



Conditions and Terms of Use

Microsoft Confidential

This training package is proprietary and confidential, and is intended only for uses described in the training materials. Content and software is provided to you under a Non-Disclosure Agreement and cannot be distributed. Copying or disclosing all or any portion of the content and/or software included in such packages is strictly prohibited.

The contents of this package are for informational and training purposes only and are provided "as is" without warranty of any kind, whether express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

Training package content, including URLs and other internet website references, is subject to change without notice. Because Microsoft must respond to changing market conditions, the content should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Copyright and Trademarks

© 2010 Microsoft Corporation. All rights reserved.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

For more information, see **Use of Microsoft Copyrighted Content** at <https://www.microsoft.com/en-us/legal/intellectualproperty/copyright/default.aspx>

Microsoft®, Internet Explorer®, Outlook®, SkyDrive®, Windows Vista®, Zune®, Xbox 360®, DirectX®, Windows Server® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other Microsoft products mentioned herein may be either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.

Agenda

- Cluster Security
- Node Application Security

Microsoft Confidential



Service Fabric cluster security scenarios

- Node-to-Node security
- Client-to-Node security
- Role-based access control (RBAC)

MICROSOFT CONFIDENTIAL

Azure Key Vault and Cluster security

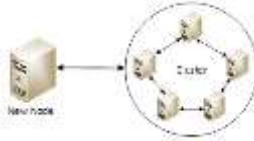
- Azure Key Vault is used to manage certificates used for cluster security
- Certificates can be for node-to-node or client-to-node security
- Azure resource provider pulls certificates from vault and installs them on the cluster
- Create your key vaults in a separate resource group



MICROSOFT CONFIDENTIAL

Node-to-Node security

- Secures communication between VMs within the cluster
- Ensures that only computers authorized to join the cluster can host applications in the cluster
- Use either Certificate based security or Windows Security
- Changing the security type (certificate vs. Windows) will require cluster redeployment



MICROSOFT CONFIDENTIAL

Node-to-Node security – Certificate based

- Certificate based security
 - X.509 certificates become part of the node-type configuration at cluster creation time
 - Certificate security can be configured via the Azure Portal or ARM templates
 - Can have both a primary and secondary certificate to be used for certificate rollovers
 - Make sure the primary and secondary certs are different than the admin client and read-only client certs
 - Private key files (.pfx) for certificates must be in a special JSON format (Azure Resource Provider requirement)
- Certificate must be installed in Azure Key Vault

MICROSOFT CONFIDENTIAL

Node-to-Node security – Windows based

- For standalone Windows Server deployments
- Requires either a Windows Server Active Directory Group or an Azure AD Group
- Requires node machines to be joined to the domain
- Using Azure Active Directory
 - Use Azure AD Domain Services (requires a classic virtual network)
 - Use VNet peering to join cluster virtual network to classic virtual network
 - Join cluster machines to the Azure AD DS domain
- Using Windows Server Active Directory
 - Create a Windows domain controller in Azure IaaS or use VPN to connect to on-premises Windows domain
 - Join node machines to the Windows domain

MICROSOFT CONFIDENTIAL

Node-to-Node security – Windows based

Setup of Windows security uses a ClusterConfig.Windows.*.JSON file

```
"security": {
  "ClusterCredentialType": "Windows",
  "ServerCredentialType": "Windows",
  "WindowsIdentities": {
    "ClusterIdentity": { "Id": "domain/machinegroup", "IsAdmin": true, "ClientIdentities": {
      [ { "identity": "domain/username",
        } ]
    }
  }
}
```

*Represents the type of cluster, ie DevCluster, MultiMachine

Download <http://go.microsoft.com/fwlink/?LinkId=730690>

MICROSOFT CONFIDENTIAL

Client-to-Node security – Certificate based

- Authenticates clients and secures communication between client and individual cluster nodes
- Only authorized users can access the cluster and apps deployed on the cluster
- Clients are uniquely identified through certificate security credentials
- Certificate security can be configured via the Azure Portal or ARM templates
- Can have both a primary and secondary certificate to be used for certificate rollovers
 - Make sure the primary and secondary certs are different than the admin client and read-only client certs
- Certificate must be installed in Azure Key Vault
- Good for service development and testing, but best practice is to use Azure AD for Client-to-Node security

