any of the following:
- Symantec Data Center Security Operations Director Reference Guide
- Symantec Data Center Security online help
- Symantec Data Center Security: Server Advanced Planning and Deployment Guide

The documents are available at:
www.symantec.com/business/support/index?page=content&id=DOC8101

See “Advantages of Operations Director” on page 11.
See “Orchestrating security using Operations Director” on page 20.

Advantages of Operations Director

Following are the advantages of Operations Director:
- Integrated into vSphere Web client and NSX; easy to deploy and get into action.
- Leverages Symantec-defined tags along with vCenter tags to derive the right security posture for you.
- Interoperates with security point products.
- Automates complex and manual decision making.
- Delivers out-of-box security intelligence using security tags mapped to best-practice mandates, controls, and security product policies, and can be easily customized to map user-defined best practice policies.
About the DCS:SA components

DCS:SA includes management console and server components, includes agent components that provide intrusion prevention and detection on physical or virtual computers, and includes the Security Virtual Appliance (SVA) that provides agentless anti-malware protection for VMware guest VMs running Windows. The management server and management console run on Windows operating systems. The management console can be accessed using thick console only. The agents run on Windows and UNIX operating systems. UMC, SVA, and OD are virtual appliances. The UMC is deployed using the VMware. The SVA is deployed into VMWare NSX using the Unified Management Console. The OD is deployed on UMC using the VMware vCenter.

The management components of DCS:SA can be installed on one system or in a distributed model. Agents are generally deployed to every supported host to be monitored and protected, including the management server, management console, and SQL server database. Remote monitoring can extend file integrity monitoring and log monitoring functionality to systems where no native agent exists. For example, such systems include mainframe zLinux, AS 400, VAX, or VMS systems. The DCS:SA management console is available in both a Web browser or as a standalone thick client.

The following diagram displays the DCS:SA environment setup:
Figure 1-1  DCS:SA environment setup

vCenter Servers
vCenter Server Application
Web Console

vCenter NSX
OD Plug-in

Panorama Management Server
(Palo Alto Networks)

Operations Director
(Virtual Appliance)

UMC Server
(Virtual Appliance)

DCS:SA Management Server
(VM/Physical Server)

DCS:Server Advanced
Console

ESXi HOST
SV A V irtual Appliance

UMC Web Console

Agent

Physical Server
LINUX

Physical Server
LINUX

Physical Server
LINUX

Physical Server
Windows

Physical Server
Windows

Physical Server
Windows

Physical Server
Windows

Symantec Data Center Security: Server Advanced Overview
About the DCS:SA components
### Table 1-2: Key components of DCS:SA

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Virtual Appliance (SVA)</td>
<td>The SVA provides agentless anti-malware security services for VMware guest virtual machines.</td>
</tr>
<tr>
<td></td>
<td>The SVA is deployed as the Datacenter Protection Service from the vSphere web client, after registering the service with the NSX Manager.</td>
</tr>
<tr>
<td></td>
<td>DCS:SA SVA's reputation based exoneration capabilities minimizes the convictions of false positives.</td>
</tr>
<tr>
<td></td>
<td>For information on deploying and using the SVA see the <em>Symantec Data Center Security: Server Advanced Implementation Guide Integration with VMware NSX</em>.</td>
</tr>
<tr>
<td>DCS:SA agent for behavior control</td>
<td>The DCS:SA agent for behavior control provides the following capabilities:</td>
</tr>
<tr>
<td></td>
<td>■ Intercepts the system calls to enforce prevention policies</td>
</tr>
<tr>
<td></td>
<td>■ Contains multiple detection sensors for monitoring system change events and log files</td>
</tr>
<tr>
<td></td>
<td>■ Contains the tools for configuration and diagnostic support</td>
</tr>
<tr>
<td></td>
<td>■ Downloads the policies and settings from the management server and uploads events and status information to the management server</td>
</tr>
<tr>
<td></td>
<td>■ Natively supports a wide variety of Windows, UNIX and Linux servers and workstations</td>
</tr>
<tr>
<td></td>
<td>■ Supported on VMware guest systems for detection and prevention with any of the operating systems that are natively supported</td>
</tr>
<tr>
<td></td>
<td>■ Can be used to remotely monitor another host without a native agent, but note that only detection features are available in this mode</td>
</tr>
<tr>
<td></td>
<td>See the <em>Symantec Data Center Security: Server Advanced Platform and Feature Matrix</em> for more information on the supported operating systems, and agent features supported on each operating system.</td>
</tr>
<tr>
<td>Management server</td>
<td>The management server is based on Tomcat Application Server software.</td>
</tr>
<tr>
<td></td>
<td>The management server provides the following capabilities:</td>
</tr>
<tr>
<td></td>
<td>■ Secure communications with agent and console</td>
</tr>
<tr>
<td></td>
<td>■ Bulk event file storage management for efficient archival storage of all logged events</td>
</tr>
<tr>
<td></td>
<td>■ Store policies in a central location and provides an integrated, scalable, flexible, agent, and policy management infrastructure.</td>
</tr>
<tr>
<td></td>
<td>■ Alert processing (SMTP, SNMP, file), data purging, and other management functions</td>
</tr>
<tr>
<td></td>
<td>■ Coordinate policy distribution, and manages agent event logging and reporting.</td>
</tr>
<tr>
<td></td>
<td>The management server supports high availability and scalability.</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Management console</td>
<td>The management console is accessed using the thick console, and provides the following capabilities:</td>
</tr>
<tr>
<td></td>
<td>■ Policy, agent, and event management</td>
</tr>
<tr>
<td></td>
<td>■ Real-time event monitoring from the dashboard</td>
</tr>
<tr>
<td></td>
<td>■ Flexible hierarchy and agent grouping support</td>
</tr>
<tr>
<td></td>
<td>■ Event Wizard for quick policy adjustment</td>
</tr>
<tr>
<td></td>
<td>■ Querying, reporting, alerting</td>
</tr>
<tr>
<td></td>
<td>■ User and role management</td>
</tr>
<tr>
<td></td>
<td>■ Auditing console actions and server events</td>
</tr>
<tr>
<td>Database</td>
<td>The database provides the following capabilities:</td>
</tr>
<tr>
<td></td>
<td>■ Accessible through JDBC/ODBC</td>
</tr>
<tr>
<td></td>
<td>■ Stores the policies, agent information, and real-time actionable events</td>
</tr>
<tr>
<td></td>
<td>■ Lets you configure encrypted communications between the database and the management server</td>
</tr>
<tr>
<td>Predefined Detection and Prevention policies</td>
<td>The predefined Detection and Prevention policies provide the following capabilities:</td>
</tr>
<tr>
<td></td>
<td>■ Best practice policy content for operating system protection of Windows, Linux, and UNIX.</td>
</tr>
<tr>
<td></td>
<td>■ Common use case templates for creating customer-specific rules</td>
</tr>
<tr>
<td></td>
<td>■ Easy policy configuration interface</td>
</tr>
<tr>
<td></td>
<td>■ Flexible administration of the policies that are applied to agents</td>
</tr>
<tr>
<td>Predefined Anti-malware policies</td>
<td>DCS:SA SVA provides out-of-the-box anti-malware policies to protect your virtual environment against malware. SVA provides two types of policies as follows:</td>
</tr>
<tr>
<td></td>
<td>■ Antivirus policies are the policies that provide basic level and advanced level protection from malware.</td>
</tr>
<tr>
<td></td>
<td>For example, antivirus policies can be configured to provide protection to the guest virtual machines from malicious virus attacks.</td>
</tr>
<tr>
<td></td>
<td>■ Configuration policies are predefined configuration settings that are applicable to the SVA.</td>
</tr>
<tr>
<td></td>
<td>For example, configuration policies define the behavior of a SVA and can generate events if any changes are made to the configuration settings of a SVA and its services, and when the settings of scheduled scans and LiveUpdate server are changed.</td>
</tr>
</tbody>
</table>
Table 1-2  Key components of DCS:SA (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unified Management Console</td>
<td>The Unified Management Console (UMC) is a console appliance that provides a web-based console to register, configure, and manage various features and products in Symantec™ Data Center Security (DCS).</td>
</tr>
<tr>
<td>Operations Director</td>
<td>Security orchestration feature powered by Operations Director is intended to:</td>
</tr>
<tr>
<td></td>
<td>■ Automate security provisioning workflow.</td>
</tr>
<tr>
<td></td>
<td>■ Provide application-centric security service.</td>
</tr>
<tr>
<td></td>
<td>■ Seamlessly integrate with VMware NSX.</td>
</tr>
<tr>
<td></td>
<td>■ Provide out-of-box security product integration.</td>
</tr>
</tbody>
</table>

See the Symantec Data Center Security: Server Advanced Planning and Deployment Guide for detailed information on planning a DCS:SA deployment in an enterprise environment, and installing the DCS:SA components. The Symantec Data Center Security: Server Advanced Planning and Deployment Guide also provides information on the system requirements for installing the product components.