MICROSOFT CONFIDENTIAL

Client-to-node security – Azure AD

- Create certificates for node-to-node security (recommended)
- Certificates will be placed in Azure Key Vault (required)
- Create two Azure AD apps ~ one for Service Fabric Explorer and one for Visual Studio (recommended)
- Assign users to the roles that are supported by Service Fabric: read-only and admin
- <https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-cluster-creation-via-arm>

MICROSOFT CONFIDENTIAL

Role-based Access Control (RBAC)

- Two different access control types for clients
 - Administrators – full access to manage capabilities (read/write)
 - Users – read-only access, query capabilities, resolve applications and services
- Certificate only client-to-node - Specify the two client roles at creation time by providing separate certificates
- Azure AD client-to-node – Setup roles in an Azure AD group
- <https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-cluster-security-roles>

MICROSOFT CONFIDENTIAL

Network Isolation with Service Fabric (example)



MICROSOFT CONFIDENTIAL

Ports settings required example topology

Priority	Name	Source	Destination	Service	Action
3900	allowSvcFabPortal	Any	Any	Custom (ANY/19080)	Allow
3910	allowSvcFabClient	Any	Any	Custom (ANY/19000)	Allow
3920	allowSvcFabCluster	VirtualNetwork	Any	Custom(ANY/1025-1027)	Allow
3930	allowSvcFabricPhemeral	VirtualNetwork	Any	Custom(ANY/49152;65534)	Allow
3940	allowSvcFabSMB	VirtualNetwork	Any	Custom(ANY/445)	Allow
3950	allowVNetRDP	VirtualNetwork	Any	Custom(ANY/3389)	Allow
3960	allowJumpBoxRDP	Any	10.0.3.4*	Custom(ANY/3389)	Allow
4000	blockAll	Any	Any	Custom(ANY/Any)	Deny

MICROSOFT CONFIDENTIAL

More information...

- <https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-cluster-security>

MICROSOFT CONFIDENTIAL



Service Fabric application security

- Applications can be secured to run under different user accounts
- Service Fabric can secure resources used by applications at deployment time
- Applications run under the account that Fabric.exe runs under
- Applications can also run under LocalUser, NetworkService, LocalService and LocalSystem
- Standalone deployments would use AD domain accounts

MICROSOFT CONFIDENTIAL

Service SetupEntryPoint – ServiceManifest.xml

- SetupEntryPoint – privileged entry point that runs as NetworkService account
- EntryPoint executable is typically a long running service host
- EntryPoint executable runs after SetupEntryPoint

```
<CodePackage Name="Code" Version="1.0.0">
  <SetupEntryPoint>
    <ExeHost>
      <Program>MySetup.bat</Program>
      <WorkingFolder>CodePackage</WorkingFolder>
    </ExeHost>
  </SetupEntryPoint>
  <EntryPoint>
    <ExeHost>
      <Program>MyServiceHost.exe</Program>
    </ExeHost>
  </EntryPoint>
</CodePackage>
```

MICROSOFT CONFIDENTIAL

Running the startup script as a local system account

- Generally recommended NOT to run a startup script as an administrator
- Recommended to run as LocalSystem
- Setup in the ApplicationManifest.xml file

```
<ServiceManifestImport>
  <ServiceManifestRef ServiceManifestName="MyServiceTypePkg" ServiceManifestVersion="1.0.0" />
  <ConfigOverrides />
  <Policies>
    <RunAsPolicy CodePackageRef="Code" UserRef="SetupLocalSystem" EntryPointType="Setup" />
  </Policies>
</ServiceManifestImport>
<Principals>
  <Users>
    <User Name="SetupLocalSystem" AccountType="LocalSystem" />
  </Users>
</Principals>
</ApplicationManifest>
```

MICROSOFT CONFIDENTIAL

More information...

<https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-application-runs-as-security>

MICROSOFT CONFIDENTIAL

Demonstration

Web API Services with OWIN
Self-Hosting





© 2013 Microsoft Corporation. All rights reserved.