See the Symantec Data Center Security: Server Advanced Operations Director Reference Guide for more information on using Operations Director.

See the Symantec Data Center Security: Server Advanced Platform and Feature Matrix for information on the supported operating systems, and agent features supported on each operating system.

How do I achieve my objectives with DCS:SA

DCS:SA has enforcement components that you can independently activate on critical systems.

Prevention and Detection

The prevention component provides in-line prevention of potential security or compliance threats to the system before such access occurs. The detection component detects system configuration changes and monitors application and system logs for events of interest. Both components provide granular control over logging using policy settings and other agent configuration settings. Event logging provides visibility into actionable events as well as the efficient management of high volume events necessary for regulatory or forensic purposes.

Unlike the prevention component, which has proactive enforcement rules that can block activity before it occurs, the detection component monitors for system activity that has already occurred. However, the detection component can be configured
to perform local response actions, such as writing a log, killing a process, or terminating a network session. It can also run programs or scripts when a specific condition has been triggered. Thus, in combination, the two components provide unique capabilities to both secure a system and to address regulatory compliance requirements.

For example:

- Regulations such as PCI-DSS require that companies deploy file integrity monitoring for critical system and application files changes. The detection component of DCS:SA can help to meet this requirement. If your objective is to deny such changes unless they occur by trusted mechanisms, you want to use the prevention component.

- Detecting that an important operating system binary like svchost.exe was recently modified is very different from preventing the modification in the first place. DCS:SA lets you configure and use both detection capabilities and prevention capabilities as needed to address your auditing, compliance, and security requirements.

The detection component also contains operating system-specific policies that provide comprehensive operating system event monitoring and logging capabilities.

DCS:SA policies provide thousands of pre-built rules that comprehensively monitor and harden the operating system of enterprise systems and require minimal tuning.

**Malware protection for virtual environments**

SVA provides out-of-the-box anti-malware policies to protect your virtual environment against malware. SVA provides two types of policies as follows:

- Antivirus policies are the policies that provide basic level and advanced level protection from malware. For example, antivirus policies can be configured to provide protection to the guest virtual machines from malicious virus attacks.

- Configuration policies are predefined configuration settings that are applicable to the SVA. For example, configuration policies define the behavior of a SVA and can generate events if any changes are made to the configuration settings of a SVA and its services, and when the settings of scheduled scans and LiveUpdate server are changed.

See the *Symantec Data Center Security: Server Advanced Administrator's Guide* for detailed information on using DCS:SA to meet your objectives.
Preventing potential security or compliance threats to the assets

Prevention policies provide in-line prevention of potential security or compliance threats to the system before such access occurs. The prevention policies confine each process on a computer to its normal behavior. Programs that are identified as critical to system operation are given specific behavior controls, while generic behavior controls provide compatibility for other services and applications.

Policies have options that let you configure a policy for assignment to a target computer. Policy options comprise a simplified set of controls that you can use to enable or disable features in a policy. Some options have parameters, which let you customize the behavior of the option.

You use the Policy Builder wizard to create the prevention policies. The policies which you create are stored in the policy library.

Following are some examples of how you can use prevention policies to prevent potential security or compliance threats to the assets:

- System hardening: Lock down configuration and settings of critical servers
- Least privilege access control: Restrict the behavior of applications and operating systems using granular policy based controls
- Compensating HIPS controls: Use the policy-based least privilege access control to assist in meeting compliance requirements


Detecting configuration changes and monitoring for events of interest

Detection policies monitor important system and application files and registry entries, system and application logs, and other system data sources to detect and notify you when suspicious activity is occurring on your systems. This monitoring can provide compliance with regulatory, industry or organizational standards and requirements.

Some of the features provided by the intrusion detection policies are:

- Real-time file integrity monitoring: Identify changes to files in real-time including who made the change and what change occurred
- Configuration monitoring: Identify policy violations and suspicious activity in real-time
- Logons/Logoffs Monitoring
Security Configuration Changes
Active Directory Changes
Shares Configuration Changes
Domain Trust Changes
UNIX User/Group Account Modification

You use the Policy Builder wizard to create the detection policies. The policies which you create are stored in the policy library.


Securing guest virtual machines against malware

The DCS:SA Security Virtual Appliance (SVA) provides agentless, antivirus and antimalware security services for VMware virtual machines. SVA's uses Symantec Insight reputation technology to reduce the occurrence of false positives.

SVA provides a mechanism to secure guest virtual machines against malware attack without installing any agent software on the guest virtual machine.

The policy library contains antivirus and antimalware policies that you can use and customize to protect your virtual appliances.

SVA provides two types of policies as follows:

- Antivirus policies are the policies that provide basic level and advanced level protection from malware.
- Configuration policies are predefined configuration settings that are applicable to security virtual appliances.

You use the DCS:S to monitor the Datacenter protection status. After you register the Datacenter Protection Service with VMware, you can view the security groups, run scans on a guest virtual machine or on a security group, view the command status, run LiveUpdate on a security virtual appliance, view alerts and notifications that are received from the security virtual appliance, and the overall health of the datacenter.

SVA includes the queries and reports with charts, graphs, and tables that provide detailed and aggregated summary data about security virtual appliances, events, agents, and policies. You can also create your own queries and reports. On the basis of scan results, the guest virtual machines receive a tag to specify its state. You can decide upon the preventive measure to adopt in case a threat is detected.
See the Symantec Data Center Security: Server Advanced Implementation Guide Integration with VMware NSX for detailed information on using SVA to secure guest virtual machines against malware.

**Orchestrating security using Operations Director**

Operations Director automates a lot of manual activity involved in security provisioning where the security administrator is unable to decide the right security policies for a virtual machine/application. Based on the state of your production environment, Operations Director derives the right security profile and security policies to be applied to secure an application.

Operations Director provides a robust workflow to manage communication and sequence of security provisioning operations between:

- Server administrator (who manages the virtual infrastructure and has requirements for securing the virtual infrastructure) and
- Security administrator (who manages the security provisioning).

Operations Director interoperates with registered security products such as, Symantec Data Center Security: Server Advanced, and Palo Alto Networks Next Generation Firewall to synchronize and leverage the latest security policies from these security products for securing a virtual machine/vApp.

See “About Operations Director” on page 10.

See “Advantages of Operations Director” on page 11.

**Integrating with data center orchestration tools**

RESTful APIs provide support for additional platforms and integration.

To access the RESTful APIs, you must perform the following tasks:

- Generate UMC token
  See To generate UMC token

- Access RESTful APIs
  See To access RESTful APIs
To generate UMC token

1. Make a post request to the following URL with the Json request:

   ```
   POST https://<UMC server IP>:8443/umcservices/rest/v1.0/auth/token
   
   Json request: { "username":"dcsadmin", "password":"password" }
   ```

   The password for dcsadmin is the one specified while deploying UMC. In case of an AD user, the username is domain alias name\username and the password is the configured AD password for that user.

   A token is generated.

2. Pass the token that is generated in step 1 to all the subsequent requests.

   Pass token header:

   ```
   Content-Type: application/json
   Authorization: bearer UMC token
   ```

To access RESTful APIs

1. Enter the following URL in your browser:

   ```
   https://<DCS server-IP:PortNumber>/sis-ui/api/
   ```

   Enter the IP address and the port number of the Management Server, in the Server and Port fields.

2. In the Data Center Security: Server API documentation page, click Details. API information is displayed.

How DCS:S works

DCS:S provides a mechanism to secure guest virtual machines against malware attack. The DCS:S policy page displays policies that are published, unpublished, and modified. The unpublished policies are editable and can be applied to guest virtual machines only when they are published.

The three types of policies are as follows:

- Antivirus policies
  Antivirus policies provide basic level and advanced level protection from malware. For example, antivirus policies can be configured to provide protection to the guest virtual machines from malicious virus attacks.

- Network security policies
  Network Security policies are used for specifying settings to monitor Network traffic.
SVA configuration policies
SVA configuration policies are predefined configuration settings that are applicable to Security Virtual Appliances.

For example, configuration policies define the behavior of a SVA and can generate events if any changes are made to the configuration settings of a SVA and its services, and when the settings of scheduled scans and LiveUpdate server are changed.

The following diagram illustrates a high-level work flow of DCS:S.

Figure 1-2 DCS:S work flow diagram

You use the Unified Management Console to monitor the Datacenter protection status. After you register the Datacenter Protection Service with VMware, you can view the security groups, run scans on a guest virtual machine or on a security group, view the command status, run LiveUpdate on a SVA, view alerts and notifications that are received from the SVA, and the overall health of the datacenter.

DCS:SA also allows you to create queries and reports with charts, graphs, and tables that provide detailed and aggregated summary data about Security Virtual Appliances, events, agents, and policies appears in DCS:SA. On the basis of command result, the guest virtual machines receive a tag to specify its state. You can decide upon the preventive measure to adopt in case a threat is detected.
About predefined policies

DCS:S offers three predefined policies — two antivirus policies, one network security policy, and one configuration policy. The antivirus policies consist of the configuration settings on how protection can be provided to the guest virtual machines. The configuration policy has the configuration settings that are applicable to the security virtual appliances. At any point in time, only one SVA configuration policy and one Network security policy can be published for all the security virtual appliances.

**AV Policy – Scan On Apply**

The **AV Policy – Scan On Apply** scans the guest virtual machines within a security group for virus and threats as per the configured settings in the policy. When an antivirus policy is bound with the NSX security policies, and then applied to a security group, and the **AV Policy – Scan On Apply** is applied, all the guest virtual machines within the security group are scanned as per the configured settings. The configuration settings for this policy that are available by default are:

- On-access threat protection
- Reputation lookups
- Delete threat on detection
- Add security tags to the guest virtual machines on threat detection
- Scan guest virtual machines when the policy is applied
- Remove tag after clean and successful completion of scan

**AV Policy – Scan On Access**

Whenever a file or folder is accessed on a guest virtual machine, all the settings that were configured for the **AV Policy – Scan On Access** comes into effect. The default options available are on-access threat protection, reputation lookups, and add security tags to the guest virtual machines. The delete threat on detection and scan the guest virtual machines when the policy applied options are not available by default.

Whenever a file or folder is accessed on a guest virtual machine, all the settings that were configured for the **AV Policy – Scan On Access** comes into effect. The
**AV Policy – Scan On Access** can be applied on Windows and Linux GVMs. The default options available are on-access threat protection, reputation lookups, and add security tags to the guest virtual machines. The delete threat on detection and scan the guest virtual machines when the policy applied options are not available by default.

While configuring the AV Policy – Scan On Access settings, if you do not enable the Delete Threat option, multiple events are generated each time the same threat is detected. The events are not suppressed, and you can view them in the web console by grouping the related events together.

**Network Security Policy**

Network Security policies are used for specifying settings to monitor Network traffic. If the block option is checked, it detects, logs, and blocks the network threat. If the block option is unchecked, then it detects and logs the Network threat.

You can define the traffic to be monitored by selecting from the following options:

- All endpoints (servers and desktops)
- All server
- Only Microsoft Exchange Server
- All desktops

**SVA Config Base Policy**

The **SVA Config Base Policy** defines the communication settings and external server settings of the security virtual appliance. Only one predefined **SVA Config Base Policy** gets published after the security virtual appliance is registered. This policy cannot be unpublished, but can be replaced with a new instance of the **SVA Config Base Policy**.

**Where to get more information**

Product manuals for DCS:SA are available on the DCS:SA product media. Updates to the documentation are available from the Symantec Technical Support and Business Critical Services (BCS) Web sites.

The DCS:SA product manuals are as follows:

- Installation Guide Online Help
- DCS:SA Online Help
- Planning and Deployment Guide
- Overview Guide
The following table lists additional information that is available from the Symantec Web sites.

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Web address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Knowledge Base</td>
<td><a href="http://www.symantec.com/business/support/">http://www.symantec.com/business/support/</a></td>
</tr>
<tr>
<td>Releases and updates</td>
<td></td>
</tr>
<tr>
<td>Manuals and other documentation</td>
<td></td>
</tr>
<tr>
<td>Contact options</td>
<td></td>
</tr>
<tr>
<td>Virus and other threat information and updates</td>
<td><a href="http://securityresponse.symantec.com">http://securityresponse.symantec.com</a></td>
</tr>
</tbody>
</table>